TACACS+ op een Aironet access point voor loginverificatie met gebruik van het GUIconfiguratievoorbeeld

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Configureren Netwerkdiagram Configureer de TACACS+ server voor inlogverificatie - met behulp van ACS 4.1 Configureer de TACACS+ server voor inlogverificatie - met behulp van ACS 4.1 Configureer de Aironet AP voor TACACS+ verificatie Verifiëren Verificatie voor ACS 5.2 Problemen oplossen Gerelateerde informatie

Inleiding

Dit document legt uit hoe u TACACS Plus (TACACS+) services kunt inschakelen op een Cisco Aironet Access Point (AP) om inlogverificatie met gebruik van een TACACS+ server uit te voeren.

Voorwaarden

<u>Vereisten</u>

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Kennis van de manier waarop u fundamentele parameters op Aironet APs kunt configureren
- Kennis van de manier waarop u een TACACS+ server kunt configureren zoals Cisco Secure Access Control Server (ACS)
- Kennis van TACACS+-concepten

Raadpleeg voor informatie over de manier waarop TACACS+ werkt het <u>begrip TACACS+</u> gedeelte van <u>RADIUS- en TACACS+ servers configureren</u>.

Gebruikte componenten

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

- Aironet Cisco Aironet 1240/1140 Series access points
- ACS dat softwareversie 4.1 uitvoert
- ACS dat softwareversie 5.2 uitvoert

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.

<u>Configureren</u>

Deze sectie legt uit hoe u Aironet AP en de TACACS+ server (ACS) moet configureren voor TACACS+-gebaseerde aanmelding-verificatie.

Dit configuratievoorbeeld gebruikt deze parameters:

- IP-adres van de ACS-172.16.1.1/255.255.0.0
- IP-adres van AP-172.16.1.30/255.255.0.0
- Gedeelde geheime sleutel die op AP en TACACS+ server-Voorbeeld wordt gebruikt

Dit zijn de referenties van de gebruiker die dit voorbeeld op ACS vormt:

- Gebruikersnaam-Gebruiker1
- Wachtwoord—Cisco
- Groep-Admin-gebruikers

U dient de functies TACACS+ te configureren om de gebruikers te valideren die proberen verbinding te maken met de AP via de webinterface of via de opdrachtregel interface (CLI). Om deze configuratie te kunnen uitvoeren, dient u deze taken uit te voeren:

- 1. Configureer de TACACS+ server voor inlogverificatie.
- 2. Configureer de Aironet AP voor TACACS+ verificatie.

N.B.: Gebruik het <u>Opdrachtupgereedschap</u> (<u>alleen geregistreerde</u> klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configureer de TACACS+ server voor inlogverificatie - met behulp van ACS 4.1

De eerste stap is het instellen van een TACACS+-daemon om de gebruikers te valideren die proberen toegang te krijgen tot de AP. U moet de ACS voor TACACS+ verificatie instellen en een gebruikersdatabase maken. U kunt elke TACACS+ server gebruiken. Dit voorbeeld gebruikt ACS als de TACACS+ server. Voer de volgende stappen uit:

 Voltooi deze stappen om het AP toe te voegen als een verificatie-, autorisatie- en boekhoudcliënt (AAA):Klik vanuit de ACS-GUI op het tabblad Netwerkconfiguratie.Klik onder AAA-clients op Toevoegen.Voer in het venster Add AAA Client de AP host-naam, het IPadres van de AP en een gedeelde geheime sleutel in.Deze gedeelde geheime sleutel moet dezelfde zijn als de gedeelde geheime sleutel die u op de AP vormt.Selecteer in het vervolgkeuzemenu Verifiëren met behulp van TACACS+ (Cisco IOS).Klik op Indienen + Herstart om de configuratie op te slaan.Hierna volgt een

CiscoSecure ACS - 1	Microsoft Internet Explorer	
Elle Edit View Fg	prantes Iools Help	Leás 🏁 🎊
Address 🙆 http://127.	0.0.1:1065/	🔊 🔁 🐑
Cisco Storeus	Network Configuration	×
allboatlbo		A Help
User Setup	Add AAA Client	AAA (lisst Hestning
Eroup Setup		AAA Client IP Address Shared Secret
(b. Shared Profile	AAA Client Hostname AccessPoint	Saturate Device Group BADDIS For Write
Components	AAA Client IP Address	Authenticate Using Single Cenerct TACACS+ AAA Client
Configuration	<u>×</u>	Log Undate/Watchdog Packets from this AAA Client
System Configuration	Shared Secret Example	Log SADIUS Tonneling Packets from this AAA.Client
Configuration	RADIUS Key Wrap	Beplace RADUPS Part into with Username from this AAA Client Model from the AAA Client
Administration	Key Encryption Key	address for accounting packets from this AAA client
10 External User	Message Authenticator Code	
0 Ol Dutabases	Key Input Format C ASCII @ Hexadecimal	AAA Client Hastaure
Validation		
Network Access Profiles	Authenticate Using TACACS+ (Cisco IOS)	name assigned to the AAA client.
Reports and Activity	Single Connect TACACS+ AAA Client (Record stop in accounting on failure)	Back to Teel
In Dalias	Log Update/Watchdog Packets from this AAA Client	AAA Client IP Address
Carl Documentation	Log RADIUS Tunneling Packets from this AAA Client	The AAA Client IP Address is the IP address assigned to the
	Replace RADIUS Port info with Username from this AAA Client	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 reactly the IP address for each
	Submit Submit + Apply Cancel	AAA client to be represented by this AAA client entry. To reparate each IP address, press Eater.
Lana and the second		- L-L

