

# Autenticazione EAP con server RADIUS

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Autenticazione di rete EAP o aperta con EAP](#)

[Definisci server di autenticazione](#)

[Definizione dei metodi di autenticazione client](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Procedura di risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Informazioni correlate](#)

## [Introduzione](#)

In questo documento viene fornita una configurazione di esempio di un punto di accesso basato su Cisco IOS® per l'autenticazione EAP (Extensible Authentication Protocol) di utenti wireless su un database a cui si accede da un server RADIUS.

A causa del ruolo passivo che il punto di accesso svolge in EAP (crea un ponte tra i pacchetti wireless del client e i pacchetti cablati destinati al server di autenticazione e viceversa), questa configurazione viene utilizzata praticamente con tutti i metodi EAP. Questi metodi includono (ma non sono limitati a) LEAP, Protected EAP (PEAP)-MS-Challenge Handshake Authentication Protocol (CHAP) versione 2, PEAP-Generic Token Card (GTC), EAP-Flexible Authentication via Secure Tunneling (FAST), EAP-Transport Layer Security (TLS) e EAP-Tunneled TLS (TTLS). È necessario configurare in modo appropriato il server di autenticazione per ognuno di questi metodi EAP.

In questo documento viene descritto come configurare il punto di accesso (AP) e il server RADIUS, ovvero Cisco Secure ACS nell'esempio di configurazione riportato in questo documento.

## [Prerequisiti](#)

### [Requisiti](#)

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

- L'utente ha familiarità con la GUI o la CLI di Cisco IOS.
- L'utente ha familiarità con i concetti alla base dell'autenticazione EAP.

## Componenti usati

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

- Prodotti Cisco Aironet AP con Cisco IOS.
- Si presume che la rete includa una sola VLAN (Virtual LAN).
- Prodotto server di autenticazione RADIUS che si integra correttamente in un database utenti. Questi sono i server di autenticazione supportati per Cisco LEAP e EAP-FAST: Cisco Secure Access Control Server (ACS) Cisco Access Registrar (CAR) Funk Steel Belted RADIUS Merito interlink. Questi sono i server di autenticazione supportati per Microsoft PEAP-MS-CHAP versione 2 e PEAP-GTC: Servizio di autenticazione Internet Microsoft (IAS) Cisco Secure ACS Funk Steel Belted RADIUS Merito interlink. Qualsiasi altro server di autenticazione che Microsoft può autorizzare. **Nota:** le password GTC o One-Time richiedono servizi aggiuntivi che richiedono software aggiuntivo sia sul lato client che su quello server, nonché generatori di token hardware o software. Per informazioni dettagliate sui server di autenticazione supportati con i relativi prodotti per EAP-TLS, EAP-TTLS e altri metodi EAP, rivolgersi al produttore del client richiedente.

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 [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

## Configurazione

In questa configurazione viene descritto come configurare l'autenticazione EAP su un access point basato su IOS. Nell'esempio riportato nel presente documento, il protocollo LEAP viene utilizzato come metodo di autenticazione EAP con un server RADIUS.

**Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

Come con la maggior parte degli algoritmi di autenticazione basati su password, Cisco LEAP è vulnerabile agli attacchi dei dizionari. Questo non è un nuovo attacco o una nuova vulnerabilità di Cisco LEAP. La creazione di un criterio di password efficace è il modo più efficace per ridurre gli attacchi dei dizionari. Ciò include l'uso di password sicure e la scadenza periodica delle password. Per ulteriori informazioni sugli attacchi dei dizionari e su come prevenirli, fare riferimento a [Attacco del dizionario su Cisco LEAP](#).

In questo documento viene usata questa configurazione sia per la GUI che per la CLI:

- L'indirizzo IP dell'access point è 10.0.0.106.
- L'indirizzo IP del server RADIUS (ACS) è 10.0.0.3.

