

# ASA 8.0: Konfigurieren der RADIUS-Authentifizierung für WebVPN-Benutzer

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Konfigurieren des ACS-Servers](#)

[Konfigurieren der Sicherheits-Appliance](#)

[ASDM](#)

[Befehlszeilenschnittstelle](#)

[Überprüfen](#)

[Test mit ASDM](#)

[Test mit CLI](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## [Einführung](#)

Dieses Dokument veranschaulicht, wie die Cisco Adaptive Security Appliance (ASA) so konfiguriert wird, dass sie einen RADIUS-Server (Remote Authentication Dial-In User Service) für die Authentifizierung von WebVPN-Benutzern verwendet. Der RADIUS-Server in diesem Beispiel ist ein Cisco Access Control Server (ACS)-Server, Version 4.1 Diese Konfiguration wird mit dem Adaptive Security Device Manager (ASDM) 6.0(2) auf einer ASA ausgeführt, die die Software Version 8.0(2) ausführt.

**Hinweis:** In diesem Beispiel wird die RADIUS-Authentifizierung für WebVPN-Benutzer konfiguriert. Diese Konfiguration kann jedoch auch für andere VPN-Typen für den Remote-Zugriff verwendet werden. Weisen Sie einfach die AAA-Servergruppe dem gewünschten Verbindungsprofil (Tunnelgruppe) wie gezeigt zu.

## [Voraussetzungen](#)

- Eine grundlegende WebVPN-Konfiguration ist erforderlich.
- Für den Cisco ACS müssen Benutzer für die Benutzerauthentifizierung konfiguriert sein. Weitere Informationen finden Sie im Abschnitt [Hinzufügen eines einfachen Benutzerkontos](#) im [Bereich Benutzerverwaltung](#).

## [Konfigurieren des ACS-Servers](#)

In diesem Abschnitt werden die Informationen zur Konfiguration der RADIUS-Authentifizierung auf dem ACS und der ASA angezeigt.

Führen Sie diese Schritte aus, um den ACS-Server für die Kommunikation mit der ASA zu konfigurieren.

1. Wählen Sie im linken Menü des ACS-Bildschirms **Network Configuration** (Netzwerkkonfiguration) aus.
2. Wählen Sie **Add Entry (Eintrag hinzufügen)** unter **AAA Clients** aus.
3. Geben Sie die Kundeninformationen an:**AAA-Client-Hostname** - ein Name Ihrer Wahl**AAA-Client-IP-Adresse** - die Adresse, von der die Sicherheits-Appliance den ACS kontaktiert**Shared Secret** - ein geheimer Schlüssel, der auf dem ACS und der Sicherheits-Appliance konfiguriert ist.
4. Wählen Sie im Dropdown-Menü **Authenticate Using (Authentifizierung mithilfe)** die Option **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**.
5. Klicken Sie auf **Senden+Übernehmen**.