In dit voorbeeld wordt gebruik gemaakt van:Het AAA-**clientadapterpunt**Het adres **172.16.1.30/16** als het AAA-client-IP-adresHet gedeelde geheime sleutelvoorbeeld

2. Voltooi deze stappen om een groep te maken die alle administratieve (admin) gebruikers bevat:Klik op Groepsinstelling in het menu links.Er verschijnt een nieuw venster.Selecteer in het venster Groepsinstallatie een groep die u in het vervolgkeuzemenu wilt configureren en klik op Hernoemen.Dit voorbeeld selecteert Groep 6 in het vervolgkeuzemenu en geeft de groep AdminGebruikers een andere naam.Klik op Inzenden.Hierna volgt een voorbeeld:

CiscoSecure ACS -	Microsoft Internet Explorer	
Ele Edt Yew Fg	workes Iools Help	Leis 🀲 🍂
Address http://127.	0.0.1:1965/	ى 🛃 💌
Cisco Statens	Group Setup	×
at the at the	Select	Help
User Setup	Renaming Group: Group 6	Rename Group
Betup		
StaredProfile Components	Group AdminUsers	Rename Group
Network Configuration	Submit Cancel	Type a new group name and click Submit to assign a more descriptive name to the group posfis. This is useful if different groups have been configured to allow specific authorization privileges, such to DBA or Today and to allow specific authorization privileges, such
Configuration	😤 Back to Hirlp	Click Cancel to return to the Group Setup window without saving a new cross name.
Configuration		March at Wash
Administration Centrel		LEACE TO THE
Diternal User Databases		
Validation		
Parfiles		
Reports and Activity		
Documentation		
		internet.

3. Voltooi deze stappen om de gebruikers aan de TACACS+-database toe te voegen:Klik op het tabblad Gebruikersinstelling.Als u een nieuwe gebruiker wilt maken, voert u de gebruikersnaam in het veld Gebruiker in en klikt u op Toevoegen/Bewerken.Hier is een voorbeeld dat Gebruiker1 maakt:



Nadat u op Toevoegen/Bewerken klikt, verschijnt het venster Toevoegen/Bewerken voor deze gebruiker.

4. Voer aanmeldingsgegevens in die specifiek zijn voor deze gebruiker en klik op Indienen om de configuratie op te slaan.De geloofsbrieven die u kunt binnengaan omvatten:Aanvullende gebruikersinformatieInstellingen gebruikerDe groep waaraan de gebruiker is toegewezenHierna volgt een voorbeeld:

CiscoSecure ACS - Microsoft Internet Explorer	X
Ele Edt Yew Favortes Iools Help	Links 🇯 👫
Address a http://127.0.0.1:1065/	💌 🄁 60
User Setup	
User User: User1 (New User) Strop Account Disabled SharedPrefile Account Disabled Supplementary User Info ? Supplementary User Info ? Supplementary User Info ? Configuration Real Name User1 Description Description Pestweek Database ? Password Authentication: ACS Internal Database Validation CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not	Account Disabled Deleting a Username Supplementary User Infe Passweed Authentication Callback Callback Callback Callback Callback Callback Meansed Settlines Mars Sections Vasae Overlaw Antiperson Vasae Overlaw Vasae Overlaw TACASS - Enable: Control TACASS - Shell Common A Authorization Cammand Authorization for Network Device Management Applications TACASS - Usebared Passweed TACASS - Shell Command Authorization Command Authorization for Network Device Management Applications TACASS - Usebared Passweed TACASS - Usebared Passweed TACASS - Usebared Passweed TACASS - Shell Command Authorization Command Authorization for Network Device Management Applications TACASS - Usebared Passweed TA
Reports and Activity Checked.) Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password Confirm Password Submit Cancel	Account Disabled Status Select the Account Disabled check box to disable this account; clear the check box to anable the account. [Back to Top] 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 current user account from the database, click Delete. When asked to cenfirm your action, click OK.
a)	g Internet

U kunt zien dat dit voorbeeld de gebruiker User1 aan de groep AdminGebruikers toevoegt.

EiscoSecure ACS -	Microsoft Internet Explorer	X
Ele Edt Yew Fg	vorites Iools Help	Links 🍟 🎇
Address an http://127.	0.0.1:1065/	💌 🄁 😡
Custe Startens	User Setup	×
User	User Setup	A Help
Composents Composents Composents Configuration Configuration	Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.) Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.	Account Disabled Orielises a Unername Supplementary User Info Reserved Arthentication Croup to which the user is assigned Callback Client IP Address Assignment Advanced Settings Network Access Restrictions Network Restrictions Networ
Reports and Activity Online Documentation	Group to which the user is assigned: AdminUsers Callback Use group setting No callback allowed Callback using this number	Account Disabled Status Select the Account Disabled check box to disable this account; clear the check box to enable the account. [Back to Tap] 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

N.B.: Als u geen specifieke groep maakt, worden de gebruikers toegewezen aan de

standaardgroep.

