# Esempio di configurazione di RSA SecurID Ready con Wireless LAN Controller e Cisco Secure ACS

## Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Premesse Configurazione Configurazione host agente Uso di Cisco Secure ACS come server RADIUS Utilizzo di RSA Authentication Manager 6.1 RADIUS Server Configurazione agente di autenticazione Configurazione di Cisco ACS Configurazione di Cisco Wireless LAN Controller per 802.1x Configurazione client wireless 802.11 Problemi noti Informazioni correlate

# **Introduzione**

Questo documento spiega come configurare Cisco Lightweight Access Point Protocol (LWAPP) e Wireless LAN Controller (WLC), nonché Cisco Secure Access Control Server (ACS) da utilizzare in un ambiente WLAN autenticato RSA SecurID. Le guide all'implementazione specifiche per RSA SecurID sono disponibili all'indirizzo <u>www.rsasecured.com</u>.

# **Prerequisiti**

## **Requisiti**

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Conoscenza dei WLC e come configurare i parametri base del WLC.
- Informazioni su come configurare il profilo di Cisco Wireless Client con Aironet Desktop Utility (ADU).
- Conoscere le funzionalità di Cisco Secure ACS.

- Conoscere LWAPP.
- Conoscere le nozioni di base sui servizi Active Directory di Microsoft Windows, nonché sui concetti relativi al controller di dominio e al DNS.Nota: prima di provare questa configurazione, verificare che il server ACS e RSA Authentication Manager si trovino nello stesso dominio e che l'orologio di sistema sia esattamente sincronizzato. Se si utilizzano i servizi AD di Microsoft Windows, consultare la documentazione di Microsoft per configurare il server ACS e RSA Manager nello stesso dominio. Per ulteriori informazioni, fare riferimento a Configurazione di Active Directory e del database utenti di Windows.

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- RSA Authentication Manager 6.1
- RSA Authentication Agent 6.1 per Microsoft Windows
- Cisco Secure ACS 4.0(1) Build 27**Nota:** il server RADIUS incluso può essere utilizzato al posto del Cisco ACS. Per informazioni su come configurare il server, vedere la documentazione RADIUS inclusa con RSA Authentication Manager.
- Cisco WLC e Lightweight Access Point per la versione 4.0 (versione 4.0.15.0)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## **Convenzioni**

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

## **Premesse**

Il sistema RSA SecurID è una soluzione di autenticazione utente a due fattori. Utilizzato insieme a RSA Authentication Manager e a un agente di autenticazione RSA, l'autenticatore RSA SecurID richiede agli utenti di identificarsi utilizzando un meccanismo di autenticazione a due fattori.

Uno è il codice RSA SecurID, un numero casuale generato ogni 60 secondi sul dispositivo di autenticazione RSA SecureID. L'altro è il PIN.

Gli autenticatori RSA SecurID sono semplici da utilizzare come l'immissione di una password. A ciascun utente finale viene assegnato un autenticatore RSA SecurID che genera un codice monouso. All'accesso, l'utente immette semplicemente questo numero e un PIN segreto per autenticarsi correttamente. Come ulteriore vantaggio, i token hardware RSA SecurID sono in genere preprogrammati per essere completamente funzionanti alla ricezione.

Questa dimostrazione flash spiega come utilizzare un dispositivo di autenticazione RSA secureID: <u>Demo RSA</u>.

Tramite il programma RSA SecurID Ready, i server Cisco WLC e Cisco Secure ACS supportano

immediatamente l'autenticazione RSA SecurID. Il software RSA Authentication Agent intercetta le richieste di accesso, sia locali che remote, da utenti (o gruppi di utenti) e le indirizza al programma RSA Authentication Manager per l'autenticazione.

Il software RSA Authentication Manager è il componente di gestione della soluzione RSA SecurID. Viene utilizzato per verificare le richieste di autenticazione e amministrare centralmente i criteri di autenticazione per le reti aziendali. Funziona in abbinamento agli autenticatori RSA SecurID e al software RSA Authentication Agent.

