

ASA 8.0: RADIUS-verificatie voor WebVPN-gebruikers configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[De ACS-server configureren](#)

[De security applicatie configureren](#)

[ASDM](#)

[Opdrachtlijn-interface](#)

[Verifiëren](#)

[Test met ASDM](#)

[Test met CLI](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document demonstreert hoe u de Cisco adaptieve security applicatie (ASA) kunt configureren om een RADIUS-server (Dial-In User Service) op afstand te gebruiken voor verificatie van WebVPN-gebruikers. De RADIUS-server in dit voorbeeld is een Cisco Access Control Server (ACS) server, versie 4.1 Deze configuratie wordt uitgevoerd met Adaptieve Security Devices Manager (ASDM) 6.0(2) op een ASA die softwareversie 8.0(2) uitvoert.

Opmerking: In dit voorbeeld is de RADIUS-verificatie ingesteld voor WebVPN-gebruikers, maar deze configuratie kan ook worden gebruikt voor andere typen VPN-toegang op afstand. U kunt de AAA-servergroep gewoon toewijzen aan het gewenste verbindingsprofiel (tunnelgroep) zoals wordt weergegeven.

[Voorwaarden](#)

- Een basisconfiguratie voor Webex is vereist.
- Cisco ACS moet gebruikers voor gebruikersverificatie hebben geconfigureerd. Raadpleeg het gedeelte [Een basisgebruikersaccount](#) toevoegen van [gebruikersbeheer](#) voor meer informatie.

[De ACS-server configureren](#)

In deze sectie, wordt u voorgesteld met de informatie om de authenticatie van RADIUS op ACS en ASA te configureren.

Voltooi deze stappen om de ACS server te configureren om te communiceren met de ASA.

1. Kies **Netwerkconfiguratie** in het linkermenu van het ACS-scherm.
2. Kies **Indeling toevoegen** onder **AAA-clients**.
3. Geef de clientinformatie op:**AAA-clientnaam** - een naam naar keuze**AAA client-IP-adres**: het adres waar het beveiligingsapparaat contact met de ACS opneemt**Gedeeld geheim** - een geheime sleutel die op ACS en op het veiligheidsapparaat is ingesteld
4. In de optie **Verificeren met verwijdering** kiest u **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**.
5. Klik op **Inzenden+Toepassen**.

Bijvoorbeeld AAA-clientconfiguratie

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:

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

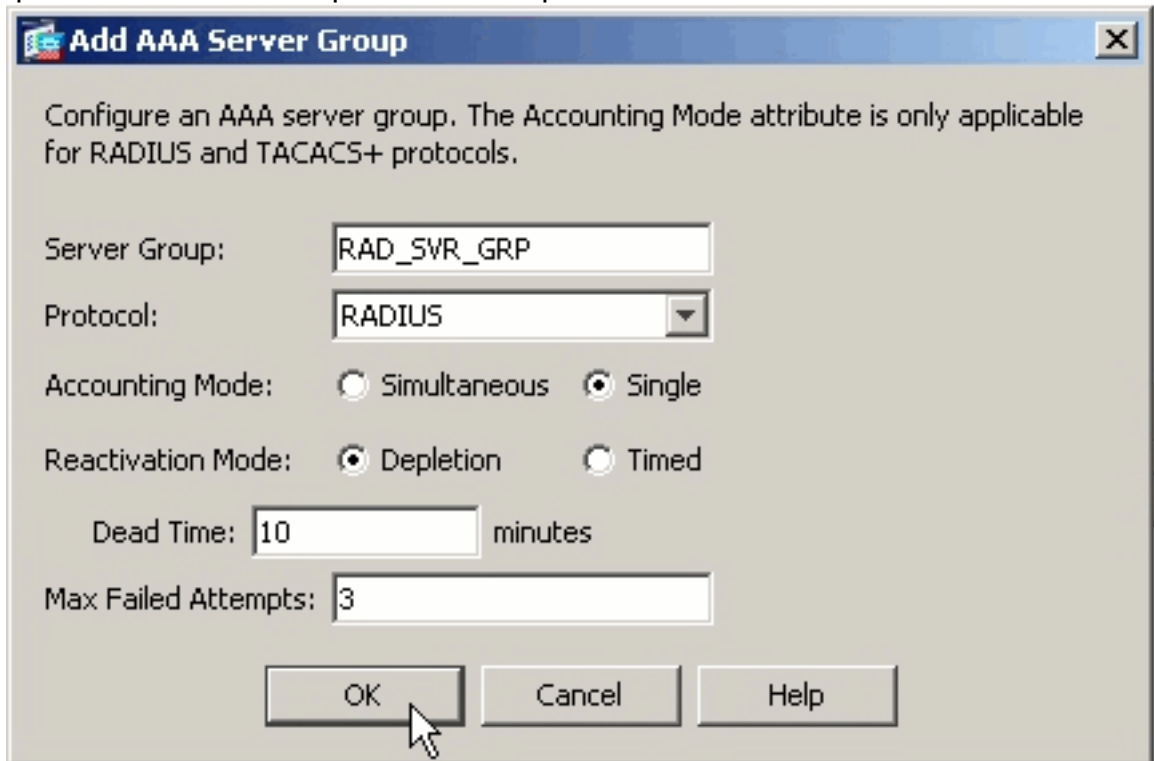
[De security applicatie configureren](#)

