RSA SecureID Klaar met draadloze LANcontrollers en Cisco Secure ACSconfiguratievoorbeeld

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Achtergrondinformatie Configureren Agent-hostconfiguratie Cisco Secure ACS als RADIUS-server gebruiken RSA-verificatie Manager gebruiken 6.1 RADIUS-server Configuratie van verificatieagent Cisco ACS configureren Configuratie Cisco draadloze LAN-controller voor 802.1x 802.11 clientconfiguratie voor draadloos LAN Bekende problemen Gerelateerde informatie

Inleiding

Dit document legt uit hoe u Cisco Lichtgewicht Access Point Protocol (LWAPP)-compatibele AP's en draadloze LAN-controllers (WLC's) kunt instellen en configureren, evenals Cisco Secure Access Control Server (ACS) die in een RSA Secure Security ID-omgeving wordt gebruikt. RSA SecurID-specifieke implementatiegids zijn te vinden op <u>www.rsasecured.com</u>.

Voorwaarden

Vereisten

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

- Kennis van WLC's en hoe u de WLC-fundamentele parameters kunt configureren.
- Kennis over het configureren van het profiel van Cisco draadloze client met behulp van Aironet Desktop Utility (ADU).
- beschikken over functionele kennis van Cisco Secure ACS.

- beschikken over basiskennis van LWAPP.
- U hebt basiskennis van de services van Microsoft Windows Active Directory (AD), evenals van domeincontrollers en DNS-concepten. Opmerking: Voordat u deze configuratie probeert, moet u ervoor zorgen dat de ACS- en de RSA Verification Manager-server in hetzelfde domein zijn en dat hun systeemklok precies gesynchroniseerd is. Als u Microsoft Windows AD Services gebruikt, raadpleeg de Microsoft documentatie om de ACS- en RSA Manager-server in hetzelfde domein te configureren. Raadpleeg <u>Actieve Map- en Windows</u> <u>Gebruikersdatabase instellen</u> voor relevante informatie.

Gebruikte componenten

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

- RSA-verificatie Manager 6.1
- RSA-verificatie Agent 6.1 voor Microsoft Windows
- Cisco Secure ACS 4.0(1) gebouwd 27**Opmerking:** De RADIUS-server die hieronder valt, kan in de plaats van Cisco ACS worden gebruikt. Zie de RADIUS-documentatie die bij de RSA-verificatiebeheer is meegeleverd over de manier waarop u de server kunt configureren.
- Cisco WLC's en lichtgewicht access points voor release 4.0 (versie 4.0.15.0)

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 de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

Het RSA SecurID-systeem is een tweeledige gebruikersverificatieoplossing. In combinatie met RSA Verificatiebeheer en een RSA Verificatieagent, vereist de authenticator RSA SecurID van gebruikers om zichzelf te identificeren met een twee-factor authenticatiemechanisme.

Eén is de RSA SecurID code, een willekeurig aantal dat elke 60 seconden gegenereerd wordt op het RSA SecureID authenticator apparaat. Het andere is het Persoonsidentificatienummer (PIN).

RSA SecureID-authenticators zijn net zo eenvoudig te gebruiken als het invoeren van een wachtwoord. Aan elke eindgebruiker wordt een RSA SecurID-authenticator toegewezen die een eenmalige gebruikerscode genereert. Wanneer u inlogt, voert de gebruiker dit nummer in en er wordt een geheime PIN ingevoerd die echt gemaakt is. Als extra voordeel zijn RSA SecurID hardwarepenningen doorgaans voorgeprogrammeerd om na ontvangst volledig functioneel te zijn.

Deze flitsdemonstratie legt uit hoe een RSA securityID authenticator apparaat gebruikt: <u>RSA</u> <u>demo</u>.

Via het programma RSA SecureID Ready ondersteunen Cisco WLCs en Cisco Secure ACSservers RSA SecureID-verificatie direct uit het vak. De software van RSA Verificator intercepteert toegangsverzoeken, lokaal of ver, van gebruikers (of groepen gebruikers) en leidt hen naar het RSA Verificatiebeheer programma voor authenticatie.