In questo documento, viene usato un server Cisco ACS come agente di autenticazione RSA installando il software dell'agente su di esso. Il WLC è il Network Access Server (NAS) (client AAA) che a sua volta inoltra le autenticazioni dei client all'ACS. Nel documento vengono illustrati i concetti e le impostazioni che utilizzano l'autenticazione client PEAP (Protected Extensible Authentication Protocol).

Per ulteriori informazioni sull'autenticazione PEAP, fare riferimento al <u>protocollo Cisco Protected</u> <u>Extensible Authentication Protocol</u>.

# **Configurazione**

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nel documento vengono usate queste configurazioni:

- <u>Configurazione host agente</u>
- <u>Configurazione agente di autenticazione</u>

## Configurazione host agente

#### Uso di Cisco Secure ACS come server RADIUS

Per facilitare la comunicazione tra Cisco Secure ACS e l'appliance RSA Authentication Manager/RSA SecurID, è necessario aggiungere un record Host agente al database di RSA Authentication Manager. Il record Host agente identifica l'ACS Cisco Secure nel relativo database e contiene informazioni sulla comunicazione e la crittografia.

Per creare il record Host agente, sono necessarie le seguenti informazioni:

- Nome host del server Cisco ACS
- Indirizzi IP per tutte le interfacce di rete del server Cisco ACS

Attenersi alla seguente procedura:

- 1. Aprire l'applicazione RSA Authentication Manager in modalità host.
- 2. Selezionare Host agente > Aggiungi host agente.



Viene visualizzata la seguente

t Agent Host	
Name: SB-ACS	hostname of the ACS Server
Site:	Select
Agent type: Communication Ser Single-Transaction Net OS Agent	Comm Server
Encryption Type: SDI & DES	ed .
Search Other Real	ns for Unknown Users
I⊽ Enable Offline Auth I⊽ Enable Windows P	entication assword Integration
🗖 Create Verifiable Au	uthentications
Group Activations	Uscr Activations
Secondary Nodes	Delete Agent Host
Edit Agent Host Extension Data	Configure RADIUS Connection
Assign Acting Servers	Create Node Secret File

- 3. Immettere le informazioni appropriate per il nome del server Cisco ACS e l'indirizzo di rete. Scegliere **NetOS** per il tipo di agente e selezionare la casella di controllo **Apri a tutti gli utenti conosciuti localmente**.
- 4. Fare clic su OK.

## Utilizzo di RSA Authentication Manager 6.1 RADIUS Server

Per facilitare la comunicazione tra il WLC di Cisco e RSA Authentication Manager, è necessario aggiungere un record Host agente al database di RSA Authentication Manager e al database del server RADIUS. Il record Host agente identifica il WLC Cisco all'interno del relativo database e contiene informazioni sulla comunicazione e la crittografia.

Per creare il record Host agente, sono necessarie le seguenti informazioni:

- Nome host WLC
- Indirizzi IP di gestione del WLC
- RADIUS secret, che deve corrispondere al segreto RADIUS sul WLC Cisco

Quando si aggiunge il record host dell'agente, il ruolo del WLC viene configurato come server di comunicazione. Questa impostazione viene utilizzata da RSA Authentication Manager per determinare la modalità di comunicazione con il WLC.

**Nota:** i nomi host all'interno di RSA Authentication Manager/RSA SecurID Appliance devono essere risolti in indirizzi IP validi sulla rete locale.