## Autenticazione di rete EAP o aperta con EAP

In qualsiasi metodo di autenticazione basato su EAP/802.1x è possibile stabilire quali sono le differenze tra l'autenticazione EAP in rete e l'autenticazione aperta con EAP. Questi elementi fanno riferimento ai valori del campo Authentication Algorithm nelle intestazioni dei pacchetti di gestione e associazione. La maggior parte dei produttori di client wireless imposta questo campo sul valore 0 (Autenticazione aperta), quindi segnala il desiderio di eseguire l'autenticazione EAP in una fase successiva del processo di associazione. Cisco imposta il valore in modo diverso dall'inizio dell'associazione al flag Network EAP.

Se nella rete sono presenti client:

- Client Cisco: utilizzare Network-EAP.
- Client di terze parti (inclusi prodotti compatibili con CCX): utilizzare Open con EAP.
- Combinazione di client Cisco e di terze parti: scegliere sia Network-EAP che Open with EAP.

## Definisci server di autenticazione

Il primo passaggio della configurazione EAP consiste nel definire il server di autenticazione e stabilire una relazione con esso.

1. Nella scheda Access point Server Manager (sotto la voce di menu **Protezione > Server Manager**), attenersi alla seguente procedura: Immettere l'indirizzo IP del server di autenticazione nel campo Server. Specificare il segreto condiviso e le porte. Per creare la definizione e popolare gli elenchi a discesa, fare clic su **Apply** (Applica). Impostare il campo Tipo di autenticazione EAP Priorità 1 sull'indirizzo IP del server in Priorità server predefinite. Fare clic su **Apply** (Applica).

The screenshot displays the configuration page for a Cisco 1200 Access Point. The left sidebar contains navigation options like HOME, EXPRESS SET-UP, SECURITY, and SERVICES. The main area is titled 'SERVER MANAGER' and 'GLOBAL PROPERTIES'. It shows the hostname 'AP' and the date '12:18:46 Mon Sep 20 2004'. The 'Backup RADIUS Server' section has input fields for the server address and shared secret. The 'Corporate Servers' section lists a server with IP '10.0.0.3' and ports '1645' for authentication and '1646' for accounting. The 'Default Server Priorities' section shows 'EAP Authentication' with priority 1 set to '10.0.0.3'. Other sections include MAC Authentication, Accounting, Admin Authentication (RADIUS and TACACS+), and Proxy Mobile IP Authentication.

Dalla CLI, è possibile anche usare questi comandi:

```
AP#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
AP(config)#aaa group server radius rad_eap
```

```
AP(config-sg-radius)#server 10.0.0.3 auth-port 1645 acct-port 1646
```

```
AP(config-sg-radius)#exit
AP(config)#aaa new-model
AP(config)#aaa authentication login eap_methods group rad_eap
AP(config)#radius-server host 10.0.0.3 auth-port 1645
acct-port 1646 key labap1200ip102
AP(config)#end
AP#write memory
```

2. Il punto di accesso deve essere configurato nel server di autenticazione come client AAA. Ad esempio, in Cisco Secure ACS, questo accade nella pagina [Configurazione di rete](#) in cui sono definiti il nome del punto di accesso, l'indirizzo IP, il segreto condiviso e il metodo di autenticazione (RADIUS Cisco Aironet o RADIUS Cisco IOS/PIX). Per altri server di autenticazione non ACS, consultare la documentazione del produttore.

**Network Configuration**

AAA Client Hostname: AP

AAA Client IP Address: 10.0.0.106

Key: sharedsecret

Authenticate Using: RADIUS (Cisco IOS/PIX)

Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

Submit Submit + Restart Cancel

**Help**

- [AAA Client Hostname](#)
- [AAA Client IP Address](#)
- [Key](#)
- [Network Device Group](#)
- [Authenticate Using](#)
- [Single Connect TACACS+ AAA Client](#)
- [Log Update/Watchdog Packets from this AAA Client](#)
- [Log RADIUS Tunneling Packets from this AAA Client](#)
- [Replace RADIUS Port info with Username from this AAA Client](#)

**AAA Client Hostname**

The AAA Client Hostname is the name assigned to the AAA client.