5. Voltooi deze stappen om het voorkeursniveau te bepalen:Klik op het tabblad Groepsinstallatie.Selecteer de groep die u eerder aan deze gebruiker hebt toegewezen en klik op Instellingen bewerken.Dit voorbeeld gebruikt de groep AdminGebruikers.Controleer onder TACACS+ instellingen het aanvinkvakje Shell (exec) en controleer het aanvinkvakje Privileniveau dat een waarde van 15 heeft.Klik op Inzenden + opnieuw starten

CiscoSecure ACS - M	licrosoft Internet Explorer					
Elle Edit View Fav	orites Iools Help	Links ¹⁹ 💐				
Address Altp://127.0	1.0.1:1065/					
Cisco Systems	Group Setup					
albudb.	Jump To Access Restrictions	Help				
User Setup	In access control list	Group Disabled Voice-over-IP (YoTP) Support				
Shared Profile	Out access control list Route Route	Ourfault Time:of-Day Access Settings Callback Notwork Access Bestrictions				
Network Configuration	Routing Enabled Note: PPP LCP will be automatically enabled if this service is enabled	Man Sessions Unace Quetas Enable Options Takes Card Settings				
System Configuration	Shell (exec)	Passessed Aging Bales PLAssignmentS Devenleadable ASLs TACACS - Settings				
Administration Centrel	Auto command	TACACS+ Shell Command Authorization Command Authorization for Network Device Management Applications TACACS+ Unknown Services TATE RANDUS Attributes				
Dutabases	Calback rotary	RADIUS Yender Specific Attributes				
Network Access Profiles	Idle time No callback verify Enabled No escape Enabled	To enable administrators to tailor what authorizations are displayed for a configuration and to simplify the interface, ACS displays only the information for the current configuration. Specific Group Setup				
Activity	No hangup Enabled	configuration options and security protocol attributes are displayed in Group Setup only in the following circumstances:				
Documentation	Timeout	 A AAA dient that uses the specified protocol has been configured in the Network Configuration section. For example, RADDUS settings appear only if you have configured a AAA client that uses RADDUS. The specific services, protocols, and attributes have been selected 				
	Shell Command Authorization Set	for display for the appropriate protocol in the Interface Configuration section. • A Token Card Server has been configured in the External User Databases section.				
	Assign a Shell Command Authorization Set for any Submit Submit + Restart Cancel	Group Setup is used to enable and configure the particular authorizations assigned to an entire group of users. The group a user is assigned to is configured in the User Setup				
a)	1	X Diternet				

Opmerking: Privacyniveau 15 moet voor de GUI en telnet worden gedefinieerd om toegankelijk te zijn als niveau 15. Anders kan de gebruiker standaard alleen toegang hebben tot niveau 1. Als het voorkeursniveau niet is gedefinieerd en de gebruiker probeert om mode op de CLI (met gebruik van telnet) in te schakelen, wordt deze foutmelding weergegeven door AP:

AccessPoint>enable % Error in authentication

Herhaal stap 2 tot en met 4 van deze procedure als u meer gebruikers aan de TACACS+ database wilt toevoegen. Nadat u deze stappen hebt voltooid, is de TACACS+ server klaar om gebruikers te valideren die proberen in te loggen op AP. U moet nu de AP configureren voor TACACS+ verificatie.

Configureer de TACACS+ server voor inlogverificatie - met behulp van ACS 5.2

De eerste stap is om AP als een AAA-client in de ACS toe te voegen en een TACACS-beleid te maken voor de inlognaam.

1. Voltooi deze stappen om AP als een AAA-client toe te voegen:Klik vanuit de ACS GUI, op Netwerkbronnen en vervolgens op Netwerkapparaten en AAA-clients.Klik onder Netwerkapparaten op Maken.Voer de hostnaam van de AP in in Name, en geef een beschrijving van de AP.Selecteer de locatie en het type apparaat als deze categorieën zijn gedefinieerd.Omdat slechts één AP wordt gevormd, klik op ÉÉN IP Adres. U kunt het bereik van IP-adressen toevoegen voor meerdere AP's door op IP-bereik(s) te klikken. Voer vervolgens het IP-adres van het AP in.Onder Verificatieopties, controleer het TACACS+ vakje en voer het gedeelde geheim in.Hierna volgt een voorbeeld:

* 🚭 My Workspace	Network Resources - Network Devices and AAA Clients - Create							
Ale Terrere Development Network Device Groups Location Device Type	e Name AP1140 Description: Autonomous AP1140 et foor 1 Network Device Groups							
Default Network Device	Cocason Al Cocasons	Deed						
Surray and identity Divers	Device Type All Device Types	Seed						
Gy Policy Elements	P Address		Authentication Options + TACACE+ - 2					
 Access Policies 	Single P Address () IP Range(s)		Engrad Secret circo					
 Monitoring and Reports 	6 P 172161.30		Engle Connect Desize					
 Bystem Administration 			Legacy TACACS+ Single Connect Support TACACS+ Draft Compliant Single Connect Support RADIUS					
Alternation of the second	a - Required fields							
	Gubmit: Cancel							