Attenersi alla seguente procedura:

- 1. Aprire l'applicazione RSA Authentication Manager in modalità host.
- 2. Selezionare Host agente > Aggiungi host



Viene visualizzata la seguente

Name: 1	92.168.10.102	Point to WLC when using RSA's RADIUS	
Network address: 1	92.168.10.102	Server	
Site:			Selec
Agent type: U	NIX Agent ommunication Serve	·	
Encryption Type:	SDI @ DES		
	pen to All Locally Kn	own Users	
<b>□</b> S	earch Other Realms	for Unknown Users	
E R	equires Name Lock		
E E	nable Offline Authen	tication	
FΕ	nable Windows Pas:	sword Integration	
Г C	reate Verifiable Auth	entications	
Group Activ	ations	User Activations	Ĩ.
Secondary Nodes		Delete Agent Host	
Edit Agent Host Ex	tension Data	Contigure RADIUS Connection	
	Canada	Create Node Secret File	

finestra:

- 3. Immettere le informazioni appropriate per il nome host WLC (un FQDN risolvibile, se necessario) e l'indirizzo di rete. Scegliere **Communication Server** per il tipo di agente e selezionare la casella di controllo **Apri a tutti gli utenti noti localmente**.
- 4. Fare clic su OK.
- 5. Dal menu selezionare RADIUS > Gestisci server
  - RADIUS.



Viene visualizzata una nuova finestra di amministrazione.

6. In questa finestra selezionare **Client RADIUS**, quindi fare clic su **Aggiungi**.



7. Immettere le informazioni appropriate per il WLC di Cisco. Il segreto condiviso deve corrispondere al segreto condiviso definito nel WLC di

d RADIUS Client		
Name:	GSCOARONET	Any RADIUS Client
Description:		]
P Address:	10.100.10.11	_
Shared secret:	12345678	
Make/model:	- Standard Radius -	<u>VV</u> eb Info
Advanced		
Use different :	shared secret for Accounting	
Assume down	n if no keepalive packets after	seconds
L		
	OK Cancel	

8. Fare clic su OK.

# Configurazione agente di autenticazione

La tabella seguente rappresenta la funzionalità RSA Authentication Agent di ACS:

Partner Integration Overview		
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		

**Nota:** vedere la documentazione RADIUS inclusa con RSA Authentication Manager per informazioni su come configurare il server RADIUS, se si tratta del server RADIUS che verrà utilizzato.

## Configurazione di Cisco ACS

#### Attivazione dell'autenticazione RSA SecurID

Cisco Secure ACS supporta l'autenticazione RSA SecurID degli utenti. Completare questa procedura per configurare Cisco Secure ACS per autenticare gli utenti con Authentication Manager 6.1:

- 1. Installare RSA Authentication Agent 5.6 o versione successiva per Windows sullo stesso sistema del server Cisco Secure ACS.
- 2. Verificare la connettività eseguendo la funzione Test di autenticazione dell'agente di autenticazione.
- 3. Copiare il file acecInt.dll dalla directory server RSA c:\Programmi\RSA Security\RSA Authentication Manager\prog nella directory c:\WINNT\system32 del server ACS.
- 4. Nella barra di spostamento fare clic su **Database utente esterno**. Fare quindi clic su **Configurazione database** nella pagina Database esterno.

	+ 🕲 🖪	[1] 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이 이	dex2.htm 🔄 📆 – 🕫 🗴
	Craco Systems	External User Databases	×
	Lid His-id Dive	Select	Help
	User Setup Setup Setup Setup Onered Profile Components	<ul> <li>Unknown User Pohey</li> <li>Database Configuration</li> </ul>	<ul> <li>Unknown User Policy</li> <li>Database Group Mappings</li> <li>Database Configuration</li> </ul>
	Network Configuration	Basic to Help	Unknown User Policy
	Configuration		Click to configure the authentication procedure for unknown users not configured in the CiscoSecure user database.
0	and Administration		[Back to Top]
	93 Databases		Database Group Mappings
	Coline Decementation		Click to configure the Cisco Secure ACS group authorization privileges that unknown users who authenticate to an external database will inherit.
			[Back to Top]
			Database Configuration
			Click to configure a particular external database type for users to authenticate against. Cisco Secure ACS can authenticate against the Windows NTP2000 user database as well as against usernames in token card servers and other supported third-party databases.
			[Back to Top]