RSA-verificatiebeheersoftware is de beheercomponent van de RSA SecurID-oplossing. Het wordt gebruikt om verificatieverzoeken te verifiëren en centraal het authenticatiebeleid voor ondernemingsnetwerken te beheren. Het werkt in combinatie met RSA Security ID-authenticators en software van RSA-verificatieagent.

In dit document wordt een Cisco ACS-server gebruikt als RSA Verificatieagent door de agentensoftware op het te installeren. WLC is de Network Access Server (NAS) (AAA-client) die op zijn beurt de client-authenticaties naar het ACS doorstuurt. Het document demonstreert de concepten en instellingen door middel van PEAP-clientverificatie (Protected Extensible Authentication Protocol).

Raadpleeg voor meer informatie over PEAP-verificatie het <u>Cisco Protected Extensible</u> <u>Authentication Protocol</u>.

Configureren

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

Dit document gebruikt deze configuraties:

- <u>Agent-hostconfiguratie</u>
- Configuratie van verificatieagent

Agent-hostconfiguratie

Cisco Secure ACS als RADIUS-server gebruiken

Om de communicatie tussen de Cisco Secure ACS en de RSA Verificatiebeheer / RSA SecureIDapplicatie te vergemakkelijken, moet een Agent Host Record worden toegevoegd aan de RSA VerificatieManager-database. Het Agent Host Record identificeert Cisco Secure ACS binnen zijn database en bevat informatie over communicatie en encryptie.

Om het Agent Host Record te maken, hebt u deze informatie nodig:

Hostnaam van de Cisco ACS-server

• IP-adressen voor alle netwerkinterfaces van de Cisco ACS-server Voer de volgende stappen uit:

- 1. Open de Host Mode-toepassing van RSA-verificatie Manager.
- 2. Selecteer Agent Host > Add Agent Host.



U ziet dit

nster:	
t Agent Host	2
Name: SB-ACS	hostname of the ACS Server
Network address: 192.168.30.18	
Site:	Select
Agent type: Communication Set Single-Transaction Net OS Agent	rver A Comm Server
Encryption Type: C SDI @ DES	
☑ Node Secret Create	ed
○ Open to All Locally	Known Users
E Search Other Reals	ns for Unknown Users
🗖 Requires Name Lo	ck
🔽 Enable Offline Auth	entication
Enable Windows P	assword lategration
🗖 Create Verifiable A	uthentications
Group Activations	User Activations
Secondary Nodes	Delete Agent Host
Edit Agent Host Extension Data	Configure RADIUS Connection
Assign Acting Servers	Create Node Secret File

- 3. Voer de juiste informatie in voor de Cisco ACS-servernaam en -netwerkadres. Kies **NetOS** voor het type Agent en controleer het selectieteken voor **Openen voor Alle lokaal bekende gebruikers**.
- 4. Klik op OK.

RSA-verificatie Manager gebruiken 6.1 RADIUS-server

Om de communicatie tussen de Cisco WLC en de RSA Verificatiebeheer te vergemakkelijken, moet een Agent Host Record worden toegevoegd aan de RSA Verification Manager-database en de RADIUS-serverdatabase. Het Agent Host Record identificeert de Cisco WLC in zijn database en bevat informatie over communicatie en encryptie.

Om het Agent Host Record te maken, hebt u deze informatie nodig:

- Hostnaam van WLC
- IP-adressen van beheer van de WLC
- RADIUS-geheim dat moet overeenkomen met het RADIUS-geheim op Cisco WLC

Wanneer het toevoegen van het Agent Host Record, wordt de rol van de WLC gevormd als een Communicatieserver. Deze instelling wordt gebruikt door de RSA Authentication Manager om te bepalen hoe de communicatie met de WLC zal plaatsvinden.

Opmerking: Hostnamen binnen de RSA Verificatiebeheer / RSA SecureID-applicatie moeten tot geldige IP-adressen op het lokale netwerk worden opgelost.