2. De volgende stap is het maken van een inloggebruikersnaam en een wachtwoord:Klik op Gebruikers en identiteitsopslag en vervolgens op gebruikers.Klik op Maken.Geef de gebruikersnaam op onder Naam en geef een beschrijving.Selecteer de eventuele identiteitsgroep.Voer het wachtwoord in onder het tekstvak Wachtwoord en voer het opnieuw in onder Wachtwoord voor bevestigen.U kunt het wachtwoord voor het inschakelen wijzigen door een wachtwoord in te voeren onder Wachtwoord voor inschakelen. Voer dit nogmaals in om het te bevestigen.Hierna volgt een voorbeeld:

By Network Resources	Comment of	Concerne and the second	Consider the Constant of the				
Identify Oncups Indemail Identify Stores Hotols Idential Identify Stores LDAP Active Directory RIAL Security Textee Centificate Authonities Centificate Authonities	Name Stand St	Babs: Enabled	Select Select	Enable Password Info Password must. • Contain 4 - 12 Enable Password Optime Password	ormation characters		

3. Voltooi deze stappen om het voorkeursniveau te bepalen:Klik op **Beleidselementen** > **Vergunningen en toegangsrechten** > **Apparaatbeheer** > **Shell-profielen**.Controleer het

dialoogvenster **Toegang toestaan** en klik op **Dupliceren**.

• of MyWorkspace	Policy Denents + Authorization and Pensissions + Device Automativation + Shell Profiles	
+ () Network Resources		and the second
• 🗃 Users and Identity Stores	Shell Proteins	Showing 1-1 of 1 50 + per page 00
+ Q. Policy Lienants	Fiber • Match if • 00 •	
+ Session Conditions	🛛 📝 Name 🔺 Description	
Date and Time	Pernel Access	
Aldhorcation and Permissions Network Access Derice Administration Command Bets Named Permission Objects Access Policies Monitoring and Reports		
 Bydem Administration 		
	Consta Dunkrata Edit Deleta	TO TE Pane 1 of the Pa

Voer de naam en de beschrijving

in.		
cisco Cisco Secure	ACS	wey) LogOut Almost Help
• 😴 MyWorkspace	Policy Benerits + Authorization and Pennissions + Device Administration + Shell Publics + Duplicate: "Pennit Access"	
Session Conditions	General Common Tasks Custom Attributes Name: Autonomous AP Description: TACAC9+ login for Autonamous AP	
Date and Time	Required fields	A STATE OF A
Network Conditions Authorization and Permissions Network Access Device Administration Original Administration Command Sets Namee Permission Objects		
• 🕞 Access Policies		
• 🔯 Monitoring and Reports		
	Gutmit Carxiel	

Selecteer het tabblad Common Tasks en kies **15** voor de maximale prioriteit.

🚯 MyWorkspace	Policy Denents > Authorization	and Permissions	+ Device	Administr	ation > Shell Profi	es > Daploate	"Peret Access"			
Antwork Resources Users and Identify Sores Descin Conditions Date and Time Date and Time Suborx Conditions Network Access Network Access Network Access Antwictation and Persons Antwictation and Reports Manteoing and Reports System Administration	General Common Ia Philosof Level Dataut Philosof I Scient Philosof I Scient Philosof I Scient Philosof I Scient Philosof I Scient Philosof I Auto Command No Caliback Venty No Escape No Hang Up Timeout Ide Time Caliback Line Caliback Line Caliback Line Caliback Line	Asks Custom Notion Uber = State = Notion Uber =	Ville	15 0 1 2 3 4 5 6 7 8 9 10 15 15 13 14 15 14 16						

Klik op Inzenden.

4. Voltooi deze stappen om een autorisatiebeleid te creëren:Klik op **Toegangsbeleid** > **Toegangsservices** > **standaard apparaatbeheer** > **autorisatie**.Klik op **Maken** om een nieuw Vergunningsbeleid te creëren.Een nieuwe pop-up lijkt de regels voor het machtigingsbeleid te creëren.Selecteer de optie **Identity Group**, **Location** enz. voor de specifieke gebruikersnaam en AAA-client (AP), indien aanwezig.Klik op **Selecteren** voor het Shellprofiel om het profiel te kiezen dat met Autonome AP is

gemaakt. cisco Cisco Secure ACS Cisco Secure ACS - Mobilia Firefo s52 diversity) Log Dut About H E https://28.306.127.36 ► ∰ MyWorkspace Access Fulcies General + (5) Network Resources Standard Pot Name: Autonomous AP Status: Enabled . . + 👪 Users and Identity Stores. Device Ar The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available for the policy rules acreen controls which * Q Policy Elements Filter Stat policy conditions and results are available here for use in policy rules Access Services
 El Service Selection Rules
 O Default Device Admin Conditions E Identity Oroup: -ANY 1 1 **Identity** NDO Location -ANY-NDO Device Type: -ANY-. O Default Network Access Time And Date: -ANI-* 📳 Monitoring and Reports Results Bystem Administration. Shell Profile: Autonomous AP Delect --Customize Hit Count Create

Klik op **Wijzigingen opslaan** nadat dit is gedaan.Klik op **Standaard apparaatbeheer** en klik vervolgens op **Toegestane protocollen**.Controleer **PAP/ASCII toestaan** en klik op **Inzenden**.Klik op **Service Selection Regels** om er zeker van te zijn dat er een TACACS-regeling wordt aangepast en dat u naar Default Devices Admin wijst.