5. Nella pagina Configurazione database utenti esterni, fare clic su RSA SecurID Token



6. Fare clic su Crea nuova

#### configurazione.

Ge Edit Vien Favorites Inde Heb ② Sack - ○ - • • 2 ☆ ♪ Search ☆ Favorites ☆ Media @ ○ - ▷ 题 - □ Address @ beta-d/122.0.0.102001	<b>A</b>
Q Sack • Q → P 2	
Addess (2) http:/// 27.0.0 (1/27.0.0)	
	nks <sup>30</sup>
Google - 😥 🚱 Search Web - 🦚 🗗 Oblicited 🌾 Avier 1 🔤 Options 🥒	
External User Databases	×
Edit Haip	-
<ul> <li>Natural: Admission Control</li> <li>Natural: Admission Co</li></ul>	
Chek to configure Windows SAM and Active Directory databases with which Cisco Secure ACS can authenticate users.	
Applet startStop started	-

7. Immettere un nome, quindi fare clic su



#### 8. Fare clic su

#### Configura. icrosoft Internet Exp - 6 × Elle Edit View Favorites Icols Help \* 🔾 Back + 🔘 - 🖻 🤰 🐔 🔎 Search 🔅 Pavorites 😽 Nedia 🕘 🔅 + 🍌 😿 + 🔛 💌 🔁 Go Links \*\* Add ess () http://127.0.0.1:3342/ 💌 🍘 Search Web 🔹 🥵 📑 O Nocked 🗐 AutoFit 🛛 💽 Options 🥒 Google -× Enter Storens External User Databases adding adding. Edit Setup Network Admission Control Windows Database Setup **External User Database Configuration** 2 Novell NDS ٠ Generic LDAP StanedProfile Components Choose what to do with the RSA SecurID Token Server External ODBC Database database LEAP Proxy RADIUS Server Configuration Token Card Server Support Configure Delete **RADIUS Token Server** Configuration RSA SecurIDTeken Server Castiguration Administratio Network Admission Control Databases Click to configure Network Admission Control (NAC) Cancel databases, external policies, local policies, and rules. Cisco Secure ACS uses NAC databases to process Activity posture validation requests. Consumentation Back to Help [Back to Top] Windows Database Click to configure Windows SAM and Active Directory databases with which Cisco Secure ACS can authenticate users. 1.1 Applet startitop started Local intranet

In Cisco Secure ACS vengono visualizzati il nome del server token e il percorso della DLL di autenticazione. Queste informazioni confermano che Cisco Secure ACS può contattare l'agente di autenticazione RSA. È possibile aggiungere il database degli utenti esterni RSA SecurID alla politica utente sconosciuta o assegnare account utente specifici per utilizzare questo database per



#### Aggiunta/configurazione dell'autenticazione RSA SecurID per la policy utente sconosciuta

Attenersi alla seguente procedura:

1. Nella barra di navigazione di ACS, fare clic su **Database utente esterno > Criterio utente sconosciuto**.



 Nella pagina Criteri utente sconosciuti, selezionare Controlla i seguenti database utenti esterni, evidenziare RSA SecurID Token Server e spostarlo nella casella Database selezionati. Fare quindi clic su Invia.

a - 19 - 🕥 🗈	조 이 데 이 티 · · · · · · · · · · · · · · · · · ·	ander-2.Nen 💌 🚺	$- \sigma \approx$
Cinco Statema	External User Databases		×
and the art the s	Edit	Help	
Carporenti	Configure Unknown User Policy	<ul> <li>Unknown User Policy</li> <li>Eail the Attempt</li> <li>Check the following external users databases</li> </ul>	
Befureri Derfigeration	C Failthe attempt	Unknown User Policy	
Carrigentian	Check the following external user databases	Use this window to define how to handle usemanars not found in the Circo Secure ACS database.	
Administration Cost rol		Fail the attempt	
Balanses		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	
Det Beitere		[Back to Top]	
		Check the following external user databases	
	P Card to Party	If you want Cisco Secure ACS to use specific external user dathases to authenticate takenoun users, select this option. You can choose the databases and the order in which Cisco Secure ACS uses them to try to authenticate unknown users.	
		For each database that Circo Secure ACS should use to try to authenticate unknown users, relect the database name in the Esternal Databases list and check the right arrow button to move it to the Selected Databases list.	
	Subme Concel	<ul> <li>The order of databases on the Selected Databases list determines the sequence of databases that Cisco Secure</li> </ul>	

