

ASA 8.0: Configura autenticazione RADIUS per utenti WebVPN

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Configurazione del server ACS](#)

[Configurare l'appliance di sicurezza](#)

[ASDM](#)

[Interfaccia della riga di comando](#)

[Verifica](#)

[Test con ASDM](#)

[Test con CLI](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene illustrato come configurare Cisco Adaptive Security Appliance (ASA) in modo che utilizzi un server RADIUS (Remote Authentication Dial-In User Service) per l'autenticazione degli utenti WebVPN. Nell'esempio, il server RADIUS è un server Cisco Access Control Server (ACS) versione 4.1. Questa configurazione viene eseguita con Adaptive Security Device Manager (ASDM) 6.0(2) su un'appliance ASA con software versione 8.0(2).

Nota: in questo esempio l'autenticazione RADIUS è configurata per gli utenti WebVPN, ma è possibile utilizzare questa configurazione anche per altri tipi di VPN di accesso remoto. Assegnare il gruppo di server AAA al profilo di connessione desiderato (gruppo di tunnel), come mostrato.

[Prerequisiti](#)

- È necessaria una configurazione WebVPN di base.
- Gli utenti di Cisco ACS devono essere configurati per l'autenticazione degli utenti. Per ulteriori informazioni, vedere la sezione [Aggiunta di un account utente di base](#) in [Gestione utente](#).

[Configurazione del server ACS](#)

In questa sezione vengono presentate le informazioni necessarie per configurare l'autenticazione RADIUS su ACS e ASA.

Completare questa procedura per configurare il server ACS in modo che comunichi con l'appliance ASA.

1. Scegliere **Network Configuration** (Configurazione rete) dal menu a sinistra della schermata ACS.
2. Scegliere **Add Entry** in **AAA Client**.
3. Fornire le informazioni sul client: **Nome host client AAA**: un nome a scelta **Indirizzo IP client AAA**: l'indirizzo da cui l'appliance di sicurezza contatta l'ACS **Segreto condiviso**: una chiave segreta configurata su ACS e sull'appliance di sicurezza
4. Nell'elenco a discesa **Autentica tramite** scegliere **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**.
5. Fare clic su **Invia+Applica**.

Esempio di configurazione del client AAA

Network Configuration

Edit

Add AAA Client

AAA Client Hostname:

AAA Client IP Address:

Shared Secret:

RADIUS Key Wrap

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format: ASCII Hexadecimal

Authenticate Using: **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**

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

Match Framed-IP-Address with user IP address for accounting packets from

[Configurare l'appliance di sicurezza](#)

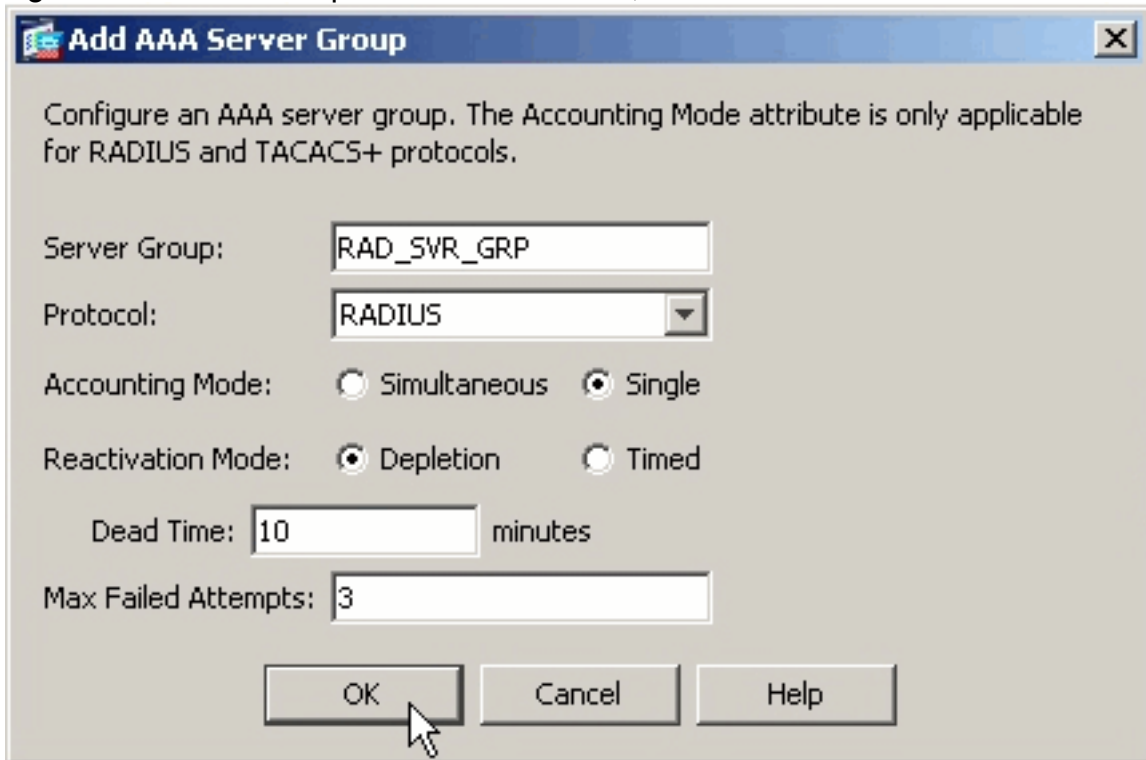
[ASDM](#)