[\[Back to Top\]](#)

Verificare che il server di autenticazione sia configurato in modo da eseguire il metodo di autenticazione EAP desiderato. Ad esempio, per un Cisco Secure ACS con protocollo LEAP, configurare l'autenticazione LEAP nella pagina [Configurazione di sistema - Impostazione autenticazione globale](#). Fare clic su **Configurazione di sistema**, quindi su **Configurazione autenticazione globale**. Per altri server di autenticazione non ACS o altri metodi EAP, consultare la documentazione del produttore.

**CISCO SYSTEMS** **System Configuration**

Select	Help
<ul style="list-style-type: none"> <li> User Setup</li> <li> Group Setup</li> <li> Shared Profile Components</li> <li> Network Configuration</li> <li> System Configuration</li> <li> Interface Configuration</li> <li> Administration Control</li> <li> External User Databases</li> <li> Reports and Activity</li> <li> Online Documentation</li> </ul>	<ul style="list-style-type: none"> <li> <a href="#">Service Control</a></li> <li> <a href="#">Logging</a></li> <li> <a href="#">Date Format Control</a></li> <li> <a href="#">Local Password Management</a></li> <li> <a href="#">CiscoSecure Database Replication</a></li> <li> <a href="#">ACS Backup</a></li> <li> <a href="#">ACS Restore</a></li> <li> <a href="#">ACS Service Management</a></li> <li> <a href="#">IP Pools Server</a></li> <li> <a href="#">IP Pools Address Recovery</a></li> <li> <a href="#">ACS Certificate Setup</a></li> <li> <a href="#">Global Authentication Setup</a></li> </ul> <p style="text-align: center;"> Back to Help</p>
	<ul style="list-style-type: none"> <li>• <a href="#">Service Control</a></li> <li>• <a href="#">Logging</a></li> <li>• <a href="#">Date Format Control</a></li> <li>• <a href="#">Local Password Management</a></li> <li>• <a href="#">CiscoSecure Database Replication</a></li> <li>• <a href="#">RDBMS Synchronization</a></li> <li>• <a href="#">ACS Backup</a></li> <li>• <a href="#">ACS Restore</a></li> <li>• <a href="#">ACS Service Management</a></li> <li>• <a href="#">IP Pools Address Recovery</a></li> <li>• <a href="#">IP Pools Server</a></li> <li>• <a href="#">VoIP Accounting Configuration</a></li> <li>• <a href="#">ACS Certificate Setup</a></li> <li>• <a href="#">Global Authentication Configuration</a></li> </ul> <hr/> <p><b>Service Control</b></p> <p>Select to open the page from which you can stop or restart Cisco Secure ACS services.</p> <p style="text-align: right;"><a href="#">[Back to Top]</a></p>

Nell'immagine viene mostrato Cisco Secure ACS configurato per PEAP, EAP-FAST, EAP-TLS, LEAP e EAP-MD5.



# System Configuration

Edit

---

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Reports and Activity
- Online Documentation

## Global Authentication Setup

### EAP Configuration ?

**PEAP**

Allow EAP-MSCHAPv2

Allow EAP-GTC

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

---

**EAP-FAST**

Allow EAP-FAST

Active master key TTL:  months

Retired master key TTL:  months

PAC TTL:  weeks

Client initial message:

Authority ID Info:

Allow automatic PAC provisioning:

EAP-FAST master server:

Actual EAP-FAST server status: **Master**

---

**EAP-TLS**

Allow EAP-TLS

Select one or more of the following options:

- Certificate SAN comparison
- Certificate CN comparison
- Certificate Binary comparison

EAP-TLS session timeout (minutes):

---

**LEAP**

Allow LEAP (For Aironet only)

---

**EAP-MD5**

Allow EAP-MD5

AP EAP request timeout (seconds):

### MS-CHAP Configuration ?

Allow MS-CHAP Version 1 Authentication

Allow MS-CHAP Version 2 Authentication

? Back to Help

Submit Submit + Restart Cancel

## Help

- [PEAP](#)
- [EAP-FAST](#)
- [EAP-TLS](#)
- [LEAP](#)
- [EAP-MD5](#)
- [AP EAP request timeout](#)
- [MS-CHAP Configuration](#)

This page specifies settings for various authentication protocols.