[ASDM](#)

Voltooi deze stappen in de ASDM om de ASA te vormen om met de ACS server te communiceren en WebVPN cliënten te authentifieren.

1. Kies **Configuration > Remote Access VPN > AAA-instelling > AAA-servergroepen**.
2. Klik op **Add** naast AAA-servergroepen.

3. Specificeer in het venster dat nu wordt weergegeven een naam voor de nieuwe AAA-servergroep en kies **RADIUS** als protocol. Klik op **OK** na



Configure an AAA server group. The Accounting Mode attribute is only applicable for RADIUS and TACACS+ protocols.

Server Group: RAD_SVR_GRP

Protocol: RADIUS

Accounting Mode: Simultaneous Single

Reactivation Mode: Depletion Timed

Dead Time: 10 minutes

Max Failed Attempts: 3

OK Cancel Help

voltooiing.

4. Zorg dat uw nieuwe groep in het bovenste venster is geselecteerd en klik op **Toevoegen** aan de rechterkant van het onderste venster.
5. Geef de serverinformatie op:
Naam interface-de interface die ASA moet gebruiken om de ACS-server te bereiken
Server Naam of IP adres-het adres dat ASA moet gebruiken om de ACS server te bereiken
Beheerde sleutel van de server - de gedeelde geheime sleutel die voor de ASA op de ACS-server is ingesteld
Bijvoorbeeld AAA-serverconfiguratie voor de ASA