Completare questa procedura in ASDM per configurare l'ASA in modo che comunichi con il server ACS e autentichi i client WebVPN.

1. Scegliere **Configurazione > VPN ad accesso remoto > Configurazione AAA > Gruppi di**

server AAA.

2. Fare clic su **Add** (Aggiungi) accanto a Gruppi di server AAA.
3. Nella finestra che viene visualizzata, specificare un nome per il nuovo gruppo di server AAA e scegliere **RADIUS** come protocollo. Al termine, fare clic su



OK.

4. Verificare che il nuovo gruppo sia selezionato nel riquadro superiore e fare clic su **Aggiungi** a destra del riquadro inferiore.
5. Fornire le informazioni sul server:
Nome interfaccia: l'interfaccia che l'ASA deve utilizzare per raggiungere il server ACS.
Nome server o indirizzo IP: l'indirizzo che l'ASA deve utilizzare per raggiungere il server ACS.
Server Secret Key: la chiave segreta condivisa configurata per l'ASA sul server ACS.
Esempio di configurazione del server AAA sull'appliance ASA

Server Group: RAD_SVR_GRP

Interface Name: inside

Server Name or IP Address: 192.168.1.2

Timeout: 10 seconds

RADIUS Parameters

Server Authentication Port: 1645

Server Accounting Port: 1646

Retry Interval: 10 seconds

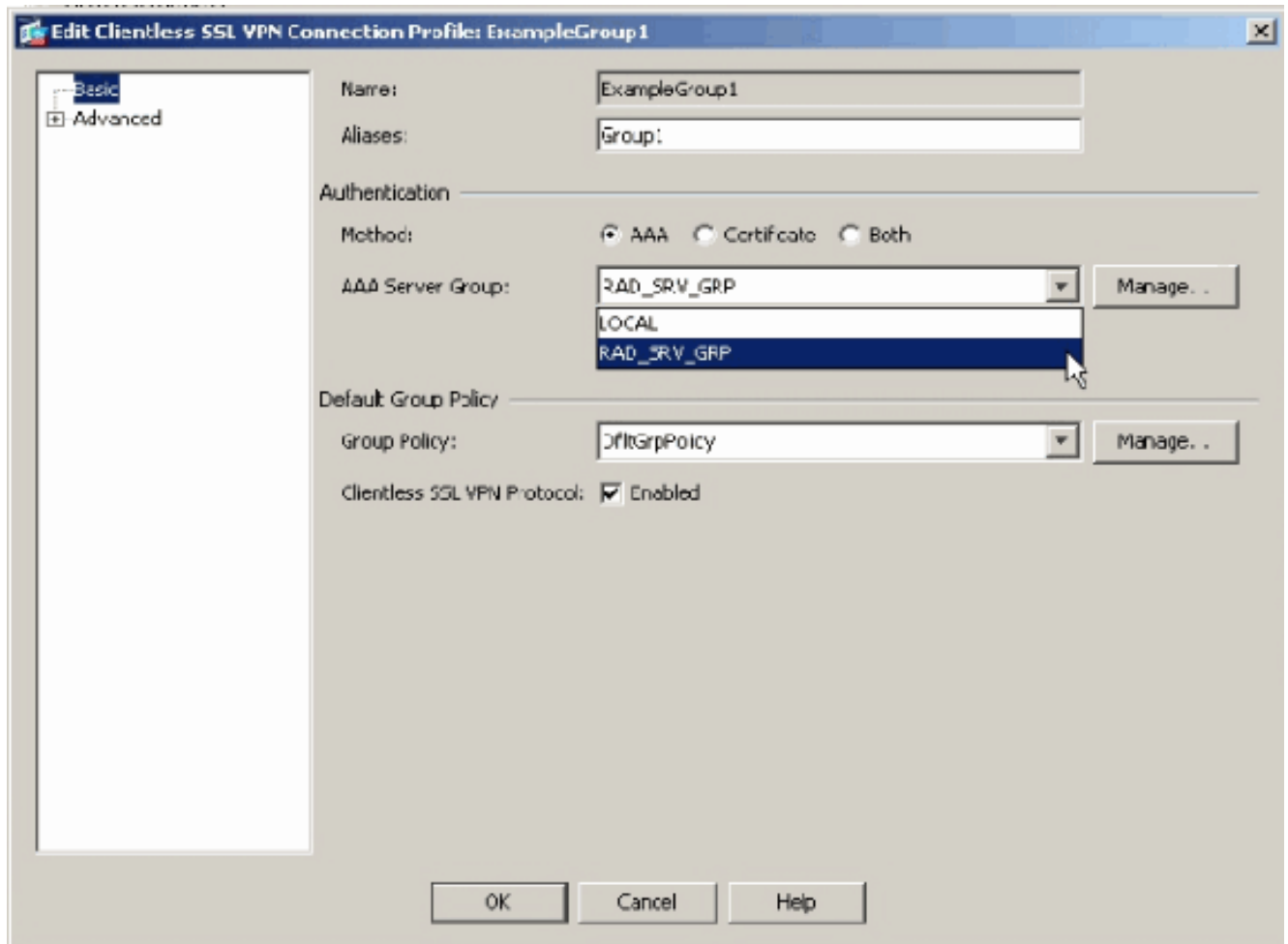
Server Secret Key: *****

Common Password:

ACL Netmask Convert: Standard

OK Cancel Help