[\[Back to Top\]](#)

**PEAP**

*Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have*

[Definizione dei metodi di autenticazione client](#)



Una volta che il punto di accesso sa dove inviare le richieste di autenticazione client, configurarlo per accettare tali metodi.

**Nota:** queste istruzioni si riferiscono a un'installazione basata su WEP. Per WPA (che utilizza cifrature anziché WEP), vedere [Panoramica sulla configurazione WPA](#).

1. Nella scheda Gestione crittografia del punto di accesso (nella voce di menu **Protezione > Gestione crittografia**), attenersi alla seguente procedura: Specificare che si desidera utilizzare la **crittografia WEP**. Specificare che WEP è **obbligatorio**. Verificare che le dimensioni della chiave siano impostate su **128 bit**. Fare clic su **Apply** (Applica).

The screenshot displays the Cisco 1200 Access Point configuration page for the radio interface RADIO0-802.11B. The page is titled "Cisco 1200 Access Point" and shows the "Security: Encryption Manager - Radio0-802.11B" configuration. The "Encryption Modes" section is active, with "WEP Encryption" selected and "Mandatory" chosen from the dropdown menu. The "Cipher" section is set to "WEP 128 bit". The "Encryption Keys" table shows four keys, all set to "128 bit". The "Global Properties" section includes "Broadcast Key Rotation Interval" set to "Disable Rotation" and "WPA Group Key Update" options.

Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1: <input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 2: <input checked="" type="radio"/>	<input type="text"/>	128 bit
Encryption Key 3: <input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 4: <input type="radio"/>	<input type="text"/>	128 bit

Buttons at the bottom: Apply-Radio0, Apply-All, Cancel.



Dalla CLI, è possibile anche usare questi comandi:

```
AP#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
AP(config)#interface dot11radio 0
```

```
AP(config-if)#encryption mode wep mandatory
```

```
AP(config-if)#end
```

```
AP#write memory
```

2. Completare la procedura seguente nella scheda Gestione SSID punto di accesso (sotto la voce di menu **Protezione > Gestione SSID**): Selezionare il SSID desiderato. In "Metodi di autenticazione accettati", selezionare la casella **Apri** e utilizzare l'elenco a discesa per scegliere **Con EAP**. Selezionare la casella **Network-EAP** se si dispone di schede client Cisco. Vedere la discussione nella sezione [Autenticazione di rete EAP o aperta con EAP](#). Fare clic su **Apply** (Applica).

RADIO0-802.11B

RADIO1-802.11A

Hostname AP

12:47:46 Mon Sep 20 2004

- HOME
- EXPRESS SET-UP
- EXPRESS SECURITY
- NETWORK MAP +
- ASSOCIATION +
- NETWORK INTERFACES +
- SECURITY**
- Admin Access
- Encryption Manager
- SSID Manager**
- Server Manager
- Local RADIUS Server
- Advanced Security
- SERVICES +
- WIRELESS SERVICES +
- SYSTEM SOFTWARE +
- EVENT LOG +

## Security: SSID Manager - Radio0-802.11B

### SSID Properties

#### Current SSID List

< NEW >  
labap1200

**SSID:** labap1200

**VLAN:** < NONE > [Define VLANs](#)

**Network ID:** (0-4096)

Delete-Radio0

Delete-All

### Authentication Settings

#### Methods Accepted:

Open Authentication: with EAP

Shared Authentication: < NO ADDITION >

Network EAP: < NO ADDITION >

#### Server Priorities:

##### EAP Authentication Servers

Use Defaults [Define Defaults](#)