Voer de volgende stappen uit:

- 1. Open de Host Mode-toepassing van RSA-verificatie Manager.
- 2. Selecteer Agent Host > Add Agent



Name: 192.168.10.102	Point to WLC when using RSA's RADIUS
Network address: 192.168.10.102	Server
Site:	Se
Agent type: UNIX Agent Communication St Single-Transaction	erver a Comm Server
Encryption Type: C SDI @ DES	
Node Secret Creat Open to All Locally	y Known Users
Search Other Real	Ims for Unknown Users
🔲 Requires Name L	ock
P Enable Offline Aut	hentication
Enable Windows I	Password Integration
Create Verifiable /	Authentications
Group Activations	User Activations
Secondary Nodes	Delete Agent Host
Edit Agent Host Extension Data	Contigure RADIUS Connection
	County Made Count File

- 3. Voer de juiste informatie in voor de WLC hostname (een oplosbare FQDN, indien nodig) en het netwerkadres. Kies **Communicatieserver** voor Agent-type en controleer het selectieteken voor **Openen voor Alle lokaal bekende gebruikers**.
- 4. Klik op OK.
- 5. Selecteer in het menu de optie RADIUS > RADIUS-server
 - beheren.



Er wordt een nieuw venster geopend.

6. Selecteer in dit venster de optie **RADIUS-clients** en klik vervolgens op **Toevoegen**.



7. Voer de juiste informatie in voor Cisco WLC. Het gedeelde geheim moet overeenkomen met het gedeelde geheim dat op de Cisco WLC is

gedefinieerd. Add RADIUS Client			×
<u>N</u> ame:	OSCOARONET	Any RADIUS Client	0
Description:			
P Address:	10.100.10.11		
Shared secret:	12345678	🔽 Unmask	
Make/model:	- Standard Radius -	<u>W</u> eb Info	
Advanced			
Use different s	nared secret for Accounting		
Assume down	if no keepalive packets after	seconds	
L	OK Cancel		

8. Klik op OK.

Configuratie van verificatieagent

Deze tabel vertegenwoordigt de functionaliteit van de RSA-verificatieagent van ACS:

Native RSA SecurID Authentication, RADIUS, Both
5.0.3
Yes
Full Replica Support
N/A
'None stored'
Communication Server
Designated Users, All Users, Default Method
No
No
No

Opmerking: Zie de RADIUS-documentatie die bij de RSA-verificatiebeheer is meegeleverd, over de manier waarop u de RADIUS-server kunt configureren als deze de RADIUS-server is die gebruikt zal worden.

Cisco ACS configureren

RSA SecureID-verificatie activeren

Cisco Secure ACS ondersteunt RSA Security ID-verificatie van gebruikers. Voltooi deze stappen om Cisco Secure ACS te configureren om gebruikers te authentiseren met Verificatiebeheer 6.1:

- 1. Installeer de RSA Verificatie Agent 5.6 of hoger voor Windows op hetzelfde systeem als de Cisco Secure ACS-server.
- 2. Controleer de connectiviteit door de testopdracht van de Verificatieagent uit te voeren.
- 3. Kopieer het bestand aceclent.dll van de RSA server c:\Program Files\RSA Security\RSA Authentication Manager\prog folder naar de c:\WINNT\system32-map van de ACS server.
- 4. Klik in de navigatiebalk op **Externe gebruikersdatabase**. Klik vervolgens op **Database Configuration** in de externe database pagina.



5. Klik in de pagina Configuratie externe gebruikersdatabase op **RSA SecureID Token**



6. Klik op Nieuwe configuratie

maken.