Configureer de Aironet AP voor TACACS+ verificatie

U kunt CLI of GUI gebruiken om de TACACS+ functies op Aironet AP in te schakelen. In deze sectie wordt uitgelegd hoe u de AP voor TACACS+ aanmelding-verificatie kunt configureren met gebruik van de GUI.

Voltooi deze stappen om TACACS+ op het AP te configureren met behulp van de GUI:

 Voltooi deze stappen om de parameters van de TACACS+ server te definiëren:Kies in de AP GUI, Security > Server Manager.Beveiliging: Het venster Server Manager verschijnt.Selecteer in het gebied Corporate Server de optie TACACS+ in het vervolgkeuzemenu Huidige serverlijst.Op dit zelfde gebied, ga het IP adres, het gedeelde geheim, en het authentificatiehavenaantal van de TACACS+ server in.Klik op Apply (Toepassen).Hierna volgt een voorbeeld:

Cisco 105 Series AP - Security	- Server Manager - Microsoft	Internet Exp	lorer provided by Cisco Sys	stems, Inc.	X
Ble Edit Yew Pavorites	Iools Help				100 M
4=8ack + 🔿 - 🎱 🛃 🚮	QSearch 🕞Favorites 🤿	teda 🎯	👌 🥥 🖾 🕑 🤪 📖		
Address http://10.77.244.194/	ap_sec_network-security_a.shtml#	CorpServers			● 🖓 Go Uniks 🏁
Cited Street	1000000				
يتطالع بطالعي	Cisco	Airon	et 1240AG Seri	es Access Point	10 -
HOME	SERVER MANAGER	1	GLOBAL PROPERTIES		
EXPRESS SET-UP	Hostname ap				ap uptime is 2 hours, 53 minutes
EXPRESS SECURITY					
ASSOCIATION +	Security: Server Manager				
NETWORK +	Backers DADRIE Corres				
INTERFACES	Backup NADIUS Server				
Admin Access	Backup RADIUS Server:			(Hostname or IP Address)	
Encryption Manager	Charad Carat				
SSID Manager	Shared Secret:				
Server Manager					Apply Delete Cancel
AP Authentication	Comorate Sensers				
Local RADIUS Server	Corporate Servers				
Advanced Security	Current Server List				
SERVICES +	TACACS.				
WRELESS SERVICES +		Server		172.16.1.1	(Hostname or IP Address)
EVENTLOG +	(NEW) 172.16.1.1		-		e lossing to a resolution
		Shared	Secret:		
	Delete	Authen	tication Port (optional):	49 (0-65536)	
		Account	ting Part (ontional)	DISARLED O COSTO	
		- Account	and i air fabranaú:	(p.00030)	
					Apply Cancel
8)					Triternet

Opmerking: standaard gebruikt TACACS+ TCP poort 49.**Opmerking:** De gedeelde geheime sleutel die u op ACS vormt en AP moet overeenkomen.

 Kies Standaardserverprioriteiten > Admin-verificatie (TACACS+), selecteer in het vervolgkeuzemenu Prioriteit 1 het IP-adres van de TACACS+ server dat u hebt ingesteld en klik op Toepassen.Hierna volgt een voorbeeld:

1	Cisco 105 Series AP - Security	- Server Manager - Microsoft	Internet Explorer provided by Cisco Sy	stems, Inc.			- 0 >	×
J	Ele Edit Yew Favorites	Toola Rep					10	
J	4=8ack = -> -> 🙆 🔁 🖨	GSearch 🖃 Favorites 🎯	Aeda 🎯 🛂 🗃 🗃 🗃 🏐 👯					
J	Address 🔊 http://10.77.244.194/	ap_sec_network-security_a.shtml#	CorpServers		<u>×</u>	60	Links ³	*
		Delete	Authentication Part (actional):	19 00000				
Π			Paarenaeadon Port (opnona).	(00000)				
Π			Accounting Port (optional):	(0-65536)			.	
Π					Apply	Cancel		
		Default Server Priorities						
Π		EAP Authentication	MAC Authentic	ation	Accounting			
Π		Priority 1: NONE > .	Priority 1: KNC	ONE > ·	Priority 1: NONE > •			
Π		Priority 2 (NONE)	Priority 2: KNC	DNE > ¥	Priority 2: (NONE)			
		Priority 3: (NONE)	Priority 3: < NC	DNE > ×	Priority 3: NONE > .			
Π		Admin Authentication (R	ADIUS) Admin Authent	ication (TACACS+)				
Π		Priority 1: NONE > .	Priority 1: 172	16.1.1				
Π		Priority 2: (NONE)	Priority 2: < NC	ONE > ·				
		Priority 3: NONE > .	Priority 3: KNC	ONE > ·				
Π								
					Apply	Cancel		
Π							-	
Ľ								
							- 1	
	Close Wr	ndew			Copyright (r) 1992-2006 by Cisco	Systems,	Inc.	
					Diritor	het	_	Ĩ