Customize

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

##### MAC Authentication Servers

Use Defaults [Define Defaults](#)

Customize

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

Portions of this image not relevant to the discussion have been edited for clarity

### Global Radio0-802.11B SSID Properties

**Set Guest Mode SSID:** < NONE >

**Set Infrastructure SSID:** < NONE >  Force Infrastructure Devices to associate only to this SSID

Apply

Cancel

Dalla CLI, è possibile anche usare questi comandi:

```
AP#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

AP(config)#interface dot11radio 0

AP(config-if)#ssid labap1200

AP(config-if-ssid)#authentication open eap eap_methods

AP(config-if-ssid)#authentication network-eap eap_methods

AP(config-if-ssid)#end

AP#write memory
```

Dopo aver confermato le funzionalità di base con una configurazione EAP di base, è possibile aggiungere ulteriori funzionalità e la gestione delle chiavi in un secondo momento. Per facilitare la risoluzione dei problemi, è possibile sovrapporre funzioni più complesse alle fondamentali.

## Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show** sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

- **show radius server-group all**: visualizza un elenco di tutti i gruppi di server RADIUS configurati sull'access point.

## Risoluzione dei problemi

### Procedura di risoluzione dei problemi

Completare questa procedura per risolvere i problemi relativi alla configurazione.

1. Nell'utilità o nel software sul lato client, creare un nuovo profilo o una nuova connessione con gli stessi parametri o con parametri simili per assicurarsi che la configurazione del client non sia danneggiata.
2. Per evitare problemi di RF che impediscano l'autenticazione, disabilitare temporaneamente l'autenticazione come mostrato di seguito: Dalla CLI, usare i comandi **no authentication open eap\_methods**, **no authentication network-eap\_methods** e **authentication open**. Dalla GUI, nella pagina SSID Manager, deselezionare **Network-EAP**, selezionare **Open**, quindi reimpostare l'elenco a discesa su **No Addition** (Nessuna aggiunta). Se il client viene associato correttamente, RF non contribuisce al problema di associazione.
3. Verificare che le password segrete condivise siano sincronizzate tra il punto di accesso e il server di autenticazione. In caso contrario, è possibile ricevere il seguente messaggio di errore:

```
Invalid message authenticator in EAP request
```

Dalla CLI, controllare la riga `radius-server host x.x.x auth-port x acct-port x key <shared_secret>`. Dalla GUI, nella pagina Server Manager, immettere nuovamente il segreto condiviso per il server appropriato nella casella denominata "Segreto condiviso". La voce segreta condivisa per il punto di accesso sul server RADIUS deve contenere la stessa password segreta condivisa indicata in precedenza.

4. Rimuovere tutti i gruppi di utenti dal server RADIUS. A volte possono verificarsi conflitti tra gruppi di utenti definiti dal server RADIUS e gruppi di utenti nel dominio sottostante. Verificare nei registri del server RADIUS i tentativi non riusciti e i motivi per cui tali tentativi non sono riusciti.

## Comandi per la risoluzione dei problemi

Alcuni comandi **show** sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

[Debug delle autenticazioni](#) fornisce una quantità significativa di dettagli su come raccogliere e interpretare l'output dei debug relativi a EAP.