### Beispiel für eine AAA-Client-Konfiguration

**Network Configuration**

**Add AAA Client**

AAA Client Hostname: asa5505

AAA Client IP Address: 192.168.1.1

Shared Secret: secretkey

**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

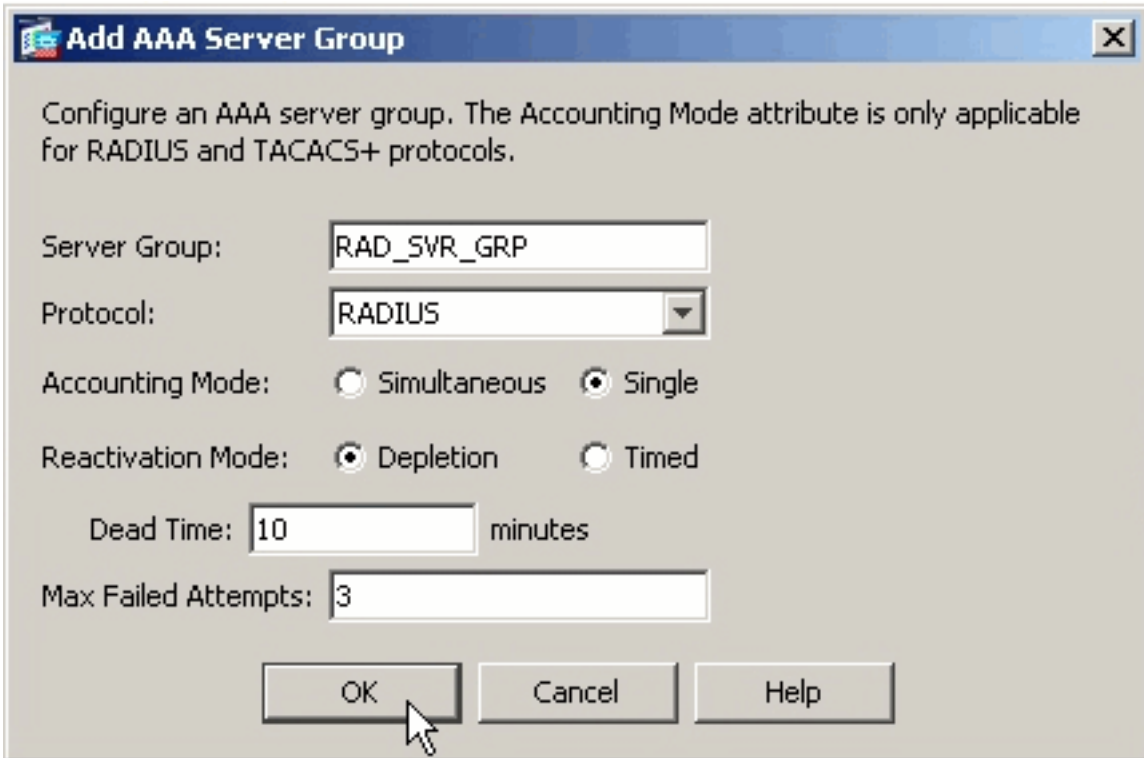
Match Framed-IP-Address with user IP address for accounting packets from

## [Konfigurieren der Sicherheits-Appliance](#)

### [ASDM](#)

Führen Sie diese Schritte im ASDM aus, um die ASA für die Kommunikation mit dem ACS-Server und die Authentifizierung von WebVPN-Clients zu konfigurieren.

1. Wählen Sie **Configuration > Remote Access VPN > AAA Setup > AAA Server Groups** aus.
2. Klicken Sie neben AAA-Servergruppen auf **Hinzufügen**.
3. Geben Sie im angezeigten Fenster einen Namen für die neue AAA-Servergruppe an, und wählen Sie **RADIUS** als Protokoll aus. Klicken Sie abschließend auf



OK.

4. Stellen Sie sicher, dass Ihre neue Gruppe im oberen Teilfenster ausgewählt ist, und klicken Sie rechts im unteren Teilfenster auf **Hinzufügen**.
5. Geben Sie die Serverinformationen an: **Schnittstellename** - die Schnittstelle, die die ASA verwenden muss, um den ACS-Server zu erreichen. **Servername oder IP-Adresse** - die Adresse, die die ASA verwenden muss, um den ACS-Server zu erreichen. **Server Secret Key** (geheimer **Schlüssel** für den **Server**) - der gemeinsam genutzte geheime Schlüssel, der für die ASA auf dem ACS-Server konfiguriert wurde. **Beispiel für eine AAA-Serverkonfiguration auf der 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