3. Kies Security > Admin Access en, voor beheerder die is gecertificeerd met:, kies alleen de verificatieserver en klik op Toepassen.Deze selectie waarborgt dat gebruikers die proberen in te loggen op AP geauthentiseerd worden door een authenticatieserver.Hierna volgt een voorbeeld:



Dit is de CLI-configuratie voor het configuratievoorbeeld:

AccessPoint
AccessPoint# show running-config
Querrant and firmunation of 2525 but of
Current Configuration : 2535 bytes
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
1
hostname AccessPoint
1
ip subnet-zero
aaa new-model
<i>! Enable AAA.</i> ! ! aaa group server radius rad_eap !
aaa group server radius rad_mac ! aaa group server
radius rad_acct ! aaa group server radius rad_admin
cache expiry 1 cache authorization profile admin_cache
cache authentication profile admin_cache ! aaa group
server tacacs+ tac_admin
! Configure the server group tac_admin. server
172.16.1.1
! Add the TACACS+ server 172.16.1.1 to the server
group. cache expiry i

```
Set the expiration time for the local cache as 24
hours. cache authorization profile admin_cache
cache authentication profile admin_cache
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default group tac_admin
!--- Define the AAA login authentication method list to
use the TACACS+ server. aaa authentication login
eap_methods group rad_eap aaa authentication login
mac_methods local aaa authorization exec default group
tac_admin
!--- Use TACACS+ for privileged EXEC access
authorization !--- if authentication was performed with
use of TACACS+. aaa accounting network acct_methods
start-stop group rad_acct aaa cache profile admin_cache
all ! aaa session-id common ! ! username Cisco password
7 00271A150754 ! bridge irb ! ! interface Dot11Radio0 no
ip address no ip route-cache shutdown speed basic-1.0
basic-2.0 basic-5.5 basic-11.0 station-role root bridge-
group 1 bridge-group 1 subscriber-loop-control bridge-
group 1 block-unknown-source no bridge-group 1 source-
learning no bridge-group 1 unicast-flooding bridge-group
1 spanning-disabled ! interface Dot11Radio1 no ip
address no ip route-cache shutdown speed station-role
root bridge-group 1 bridge-group 1 subscriber-loop-
control bridge-group 1 block-unknown-source no bridge-
group 1 source-learning no bridge-group 1 unicast-
flooding bridge-group 1 spanning-disabled ! interface
FastEthernet0 no ip address no ip route-cache duplex
auto speed auto bridge-group 1 no bridge-group 1 source-
learning bridge-group 1 spanning-disabled ! interface
BVI1 ip address 172.16.1.30 255.255.0.0 no ip route-
cache ! ip http server ip http authentication aaa
!--- Specify the authentication method of HTTP users as
AAA. no ip http secure-server ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/ea ip radius source-interface BVI1 ! tacacs-server
host 172.16.1.1 port 49 key 7 13200F13061C082F tacacs-
server directed-request radius-server attribute 32
include-in-access-req format %h radius-server vsa send
accounting ! control-plane ! bridge 1 route ip ! ! !
line con 0 transport preferred all transport output all
line vty 0 4 transport preferred all transport input all
transport output all line vty 5 15 transport preferred
all transport input all transport output all ! end
```

Opmerking: U moet beschikken over Cisco IOS-softwarerelease 12.3(7)JA of hoger om alle opdrachten in deze configuratie correct te laten werken. Een eerdere Cisco IOS-softwarerelease heeft mogelijk niet al deze opdrachten beschikbaar.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het <u>Uitvoer Tolk</u> (<u>uitsluitend geregistreerde</u> klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken. Probeer om de configuratie te verifiëren aan AP met gebruik van de GUI of de CLI in te loggen. Wanneer u toegang tot AP probeert te krijgen, leidt AP u tot een gebruikersnaam en een wachtwoord.

Enter Netv	work Passwor	d ?×						
? >	 Please type your user name and password. 							
<u>ا</u> ل	Site:	172.16.1.30						
	Realm	level_1_access						
	User Name	User1						
	Password	****						
Save this password in your password list								
		OK Cancel						

Wanneer u de gebruikersreferenties verstrekt, stuurt AP de geloofsbrieven naar de server TACACS+ door. De TACACS+ server bevestigt de geloofsbrieven op basis van de informatie die in zijn databank beschikbaar is en verleent toegang tot AP na succesvolle authenticatie. U kunt **Rapporten en Activiteit > Gepasseerde Verificatie** kiezen op de ACS en het Geautomatiseerde Verificatierapport gebruiken om voor deze gebruiker te controleren op succesvolle verificatie. Hierna volgt een voorbeeld:

Select								
Refresh	Down	load						
Passed Authentications active.csv								
Date	<u>Time</u>	Message- Type	User- Name	Group- Name	Caller-ID	NAS- Port	<u>NAS-IP-</u> <u>Address</u>	
05/10/2006	14:57:01	Authen OK	User1	AdminUsers	172.16.1.1	tty1	172.16.1.30	

U kunt de opdracht **Tacacs** ook gebruiken om de juiste configuratie van de TACACS+ server te controleren. Hierna volgt een voorbeeld:

AccessPoint#show tacacs

Tacacs+	Server :	172.16.1.1/49
	Socket opens:	348
	Socket closes:	348
	Socket aborts:	0
	Socket errors:	0
	Socket Timeouts:	0
Faile	ed Connect Attempts:	0

Total	Packets	Sent:	525
Total	Packets	Recv:	525

Verificatie voor ACS 5.2

U kunt de mislukte/gepasseerde pogingen voor inlogaanmeldingsgegevens van ACS 5.2 verifiëren:

- 1. Klik op **Monitoring and Reports > Start Monitoring and Report Viewer**.Er wordt een nieuwe pop geopend met het Dashboard.
- 2. Klik op Authenticaties-TACACS-Vandaag. Dit toont de details van mislukte/doorgegeven pogingen.