**Nota:** prima di usare i comandi di **debug**, consultare le [informazioni importanti sui comandi di debug](#).

- **debug dot11 aaa authentication state-machine:** visualizza le divisioni principali (o stati) della negoziazione tra il client e il server di autenticazione. Di seguito è riportato un output di un'autenticazione riuscita:

```
*Mar 1 02:37:46.846: dot11_auth_dot1x_send_id_req_to_client: Sending
identity request to 0040.96ac.dd05
*Mar 1 02:37:46.846: dot11_auth_dot1x_send_id_req_to_client:
0040.96ac.dd05 timer started for 30 seconds
*Mar 1 02:37:46.930: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,EAP_START) for 0040.96ac.dd05
*Mar 1 02:37:46.931: dot11_auth_dot1x_send_id_req_to_client:
Sending identity request to 0040.96ac.dd05 (client)
*Mar 1 02:37:46.931: dot11_auth_dot1x_send_id_req_to_client: Client
0040.96ac.dd05 timer started for 30 seconds
*Mar 1 02:37:46.938: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96ac.dd05
*Mar 1 02:37:46.938: dot11_auth_dot1x_send_response_to_server:
Sending client 0040.96ac.dd05 data (User Name) to server
*Mar 1 02:37:46.938: dot11_auth_dot1x_send_response_to_server:
Started timer server_timeout 60 seconds
*Mar 1 02:37:47.017: dot11_auth_dot1x_run_rfsm: Executing
Action(SERVER_WAIT,SERVER_REPLY) for 0040.96ac.dd05
*Mar 1 02:37:47.017: dot11_auth_dot1x_send_response_to_client:
Forwarding server message(Challenge) to client 0040.96ac.dd05
*Mar 1 02:37:47.018: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 20 seconds
*Mar 1 02:37:47.025: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96ac.dd05
*Mar 1 02:37:47.025: dot11_auth_dot1x_send_response_to_server:
Sending client 0040.96ac.dd05 data(User Credentials) to server
-----Lines Omitted for simplicity-----
*Mar 1 02:37:47.030: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 20 seconds
*Mar 1 02:37:47.041: dot11_auth_dot1x_run_rfsm: Executing Action
(SERVER_WAIT,SERVER_PASS) for 0040.96ac.dd05
*Mar 1 02:37:47.041: dot11_auth_dot1x_send_response_to_client:
Forwarding server message(Pass Message) to client
```

0040.96ac.dd05

```
*Mar 1 02:37:47.042: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 30 seconds
*Mar 1 02:37:47.043: %DOT11-6-ASSOC: Interface Dot11Radio0,
Station TACWEB 0040 .96ac.dd05 Associated KEY_MGMT[NONE] (Client stays
associated to the access point)
```

**Nota:** nelle versioni software Cisco IOS precedenti alla 12.2(15)JA, la sintassi del comando **debug** è **debug dot11 aaa dot1x state-machine**.