Add AAA Server

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

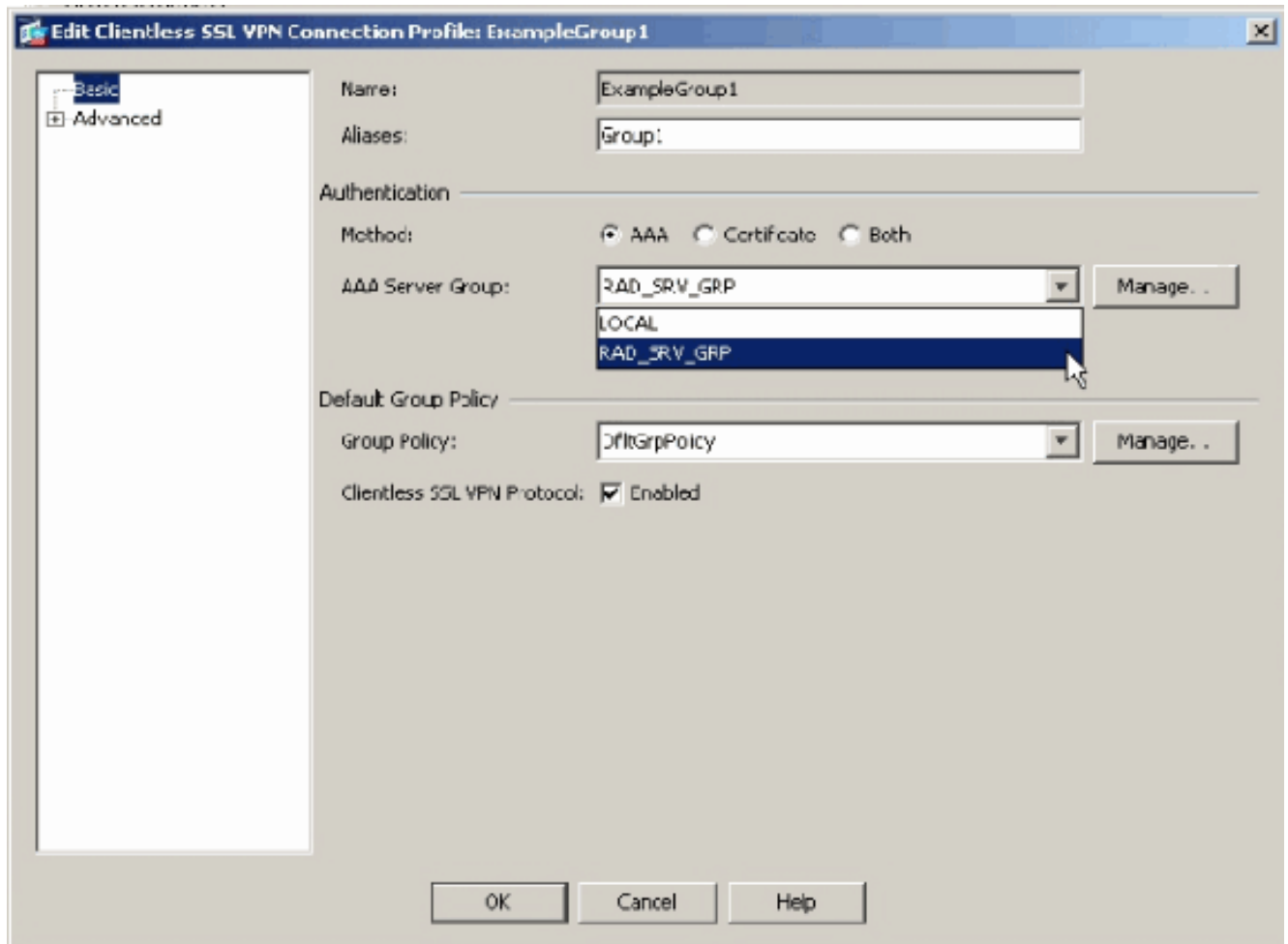
Server Secret Key: *****

Common Password:

ACL Netmask Convert: Standard

OK Cancel Help

6. Nadat u de AAA-servergroep en -server hebt ingesteld, navigeer dan naar Configuration > Remote Access VPN > Clientloze SSL VPN Access > Connection Profiles om WebVPN te configureren voor gebruik van de nieuwe AAA-configuratie. **Opmerking:** Hoewel dit voorbeeld WebVPN gebruikt, kunt u elk afstandstoegangsprofiel (tunnelgroep) instellen om deze AAA-instelling te gebruiken.
7. Kies het profiel waarvoor u AAA wilt configureren en klik op **Bewerken**.
8. Onder **Verificatie** kies de RADIUS-servergroep die u eerder hebt gemaakt. Klik op **OK** na voltooiing.