6. Dopo aver configurato il gruppo di server e il server AAA, selezionare Configurazione > VPN ad accesso remoto > Accesso VPN SSL senza client > Profili di connessione per configurare WebVPN per l'utilizzo della nuova configurazione AAA. **Nota:** anche se in questo esempio viene utilizzata WebVPN, è possibile impostare qualsiasi profilo di connessione di accesso remoto (gruppo tunnel) per utilizzare questa configurazione AAA.
7. Selezionare il profilo per il quale configurare il server AAA e fare clic su **Modifica**.
8. In **Autenticazione** scegliere il gruppo di server RADIUS creato in precedenza. Al termine, fare clic su **OK**.



Interfaccia della riga di comando

Completare questa procedura nell'interfaccia della riga di comando (CLI) per configurare l'ASA in modo che comunichi con il server ACS e autentichi i client WebVPN.

```
ciscoasa#configure terminal
```

```
!--- Configure the AAA Server group. ciscoasa(config)# aaa-server RAD_SRV_GRP protocol RADIUS
ciscoasa(config-aaa-server-group)# exit !--- Configure the AAA Server. ciscoasa(config)# aaa-
server RAD_SRV_GRP (inside) host 192.168.1.2 ciscoasa(config-aaa-server-host)# key secretkey
ciscoasa(config-aaa-server-host)# exit !--- Configure the tunnel group to use the new AAA setup.
ciscoasa(config)# tunnel-group ExampleGroup1 general-attributes ciscoasa(config-tunnel-general)#
authentication-server-group RAD_SRV_GRP
```