- **debug dot11 aaa authenticator process:** visualizza le singole voci di dialogo della negoziazione tra il client e il server di autenticazione. **Nota:** nelle versioni software Cisco IOS precedenti alla 12.2(15)JA, la sintassi del comando **debug** è **debug dot11 aaa dot1x process**.
- **debug radius authentication:** visualizza le negoziazioni RADIUS tra il server e il client, entrambe con bridging eseguito dal punto di accesso. Questo è l'output dell'autenticazione **non riuscita:**

```
*Mar 1 02:34:55.086: RADIUS/ENCODE(00000031):Orig. component type = DOT11
*Mar 1 02:34:55.086: RADIUS: AAA Unsupported Attr: ssid [264] 5
*Mar 1 02:34:55.086: RADIUS: 73 73 69 [ssi]
*Mar 1 02:34:55.086: RADIUS: AAA Unsupported Attr: interface [157] 3
*Mar 1 02:34:55.087: RADIUS: 32 [2]
*Mar 1 02:34:55.087: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.087: RADIUS/ENCODE(00000031): acct_session_id: 47
*Mar 1 02:34:55.087: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.087: RADIUS(00000031): sending
*Mar 1 02:34:55.087: RADIUS(00000031): Send Access-Request
to 10.0.0.3 :164 5 id 1645/61, len 130
*Mar 1 02:34:55.088: RADIUS: authenticator 0F 6D B9 57 4B A3 F2 0E -
56 77 A4 7E D3 C2 26 EB
*Mar 1 02:34:55.088: RADIUS: User-Name [1] 8 "wirels"
*Mar 1 02:34:55.088: RADIUS: Framed-MTU [12] 6 1400
*Mar 1 02:34:55.088: RADIUS: Called-Station-Id [30] 16 "0019.a956.55c0"
*Mar 1 02:34:55.088: RADIUS: Calling-Station-Id [31] 16 "0040.96ac.dd05"
*Mar 1 02:34:55.088: RADIUS: Service-Type [6] 6 Login [1]
*Mar 1 02:34:55.088: RADIUS: Message-Authenticato[80] 18
*Mar 1 02:34:55.089: RADIUS: 73 8C 59 C4 98 51 53 9F 58 4D 1D EB A5
4A AB 88 [s?Y??QS?XM???J??]
*Mar 1 02:34:55.089: RADIUS: EAP-Message [79] 13
*Mar 1 02:34:55.089: RADIUS: NAS-Port-Id [87] 5 "299"
*Mar 1 02:34:55.090: RADIUS: NAS-IP-Address [4] 6 10.0.0.106
*Mar 1 02:34:55.090: RADIUS: Nas-Identifier [32] 4 "ap"
*Mar 1 02:34:55.093: RADIUS: Received from id 1645/61
10.0.0.3 :1645, Access-Challenge, len 79
*Mar 1 02:34:55.093: RADIUS: authenticator 72 FD C6 9F A1 53 8F D2 -
84 87 49 9B B4 77 B8 973
-----Lines Omitted-----
*Mar 1 02:34:55.117: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.118: RADIUS/ENCODE(00000031): acct_session_id: 47
*Mar 1 02:34:55.118: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.118: RADIUS(00000031): sending
*Mar 1 02:34:55.118: RADIUS(00000031): Send Access-Request to
10.0.0.3 :164 5 id 1645/62, len 168
*Mar 1 02:34:55.118: RADIUS: authenticator 49 AE 42 83 C0 E9 9A A7 -
07 0F 4E 7C F4 C7 1F 24
*Mar 1 02:34:55.118: RADIUS: User-Name [1] 8 "wirels"
*Mar 1 02:34:55.119: RADIUS: Framed-MTU [12] 6 1400
-----Lines Omitted-----
*Mar 1 02:34:55.124: RADIUS: Received from id 1645/62
10.0.0.3 :1645, Access-Reject, len 56
*Mar 1 02:34:55.124: RADIUS: authenticator A6 13 99 32 2A 9D A6 25 -
AD 01 26 11 9A F6 01 37
*Mar 1 02:34:55.125: RADIUS: EAP-Message [79] 6
```

```
*Mar 1 02:34:55.125: RADIUS: 04 15 00 04 [????]
*Mar 1 02:34:55.125: RADIUS: Reply-Message [18] 12
*Mar 1 02:34:55.125: RADIUS: 52 65 6A 65 63 74 65 64 0A 0D
[Rejected??]
*Mar 1 02:34:55.125: RADIUS: Message-Authenticato[80] 18
*Mar 1 02:34:55.126: RADIUS(00000031): Received from id 1645/62
*Mar 1 02:34:55.126: RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
*Mar 1 02:34:55.126: RADIUS/DECODE: Reply-Message fragments, 10, total 10 bytes
*Mar 1 02:34:55.127: %DOT11-7-AUTH_FAILED: Station
0040.96ac.dd05 Authentication failed
```

- **debug aaa authentication**: visualizza le negoziazioni AAA per l'autenticazione tra il dispositivo client e il server di autenticazione.

## [Informazioni correlate](#)

- [Autenticazioni debug](#)
- [Configurazione dei tipi di autenticazione](#)
- [Autenticazione LEAP su un server RADIUS locale](#)
- [Configurazione dei server RADIUS e TACACS+](#)
- [Configurazione di Cisco Secure ACS per Windows v3.2 con autenticazione computer PEAP-MS-CHAPv2](#)
- [Cisco Secure ACS per Windows v3.2 con autenticazione computer EAP-TLS](#)
- [Configurazione di PEAP/EAP su Microsoft IAS](#)
- [Risoluzione dei problemi relativi a Microsoft IAS come server RADIUS](#)
- [Client di autenticazione Microsoft 802.1X](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)