Opdrachtlijn-interface

Voltooi deze stappen in de interface van de opdrachtregel (CLI) om de ASA te configureren om met de ACS-server te communiceren en WebVPN-clients te echt maken.

```
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
```

Verifiëren

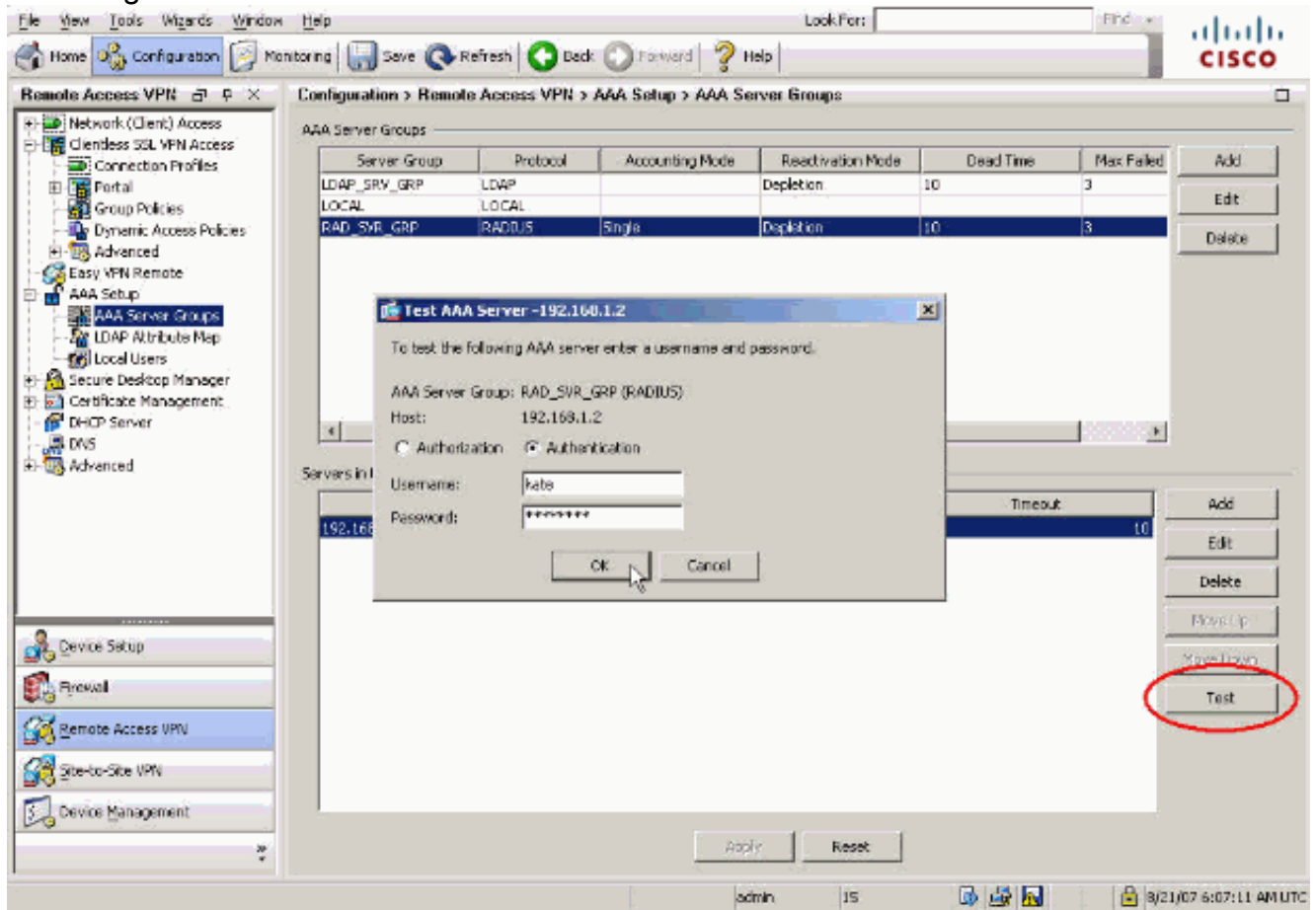
Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Test met ASDM