Verifica

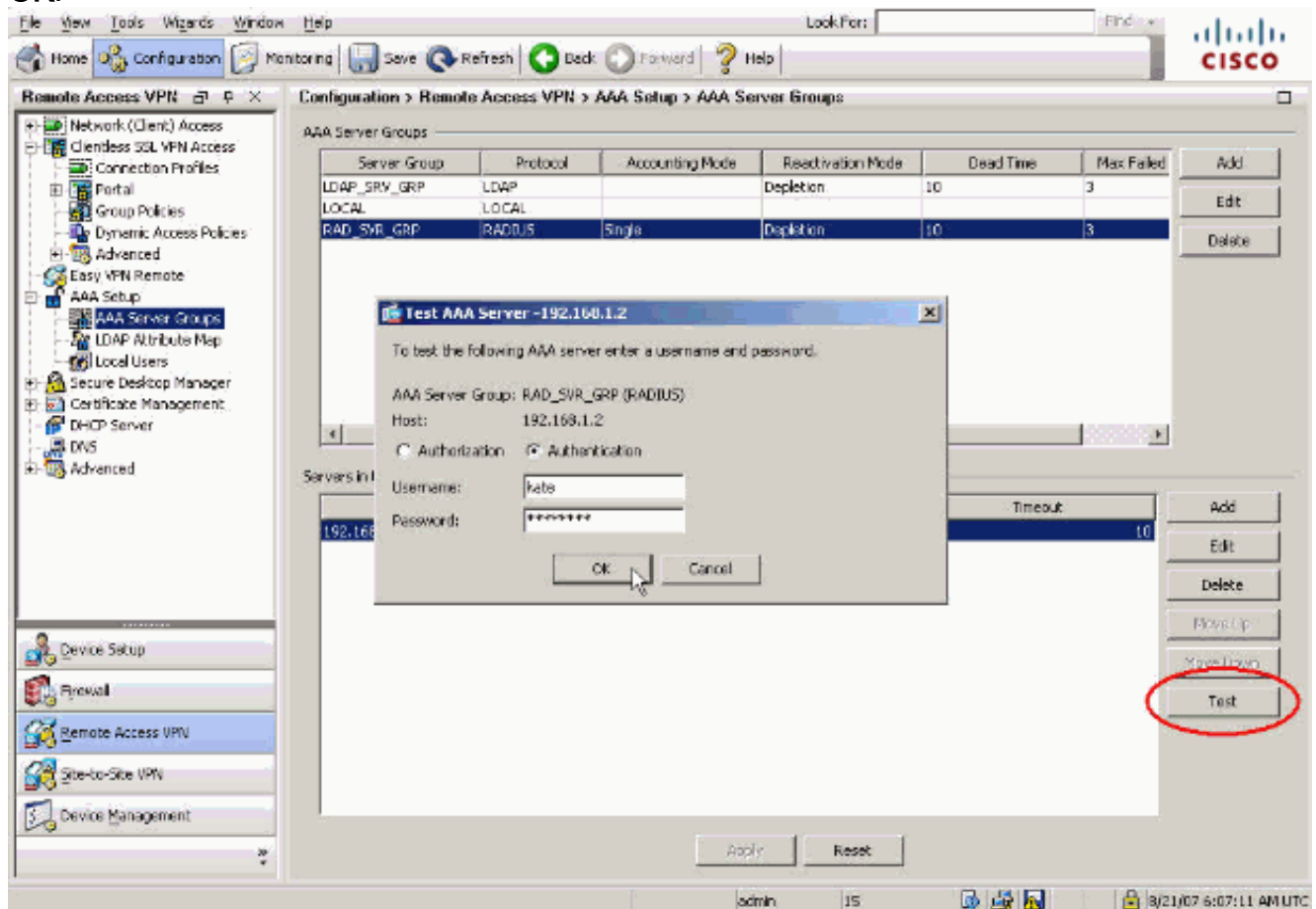
Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Test con ASDM

Verificare la configurazione RADIUS con il pulsante **Test** nella schermata di configurazione dei gruppi di server AAA. Dopo aver fornito un nome utente e una password, questo pulsante consente di inviare una richiesta di autenticazione di prova al server ACS.

1. Scegliere **Configurazione > VPN ad accesso remoto > Configurazione AAA > Gruppi di server AAA**.

2. Selezionare il gruppo di server AAA desiderato nel riquadro superiore.
3. Selezionare il server AAA che si desidera verificare nel riquadro inferiore.
4. Fare clic sul pulsante **Test** a destra del riquadro inferiore.
5. Nella finestra visualizzata fare clic sul pulsante di scelta **Autenticazione** e specificare le credenziali che si desidera verificare. Al termine, fare clic su **OK**.