Aggiunta/configurazione dell'autenticazione RSA SecurID per account utente specifici

Attenersi alla seguente procedura:

- 1. Fare clic su **User Setup** (Configurazione utente) dall'interfaccia principale di ACS Admin. Immettere il nome utente e fare clic su **Aggiungi** (o selezionare un utente esistente da modificare).
- 2. In Impostazione utente > Autenticazione password, scegliere **RSA SecurID Token Server**. Fare quindi clic su

Cisco Systems	User Setup	
ومناللة ومناللة و	Edit	
User Sotup	User: sbrsa	
Shared Profile Components	Account Disabled	
Natwork Configuration	Supplementary User Info	
System Configuration	Real Name	
Interface Configuration	Description	
Administration Central		
External User Databases	User Setup	
Posture Validation	Password Authentication:	
Selvarie Access	RSA SecurID Token Server	
Profiles	CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.)	
Reports and Activity	Password	
Doline Desimportation	Confirm	
Land -   Concentration	Password	
	Separate (CHAP/MS-CHAP/ARAP)	
	Password	
	Confirm Password	

#### Aggiungere un client RADIUS in Cisco ACS

L'installazione del server Cisco ACS richiederà gli indirizzi IP del WLC per fungere da server NAS per l'inoltro delle autenticazioni PEAP dei client agli ACS.

Attenersi alla seguente procedura:

 In Configurazione di rete, aggiungere/modificare il client AAA per il WLC da utilizzare. Immettere la chiave "shared secret" (comune a WLC) utilizzata tra il client AAA e ACS. Selezionare Autentica con > RADIUS (Cisco Airespace) per questo client AAA. Quindi, fare clic su Submit + Apply (Invia +

CIRCO STATEMA	Network Configuration
with the filler.	Edit
User Setup	
Breup Setup	AAA Client Setup For
Shared Profile Components	WLC4404
Net work Configuration	AAA Client IP Address
Earliguration	Key RSA
Administration Centrol	Authenticate RADIVS (Cisco Airespace)
Detabases	Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
Boome Validation	Log Update/Watchdog Packets from this AAA Client
Profiles	Log RADIUS Tunneling Packets from this AAA Client
Reports and Activity	Replace RADIUS Port info with Usemame from this AAA     Client
Documentation	
	Submit Submit + Apply Delete Delete + Apply
	Cancel

#### Applica).

- 2. Richiedere e installare un certificato server da un'Autorità di certificazione nota e attendibile, ad esempio RSA Keon Certificate Authority.Per ulteriori informazioni su questo processo, consultare la documentazione fornita con Cisco ACS. Se si utilizza RSA Certificate Manager, è possibile consultare la guida all'implementazione di RSA Keon Aironet per ulteriori informazioni. È necessario completare questa attività prima di continuare.Nota: è possibile utilizzare anche certificati autofirmati. Per ulteriori informazioni, consultare la documentazione di Cisco Secure ACS.
- In Configurazione di sistema > Impostazione autenticazione globale, selezionare la casella di controllo Consenti autenticazione PEAP.