7. Voer een naam in en klik vervolgens op

Inzenden.	
CiscoSecure ACS - Microsoft Internet Explorer	_(_ (_)
Bie Edit Yem Ferrarites Incle Help	
🔇 Badi. + 🕥 - 💽 😰 🐔 🔑 Search 🤌 Favorites 🐠 Media 🛷 🔝 💭 + 😓	
Address 🕘 http://127.0.0.1:3342/	💌 🛃 Go 🛛 Links 🖞
Google - 💽 🍪 Search Web 🔹 🤯 🖓 Blocked 🗐 Autoriti 🛃 Options	8
Circle System External User Databases	
Image: Started Fredition Image: St	 <u>Network Admission Control</u> <u>Windows Database</u> <u>Novell NDS</u> <u>Generic LDAP</u> <u>External ODBC Database</u> <u>LEAP Prexy RADIUS Server</u> <u>Token Card Server Support</u> <u>RADIUS Token Server</u> <u>RSA SerurIDToken Server</u>
Administration Defense User Defense User Defense Administration Possene Administration	Network Admission Control Click to configure Network Admission Control (NAC) databases, external policies, local policies, and rules. Cisco Secure ACS uses NAC databases to process posture validation requests. [Back to Top] Windows Database Click to configure Windows SAM and Active Directory databases with which Cisco Secure ACS can authenticate users.
Applet startStop started	Local intranet

8. Klik op

Configureren.	
Ele Edit View Envotes Tools Help	2 (BL.
🔾 Back + 🔿 + 🖻 🕤 🦨 Search 🛞 Favorites 🖓 Nedia 🎱 🔗 + 🚴 🕅 + 🔛	
Address (a) https://127.0.0.1:3042/	💌 🛃 Go 🛛 Linis *
Google - 💽 🍘 Search Web - 🚳 🗗 O blocked 🗐 Autorit 🔛 Option	ns 🥒
trize Sweens External User Databases	
Edit Edit Edit Edit Extract during	Heip • Nictswork Admission Control • Windows Database • Novell NDS • Generic LDAP • External ODBC Database • LEAP Proxy RADIUS Server • Token Card Server Support • RADIUS Token Server • RADIUS Token Server • REA SecuriDToken Server • Risk SecuriDToken Server • Retwork Admission Control Click to configure Network Admission Control (NAC) databases, external policies, local policies, and rales. Clace Secure ACS uses NAC databases to process posture validation requests. [Back to Top] Windows Database Click to configure Windows SAM and Active Directory databases with which Cisco Secure ACS can authenticate users

Cisco Secure ACS geeft de naam van de token server en het pad naar de authenticator DLL weer. Deze informatie bevestigt dat Cisco Secure ACS contact kan opnemen met de RSA-verificatieagent. U kunt de externe gebruikersdatabase van RSA SecurID aan uw Onbekend gebruikersbeleid toevoegen of specifieke gebruikersrekeningen toewijzen om deze database voor verificatie te



RSA SecureID-verificatie aan uw onbekend gebruikersbeleid toevoegen/configureren

Voer de volgende stappen uit:

1. Klik in de navigatiebalk ACS op **Externe gebruikersdatabase > Onbekend** gebruikersbeleid.



 Selecteer in de pagina Onbekend gebruikersbeleid de volgende externe gebruikersdatabases controleren, RSA SecureID Token Server markeren en naar het geselecteerde gegevensbestand verplaatsen. Klik vervolgens op Inzenden.

Sa = 10 - 🕥 🗊	🕼 🕼 🕼 🕼 🖓 🖏 🖓 🖷 🖄 📗 🔤 👘 Address 💌 http://pd0414742	ander-2.Non 💌 🙀 – 🖉 🛪
Cinco Storens	External User Databases	×
at the set the	Edit	Holp
C Starte Rolling	Configure Unknown User Policy 👔 Use this table to define how users will be handled when they are not found in the CistoSecure Database.	 Unknown User Policy Fail the Attempt Check the following external users databases
Betwork Diefigeratus	C Palitic attempt	Unknown User Policy
Listeriar Cartiguration	Check the following esternal user databases	Use this window to define how to handle usernames not found in the Circo Secure ACS database.
Atmitistration Cost rel		Fail the attempt
Big External licer Setatures		If you do not want Cisco Secure ACS to try authenticating users who do not exist in its internal database (unknown users), select this option
Partine Children	××	[Back to Top]
		Check the following external user databases
	These for Holes	If you want Cisco Secure ACS to use specific external user dathases to authenticate unknown users, select this option. You can choose the databases and the order in which Caso Secure ACS uses them to up to authenticate unknown users.
		For each database that Cisco Secure ACS should use to try to authenticate unknown overs, relect the database name in the External Databases list and olick the right arrow button to move it to the Selected Databases list.
	Submit Concel	 The order of databases on the Selected Databases list determines the sequence of databases that Cisco Secure