6. Quando l'appliance ASA contatta il server AAA, viene visualizzato un messaggio di riuscita o



di errore.

Test con CLI

Per verificare la configurazione del server AAA, è possibile usare il comando **test** sulla riga di comando. Una richiesta di test viene inviata al server AAA e il risultato viene visualizzato sulla riga di comando.

```
ciscoasa#test aaa-server authentication RAD_SVR_GRP host 192.168.1.2 username kate password cisco123
```

```
INFO: Attempting Authentication test to IP address <192.168.1.2> (timeout: 12 seconds)
INFO: Authentication Successful
```

Risoluzione dei problemi

Il comando **debug radius** permette di risolvere i problemi di autenticazione in questo scenario. Questo comando abilita il debug della sessione RADIUS e la decodifica dei pacchetti RADIUS. In ciascun output di debug presentato, il primo pacchetto decodificato è il pacchetto inviato dall'ASA al server ACS. Il secondo pacchetto è la risposta del server ACS.

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

Quando l'autenticazione ha esito positivo, il server RADIUS invia un messaggio di **accettazione dell'accesso**.

```
ciscoasa#debug radius
```

```
!--- First Packet. Authentication Request. ciscoasa#radius mkreq: 0x88 alloc_rip 0xd5627ae4 new
request 0x88 --> 52 (0xd5627ae4) got user '' got password add_req 0xd5627ae4 session 0x88 id 52
RADIUS_REQUEST radius.c: rad_mkpkt RADIUS packet decode (authentication request) -----
----- Raw packet data (length = 62)..... 01 34 00 3e 18 71 56 d7 c4 ad e2 73
30 a9 2e cf | .4.>.qV....s0... 5c 65 3a eb 01 06 6b 61 74 65 02 12 0e c1 28 b7 |
\e:...kate....(. 87 26 ed be 7b 2c 7a 06 7c a3 73 19 04 06 c0 a8 | .&..{,z.|.s..... 01 01 05 06
00 00 00 34 3d 06 00 00 00 05 | .....4=..... Parsed packet data..... Radius: Code = 1 (0x01)
Radius: Identifier = 52 (0x34) Radius: Length = 62 (0x003E) Radius: Vector:
187156D7C4ADE27330A92ECF5C653AEB Radius: Type = 1 (0x01) User-Name Radius: Length = 6 (0x06)
Radius: Value (String) = 6b 61 74 65 | kate Radius: Type = 2 (0x02) User-Password Radius: Length
= 18 (0x12) Radius: Value (String) = 0e c1 28 b7 87 26 ed be 7b 2c 7a 06 7c a3 73 19 |
..(..&..{,z.|.s. Radius: Type = 4 (0x04) NAS-IP-Address Radius: Length = 6 (0x06) Radius: Value
(IP Address) = 192.168.1.1 (0xC0A80101) Radius: Type = 5 (0x05) NAS-Port Radius: Length = 6
(0x06) Radius: Value (Hex) = 0x34 Radius: Type = 61 (0x3D) NAS-Port-Type Radius: Length = 6
(0x06) Radius: Value (Hex) = 0x5 send pkt 192.168.1.2/1645 rip 0xd5627ae4 state 7 id 52
rad_vrfy() : response message verified rip 0xd544d2e8 : chall_state '' : state 0x7 : timer 0x0 :
reqauth: 18 71 56 d7 c4 ad e2 73 30 a9 2e cf 5c 65 3a eb : info 0x88 session_id 0x88 request_id
0x34 user 'kate' response '***' app 0 reason 0 skey 'secretkey' sip 192.168.1.2 type 1 !---
Second Packet. Authentication Response. RADIUS packet decode (response) -----
----- Raw packet data (length = 50)..... 02 34 00 32 35 a1 88 2f 8a bf 2a 14 c5 31 78
59 | .4.25...*..1xY 60 31 35 89 08 06 ff ff ff ff 19 18 43 41 43 53 | `15.....CACs 3a 30
2f 32 61 36 2f 63 30 61 38 30 31 30 31 2f | :0/2a6/c0a80101/ 35 32 | 52 Parsed packet data.....
Radius: Code = 2 (0x02) Radius: Identifier = 52 (0x34) Radius: Length = 50 (0x0032) Radius:
Vector: 35A1882F8ABF2A14C531785960313589 Radius: Type = 8 (0x08) Framed-IP-Address Radius:
Length = 6 (0x06) Radius: Value (IP Address) = 255.255.255.255 (0xFFFFFFFF) Radius: Type = 25
(0x19) Class Radius: Length = 24 (0x18) Radius: Value (String) = 43 41 43 53 3a 30 2f 32 61 36
2f 63 30 61 38 30 | CACS:0/2a6/c0a80 31 30 31 2f 35 32 | 101/52 rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT: normal termination
RADIUS_DELETE
remove_req 0xd5627ae4 session 0x88 id 52
free_rip 0xd5627ae4
radius: send queue empty
```