## Configurazione di Cisco Wireless LAN Controller per 802.1x

Attenersi alla seguente procedura:

- 1. Connettersi all'interfaccia della riga di comando del WLC per configurare il controller in modo che possa essere configurato per la connessione al server Cisco Secure ACS.
- Immettere il comando config radius auth ip-address dal WLC per configurare un server RADIUS per l'autenticazione. Nota: quando si esegue il test con il server RADIUS RSA Authentication Manager, immettere l'indirizzo IP del server RADIUS di RSA Authentication Manager. Quando si esegue il test con il server Cisco ACS, immettere l'indirizzo IP del server Cisco Secure ACS.
- 3. Immettere il comando **config radius auth port** dal WLC per specificare la porta UDP per l'autenticazione. Le porte 1645 o 1812 sono attive per impostazione predefinita sia nel server RSA Authentication Manager che nel server Cisco ACS.
- 4. Immettere il comando **config radius auth secret** dal WLC per configurare il segreto condiviso sul WLC. Deve corrispondere al segreto condiviso creato nei server RADIUS per questo client RADIUS.
- 5. Immettere il comando **config radius auth enable** dal WLC per abilitare l'autenticazione. Se lo si desidera, immettere il comando **config radius auth disable** per disabilitare l'autenticazione. L'autenticazione è disabilitata per impostazione predefinita.
- 6. Selezionare l'opzione di sicurezza di layer 2 appropriata per la WLAN desiderata sul WLC.
- 7. Utilizzare i comandi **show radius auth statistics** e **show radius summary** per verificare che le impostazioni RADIUS siano configurate correttamente.**Nota:** i timer predefiniti per il timeout della richiesta EAP sono bassi e potrebbero dover essere modificati. A tale scopo, è

possibile usare il comando **config advanced eap request-timeout** *<seconds>*. Può inoltre essere utile modificare il timeout della richiesta di identità in base ai requisiti. A tale scopo, è possibile usare il comando **config advanced eap identity-request-timeout** *<*secondi> .

### Configurazione client wireless 802.11

Per una spiegazione dettagliata su come configurare l'hardware wireless e il supplicant client, consultare la documentazione di Cisco.

# Problemi noti

Questi sono alcuni dei problemi noti relativi all'autenticazione RSA SecureID:

- Token software RSA. Le modalità New Pin e Next Tokencode non sono supportate quando si utilizza questa forma di autenticazione con XP2. (FISSO come risultato di ACS-4.0.1-RSA-SW-CSCsc12614-CSCsd41866.zip)
- Se l'implementazione di ACS è meno recente o non si dispone della patch indicata, il client non sarà in grado di eseguire l'autenticazione fino a quando l'utente non passa da "Attivato;Modalità nuovo PIN" a "Attivato". A tale scopo, è possibile richiedere all'utente di completare un'autenticazione non wireless oppure utilizzare l'applicazione RSA "test di autenticazione".
- Nega PIN a 4 cifre/alfanumerici. Se un utente in modalità Nuovo PIN non rispetta i criteri PIN, il processo di autenticazione non riesce e l'utente non sa come o perché. In genere, se un utente non rispetta il criterio, gli verrà inviato un messaggio che informa che il PIN è stato rifiutato e verrà visualizzato un nuovo messaggio che indica di nuovo il criterio PIN (ad esempio, se il criterio PIN è composto da 5-7 cifre, ma l'utente immette 4 cifre).

# Informazioni correlate

- Esempio di configurazione del mapping delle VLAN dinamiche con WLC basati su ACS ad Active Directory
- Esempio di configurazione di Client VPN over Wireless LAN con WLC
- Esempi di configurazione dell'autenticazione sui controller LAN wireless
- <u>Esempio di autenticazione EAP-FAST con i controller LAN wireless e la configurazione del</u> server RADIUS esterno
- Tipi di autenticazione wireless su ISR fisso tramite configurazione SDM
- Tipi di autenticazione wireless su una configurazione ISR fissa Esempio
- Protocollo Cisco Protected Extensible Authentication
- <u>Autenticazione EAP con server RADIUS</u>
- Documentazione e supporto tecnico Cisco Systems