Problemen oplossen

U kunt deze debug-opdrachten op het AP gebruiken om problemen met uw configuratie op te lossen:

Opmerking: Raadpleeg <u>Belangrijke informatie over debug Commands</u> voordat u **debug**opdrachten gebruikt.

 debug tacacs gebeurtenissen—Deze opdracht toont de opeenvolging van gebeurtenissen die tijdens TACACS authenticatie plaatsvinden. Hier is een voorbeeld van de uitvoer van deze opdracht:

```
*Mar 1 00:51:21.113: TPLUS: Queuing AAA Authentication request 0 for
processing
*Mar 1 00:51:21.113: TPLUS: processing authentication start request id 0
*Mar 1 00:51:21.113: TPLUS: Authentication start packet created for 0(User1)
     1 00:51:21.114: TPLUS: Using server 172.16.1.1
*Mar
*Mar 1 00:51:21.115: TPLUS(0000000)/0/NB_WAIT/C6DC40: Started 5 sec timeout
*Mar 1 00:51:21.116: TPLUS(0000000)/0/NB_WAIT: socket event 2
*Mar 1 00:51:21.116: TPLUS(0000000)/0/NB_WAIT: wrote entire 25 bytes request
*Mar 1 00:51:21.116: TPLUS(0000000)/0/READ: socket event 1
*Mar 1 00:51:21.117: TPLUS(0000000)/0/READ: Would block while reading
*Mar 1 00:51:21.120: TPLUS(0000000)/0/READ: socket event 1
*Mar 1 00:51:21.120: TPLUS(0000000)/0/READ: read entire 12 header bytes (expect
16 bytes data)
*Mar 1 00:51:21.120: TPLUS(0000000)/0/READ: socket event 1
*Mar 1 00:51:21.120: TPLUS(00000000)/0/READ: read entire 28 bytes response
*Mar 1 00:51:21.121: TPLUS(0000000)/0/C6DC40: Processing the reply packet
*Mar 1 00:51:21.121: TPLUS: Received authen response status GET PASSWORD (8)
*Mar 1 00:51:21.121: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar 1 00:51:21.121: TPLUS: processing authentication continue request id 0
     1 00:51:21.122: TPLUS: Authentication continue packet generated for 0
*Mar
*Mar 1 00:51:21.122: TPLUS(0000000)/0/WRITE/C6DC40: Started 5 sec timeout
*Mar 1 00:51:21.122: TPLUS(0000000)/0/WRITE: wrote entire 22 bytes request
*Mar 1 00:51:21.178: TPLUS(0000000)/0/READ: socket event 1
*Mar 1 00:51:21.178: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect
6 bytes data)
*Mar 1 00:51:21.178: TPLUS(0000000)/0/READ: socket event 1
     1 00:51:21.178: TPLUS(0000000)/0/READ: read entire 18 bytes response
*Mar
*Mar
     1 00:51:21.179: TPLUS(0000000)/0/C6DC40: Processing the reply packet
*Mar 1 00:51:21.179: TPLUS: Received authen response status PASS (2)
```

• **debug ip http authenticatie**-gebruik deze opdracht om HTTP authenticatieproblemen op te lossen. De opdracht toont de authenticatiemethode die de router heeft geprobeerd en de

authenticatie-specifieke statusberichten.

• debug van verificatie—Deze opdracht geeft informatie weer over AAA TACACS+ verificatie.