RSA SecureID-verificatie toevoegen/configureren voor specifieke gebruikersrekeningen

Voer de volgende stappen uit:

- 1. Klik op **Gebruiker Setup** vanuit de hoofdACS Admin GUI. Voer de gebruikersnaam in en klik op **Toevoegen** (of selecteer een bestaande gebruiker die u wilt wijzigen).
- 2. Selecteer onder User Setup > Password-verificatie de optie **RSA SecureID Token Server**. Klik vervolgens op

Cisco Syst	User Setup
الأسمينا الأنب	Edit
User User	User: sbrsa
B-tup	
Shared Pro Component	ofik Its
Natwork Configura	ation Supplementary User Info 💡
System Configure	ation Real Name
Interface Configur	Description
Administr Control	ration
Database	User Setup
esseni Posture Validatio	Password Authentication:
	RSA SecurID Token Server
Profiles	CiscoSecure PAP (Also used for CHAP/MS-
S Reparts	and Password
- A I Online	Confirm
Document	tation 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
anden	Submit Delete Cancel

Voeg een RADIUS-client in Cisco ACS toe

De installatie van de Cisco ACS-server heeft de IP-adressen van de WLC nodig om te dienen als een NAS voor het verzenden van client-PEAP-authenticaties naar de ACS.

Voer de volgende stappen uit:

 Onder Network Configuration voert u de AAA-client voor de WLC in die wordt gebruikt. Voer de "gedeelde geheime" toets in (gebruikelijk van WLC) die tussen de AAA-client en ACS wordt gebruikt. Selecteer Verifiëren met > RADIUS (Cisco Airesponder) voor deze AAAclient. Klik vervolgens op Inzenden +

CIECO SYSTEMS	Network Configuration
and transfilling.	Edit
User Sotup	
Breup Setup	AAA Client Setup For
Shared Profile Components	WLC4404
Nat work Configuration	AAA Client IP 192.168.10.102
Configuration	Address
Configuration	Key RSA
Administration Centrol	Authenticate RADIUS (Cisco Airespace)
Detabases	Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
Normal Posture Validation	Log Update/Watchdog Packets from this AAA Client
Profiles	Log RADIUS Tunneling Packets from this AAA Client
S Reports and Activity	Replace RADIUS Port info with Usemame from this AAA Client
Documentation	
	Submit Submit + Apply Delete Delete + Apply Cancel

Toepassen.

- 2. Aanvragen en installeren van een servercertificaat van een bekende, vertrouwde certificeringsinstantie zoals de RSA Keon certificaatinstantie.Raadpleeg voor meer informatie over dit proces de documentatie die schepen met Cisco ACS. Als u RSA certificaatManager gebruikt, kunt u de RSA Keon Aironet implementatiegids voor extra hulp bekijken. U moet deze taak met succes voltooien voordat u verdergaat.**Opmerking:** Ook zelfgetekende certificaten kunnen worden gebruikt. Raadpleeg de Cisco Secure ACS-documentatie over het gebruik van deze bestanden.
- 3. Onder System Configuration > Global Authentication Setup, vinkt u het selectieteken aan op Toestaan PEAP-

verificatie.