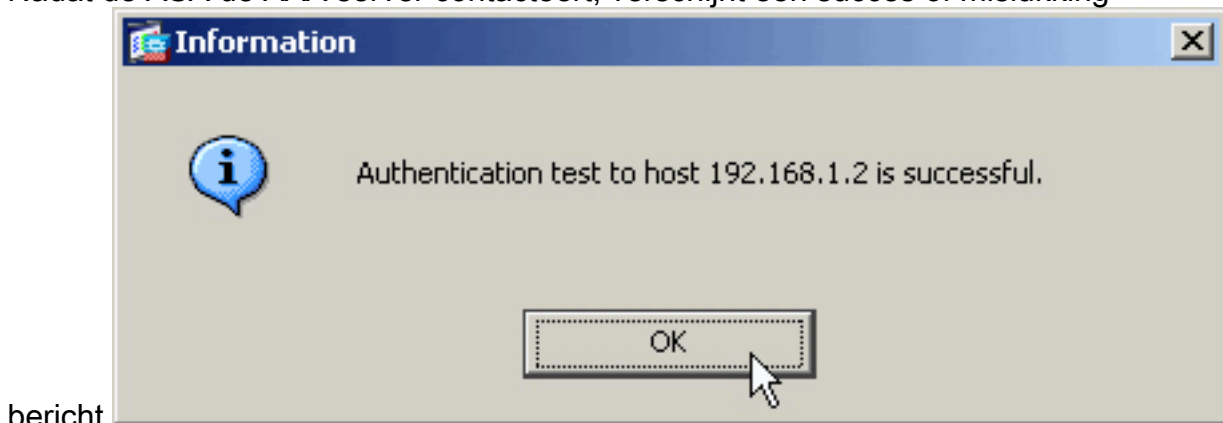
Controleer de RADIUS-configuratie met de **Test**-knop op het configuratiescherm van AAA-servergroepen. Zodra u een gebruikersnaam en wachtwoord hebt opgegeven, kunt u met deze knop een verzoek om verificatie naar de ACS-server sturen.

1. Kies **Configuration > Remote Access VPN > AAA-instelling > AAA-servergroepen**.
2. Selecteer uw gewenste AAA-servergroep in het bovenste venster.

3. Selecteer de AAA-server die u in het onderste venster wilt testen.
4. Klik op de knop **Test** rechts in het ondervenster.
5. Klik in het venster dat verschijnt op het radioknop **Verificatie** en specificeer de referenties waarmee u wilt testen. Klik op **OK** na voltooiing.



6. Nadat de ASA de AAA server contacteert, verschijnt een succes of mislukking



bericht.

Test met CLI

U kunt de testopdracht in de opdrachtregel gebruiken om de AAA-instelling te testen. Een testverzoek wordt naar de AAA server verzonden, en het resultaat verschijnt op de opdrachtregel.

```
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
```

Problemen oplossen

De opdracht **straal** debug kan u helpen bij het oplossen van problemen in dit scenario. Met deze opdracht kunnen RADIUS-sessies worden gestart, evenals RADIUS-pakketdecodering. In elke gepresenteerde debug uitvoer is het eerste pakket gedecodeerd het pakket dat van de ASA naar de ACS server wordt verzonden. Het tweede pakket is de reactie van de ACS-server.

Opmerking: Raadpleeg [Belangrijke informatie over debug Commands](#) voordat u debug-opdrachten gebruikt.

Wanneer verificatie succesvol is, verstuurt de RADIUS-server een **toegangsacceptabel** bericht.

```
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
```

Wanneer de verificatie faalt, verstuurt de ACS-server een **toegangsverwerp**-bericht.

```
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

```

[Gerelateerde informatie](#)

- [Inbelservice voor externe verificatie \(RADIUS\)](#)
- [Verzoeken om opmerkingen \(RFC's\)](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)