Als de gebruiker een gebruikersnaam invoert die niet op de TACACS+ server bestaat, mislukt de verificatie. Hier is **debug tacacs authenticatie** opdrachtoutput voor een mislukte authenticatie:

```
*Mar 1 00:07:26.624: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar 1 00:07:26.624: TPLUS: processing authentication start request id 0
*Mar 1 00:07:26.624: TPLUS: Authentication start packet created for 0(User3)
*Mar 1 00:07:26.624: TPLUS: Using server 172.16.1.1
     1 00:07:26.625: TPLUS(0000000)/0/NB_WAIT/A88784: Started 5 sec timeout
*Mar
*Mar 1 00:07:26.626: TPLUS(0000000)/0/NB_WAIT: socket event 2
*Mar 1 00:07:26.626: TPLUS(0000000)/0/NB_WAIT: wrote entire 25 bytes request
*Mar 1 00:07:26.627: TPLUS(0000000)/0/READ: socket event 1
*Mar 1 00:07:26.627: TPLUS(0000000)/0/READ: Would block while reading
*Mar 1 00:07:26.631: TPLUS(0000000)/0/READ: socket event 1
     1 00:07:26.632: TPLUS(0000000)/0/READ: read entire 12 header bytes (expect 16
*Mar
bytes data)
*Mar 1 00:07:26.632: TPLUS(0000000)/0/READ: socket event 1
*Mar 1 00:07:26.632: TPLUS(00000000)/0/READ: read entire 28 bytes response
*Mar 1 00:07:26.632: TPLUS(0000000)/0/A88784: Processing the reply packet
*Mar 1 00:07:26.632: TPLUS: Received authen response status GET_PASSWORD (8)
*Mar 1 00:07:26.632: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar 1 00:07:26.633: TPLUS: processing authentication continue request id 0
*Mar
     1 00:07:26.633: TPLUS: Authentication continue packet generated for 0
*Mar 1 00:07:26.634: TPLUS(0000000)/0/WRITE/A88784: Started 5 sec timeout
*Mar 1 00:07:26.634: TPLUS(0000000)/0/WRITE: wrote entire 22 bytes request
*Mar 1 00:07:26.688: TPLUS(0000000)/0/READ: socket event 1
*Mar 1 00:07:26.688: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 6
bytes data)
*Mar 1 00:07:26.689: TPLUS(0000000)/0/READ: socket event 1
*Mar
     1 00:07:26.689: TPLUS(0000000)/0/READ: read entire 18 bytes response
*Mar 1 00:07:26.689: TPLUS(0000000)/0/A88784: Processing the reply packet
*Mar 1 00:07:26.689: TPLUS: Received authen response status FAIL (3)
```

U kunt kiezen **Rapporten en Activiteit > Verstoring van verificatie** om de mislukte verificatiepoging op de ACS te zien. Hierna volgt een voorbeeld:

Date 🖊	<u>Time</u>	<u>Message-</u> <u>Type</u>	<u>User-</u> Name	<u>Group-</u> <u>Name</u>	Caller- ID	<u>Authen-</u> Failure-Code	<u>Author-</u> <u>Failure-</u> <u>Code</u>	Author- Data	<u>NAS-</u> <u>Port</u>
05/17/2006	19:40:14	Authen failed	User3			CS user unknown			

Als u een Cisco IOS-softwarerelease op de AP gebruikt die eerder is dan Cisco IOSsoftwarerelease 12.3(7)JA, kunt u elke keer dat u probeert in te loggen op de AP met gebruik van HTTP een bug raken. Cisco bug-ID is <u>CSCeb52431</u> (alleen <u>geregistreerde</u> klanten).

De implementatie van Cisco IOS HTTP/AAA-software vereist de onafhankelijke authenticatie van elke afzonderlijke HTTP-verbinding. De draadloze Cisco IOS-software GUI heeft betrekking op de referentie van vele tientallen afzonderlijke bestanden binnen één webpagina (bijvoorbeeld Javascript en GIF). Dus als u één pagina in de draadloze Cisco IOS-softwarerelease laadt, kunnen tientallen afzonderlijke verificatie-/autorisatieverzoeken op de AAA-server verschijnen.

Gebruik voor HTTP-verificatie RADIUS of lokale verificatie. De RADIUS-server is nog steeds onderworpen aan de meerdere verificatieverzoeken. Maar RADIUS is schaalbaarder dan TACACS+ en zal dus waarschijnlijk een minder negatieve impact hebben op de prestaties.

Als u TACACS+ moet gebruiken en u een Cisco ACS hebt, gebruik het sleutelwoord **van één verbinding** met de **tacacs-server** opdracht. Gebruik van dit sleutelwoord met het commando spaart de ACS het grootste deel van de TCP verbinding instelling/uitloopoverhead en zal waarschijnlijk de lading op de server tot op zekere hoogte verminderen.

Voor Cisco IOS-softwarereleases 12.3(7) JA en hoger op de AP bevat de software een tijdelijke oplossing. De rest van dit deel beschrijft de oplossing.

Gebruik de AAA authenticatiescachefunctie om de informatie in te delen die de TACACS+ server teruggeeft. Met de authenticatiecache en de profielfunctie kan AP de authenticatie/autorisatieresponsen voor een gebruiker in het geheugen zetten zodat latere echtheids-/autorisatieverzoeken niet naar de AAA-server hoeven te worden verstuurd. Gebruik deze opdrachten om deze optie met de CLI te activeren:

cache expiry cache authorization profile cache authentication profile aaa cache profile

Raadpleeg voor meer informatie over deze functie en de opdrachten het <u>gedeelte Verificatie-</u> <u>cache en profiel van het access point configureren</u>.

Kies **Security > Admin Access** en controleer het vakje **Caching** van **verificatieserver** inschakelen om deze optie in de GUI te schakelen. Omdat dit document Cisco IOS-softwarerelease 12.3(7)JA gebruikt, gebruikt het document de tijdelijke oplossing zoals de <u>configuraties</u> illustreren.

Gerelateerde informatie

- RADIUS- en TACACS+ servers configureren
- Opmerking over het veld: IOS access point bommen voor TACACS+ server met aanvragen
- EAP-verificatie met RADIUS-server
- Ondersteuning voor wireless producten
- Technische ondersteuning en documentatie Cisco Systems