Configuratie Cisco draadloze LAN-controller voor 802.1x

Voer de volgende stappen uit:

- 1. Sluit aan op de opdrachtregel van de WLC-interface om de controller te configureren zodat deze kan worden geconfigureerd om verbinding te maken met de Cisco Secure ACS-server.
- 2. Voer de **configuratie straal in van ip-adres** opdracht van de WLC om een RADIUS-server voor verificatie te configureren.**Opmerking:** Wanneer u test met de RADIUS-server van RSA Verificatiebeheer, voert u het IP-adres in van de RADIUS-server van RSA Verification Manager. Wanneer u met de Cisco ACS server test, voer het IP adres van de Cisco Secure ACS server in.
- 3. Voer het opdracht van de **configuratiestraal** van de WLC in om de UDP poort voor authenticatie te specificeren. poorten 1645 of 1812 zijn standaard actief in zowel de RSAverificatieManager als de Cisco ACS-server.
- 4. Voer het **configuratiestraal geheime** bevel van de **auth in** van de WLC om het gedeelde geheim op de WLC te vormen. Dit moet overeenkomen met het gedeelde geheim dat in de RADIUS-servers voor deze RADIUS-client is gemaakt.
- 5. Voer de **configuratiestraal in om** opdracht van de WLC toe te **staan** om authenticatie toe te staan. Voer desgewenst de **configuratie Straal** in **om** verificatie uit te schakelen. Merk op dat verificatie standaard uitgeschakeld is.
- 6. Selecteer de juiste Layer 2-beveiligingsoptie voor het gewenste WLAN in de WLC-modus.
- 7. Gebruik de opdrachten **Straalauth statistics van de show** en **show Straalsamenvatting** om te controleren of de instellingen van de RADIUS correct zijn geconfigureerd.**Opmerking:** de standaardtimers voor de EAP-aanvraag-uitzending zijn laag en moeten mogelijk worden

aangepast. Dit kan worden gedaan met het **configuratie geavanceerde eap request-timeout** *<seconden>opdracht.* Het zou ook kunnen helpen de time-out van de identiteitsaanvraag aan te passen aan de vereisten. Dit kan worden gedaan **met** het **configuratie geavanceerde eap Identity-request-timeout** *<seconden>opdracht.*

802.11 clientconfiguratie voor draadloos LAN

Voor een gedetailleerde uitleg over de manier waarop u uw draadloze hardware en clientapplicatie kunt configureren raadpleegt u verschillende Cisco-documentatie.

Bekende problemen

Dit zijn een aantal van de bekende problemen met RSA SecureID-verificatie:

- RSA Software Token. De nieuwe pinmodus en de volgende modus worden niet ondersteund bij gebruik van deze vorm van verificatie met XP2. (FIXED als resultaat van ACS-4.0.1-RSA-SW-CSCsc12614-CSCsd41866.zip)
- Als uw ACS-implementatie ouder is of u niet de bovenstaande patch hebt, zal de client niet echt kunnen authenticeren totdat de gebruiker overschakelt van "Enabled;New PIN Mode" naar "Enabled". U kunt dit bereiken door de gebruiker een niet draadloze authenticatie te laten voltooien, of door de "test authenticatie" RSA toepassing te gebruiken.
- Deny 4 cijfers / alfanumerieke PIN's. Als een gebruiker in de modus Nieuwe pen tegen het beleid van de PIN gaat, faalt de authenticatieprocedure en de gebruiker weet niet hoe of waarom. Meestal, als een gebruiker tegen het beleid ingaat, zullen zij een bericht worden verstuurd dat de PIN werd verworpen en opnieuw gevraagd terwijl hij de gebruiker opnieuw toont wat het PN-beleid is (bijvoorbeeld als het PN-beleid 5-7 cijfers is, maar de gebruiker 4 cijfers invoert).

Gerelateerde informatie

- Dynamische VLAN-toewijzing met WLCs op basis van ACS naar actieve Directory Group Mapping Configuration-voorbeeld
- <u>ClientVPN via draadloos LAN met Configuratievoorbeeld van WLC</u>
- Verificatie van configuratievoorbeelden voor draadloze LAN-controllers
- EAP-FAST-verificatie met draadloze LAN-controllers en configuratievoorbeeld voor externe RADIUS-servers
- Draadloze verificatietypen op Vaste ISR via het configuratiemodel van de hedendaagse Standaard
- Draadloze verificatietypen op een vaste ISR-configuratiemodel
- <u>Cisco beschermde uitvoerbaar verificatieprotocol</u>
- EAP-verificatie met RADIUS-server
- <u>Technische ondersteuning en documentatie Cisco Systems</u>