Se l'autenticazione non riesce, il server ACS invia un messaggio di **accesso-rifiuto**.

```
ciscoasa#debug radius
```

```
!--- First Packet. Authentication Request. ciscoasa# radius mkreq: 0x85 alloc_rip 0xd5627ae4 new
```



```

request 0x85 --> 49 (0xd5627ae4) got user '' got password add_req 0xd5627ae4 session 0x85 id 49
RADIUS_REQUEST radius.c: rad_mkpkt RADIUS packet decode (authentication request) -----
----- Raw packet data (length = 62)..... 01 31 00 3e 88 21 46 07 34 5d d2 a3
a0 59 1e ff | .1.>.!F.4]...Y.. cc 15 2a 1b 01 06 6b 61 74 65 02 12 60 eb 05 32 |
..*...kate..`.2 87 69 78 a3 ce d3 80 d8 4b 0d c3 37 04 06 c0 a8 | .ix.....K..7.... 01 01 05 06
00 00 00 31 3d 06 00 00 00 05 | .....1=..... Parsed packet data..... Radius: Code = 1 (0x01)
Radius: Identifier = 49 (0x31) Radius: Length = 62 (0x003E) Radius: Vector:
88214607345DD2A3A0591EFFCC152A1B Radius: Type = 1 (0x01) User-Name Radius: Length = 6 (0x06)
Radius: Value (String) = 6b 61 74 65 | kate Radius: Type = 2 (0x02) User-Password Radius: Length
= 18 (0x12) Radius: Value (String) = 60 eb 05 32 87 69 78 a3 ce d3 80 d8 4b 0d c3 37 |
`.2.ix.....K..7 Radius: Type = 4 (0x04) NAS-IP-Address Radius: Length = 6 (0x06) Radius: Value
(IP Address) = 192.168.1.1 (0xC0A80101) Radius: Type = 5 (0x05) NAS-Port Radius: Length = 6
(0x06) Radius: Value (Hex) = 0x31 Radius: Type = 61 (0x3D) NAS-Port-Type Radius: Length = 6
(0x06) Radius: Value (Hex) = 0x5 send pkt 192.168.1.2/1645 rip 0xd5627ae4 state 7 id 49
rad_vrfy() : response message verified rip 0xd544d2e8 : chall_state '' : state 0x7 : timer 0x0 :
reqauth: 88 21 46 07 34 5d d2 a3 a0 59 1e ff cc 15 2a 1b : info 0x85 session_id 0x85 request_id
0x31 user 'kate' response '***' app 0 reason 0 skey 'secretkey' sip 192.168.1.2 type 1 !---
Second packet. Authentication Response. RADIUS packet decode (response) -----
----- Raw packet data (length = 32)..... 03 31 00 20 70 98 50 af 39 cc b9 ba df a7 bd
ff | .1. p.P.9..... 06 af fb 02 12 0c 52 65 6a 65 63 74 65 64 0a 0d | .....Rejected.. Parsed
packet data..... Radius: Code = 3 (0x03) Radius: Identifier = 49 (0x31) Radius: Length = 32
(0x0020) Radius: Vector: 709850AF39CCB9BADFA7BDF06AFFB02 Radius: Type = 18 (0x12) Reply-Message
Radius: Length = 12 (0x0C) Radius: Value (String) =
52 65 6a 65 63 74 65 64 0a 0d | Rejected..
rad_procpkt: REJECT
RADIUS_DELETE
remove_req 0xd5627ae4 session 0x85 id 49
free_rip 0xd5627ae4
radius: send queue empty

```

[Informazioni correlate](#)

- [RADIUS \(Remote Authentication Dial-In User Service\)](#)
- [RFC \(Requests for Comments\)](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)