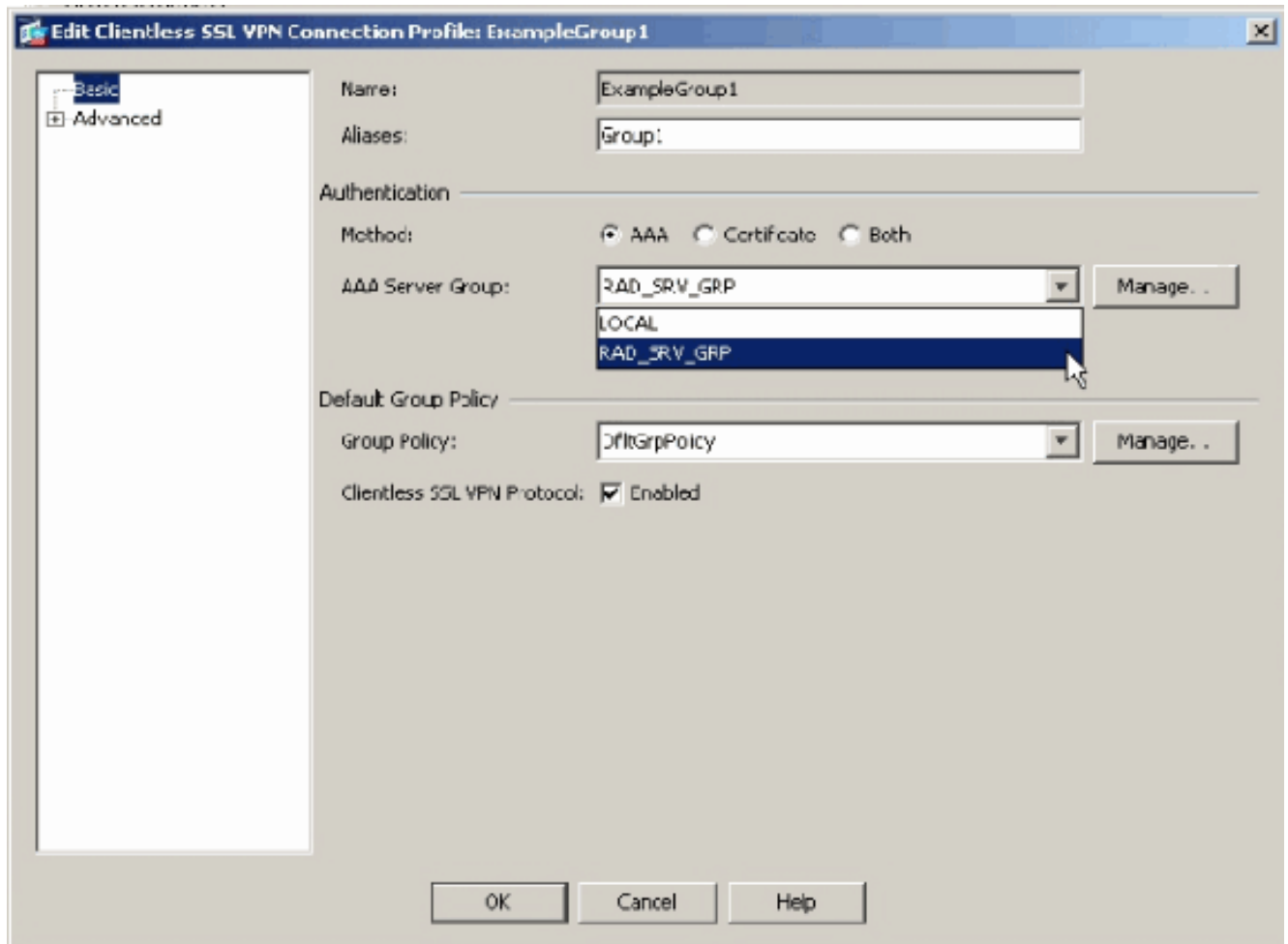
Server Secret Key: \*\*\*\*\*

Common Password:

ACL Netmask Convert: Standard

OK Cancel Help

6. Wenn Sie die AAA-Servergruppe und den -Server konfiguriert haben, navigieren Sie zu Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles, um WebVPN für die Verwendung der neuen AAA-Konfiguration zu konfigurieren. **Hinweis:** Obwohl in diesem Beispiel WebVPN verwendet wird, können Sie jedes Verbindungsprofil für den Remote-Zugriff (Tunnelgruppe) so einrichten, dass es diese AAA-Einrichtung verwendet.
7. Wählen Sie das Profil aus, für das Sie AAA konfigurieren möchten, und klicken Sie auf **Bearbeiten**.
8. Wählen Sie unter **Authentifizierung** die zuvor erstellte RADIUS-Servergruppe aus. Klicken Sie abschließend auf **OK**.



## Befehlszeilenschnittstelle

Führen Sie diese Schritte in der Befehlszeilenschnittstelle (CLI) aus, um die ASA für die Kommunikation mit dem ACS-Server und die Authentifizierung von WebVPN-Clients zu konfigurieren.

```
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
```

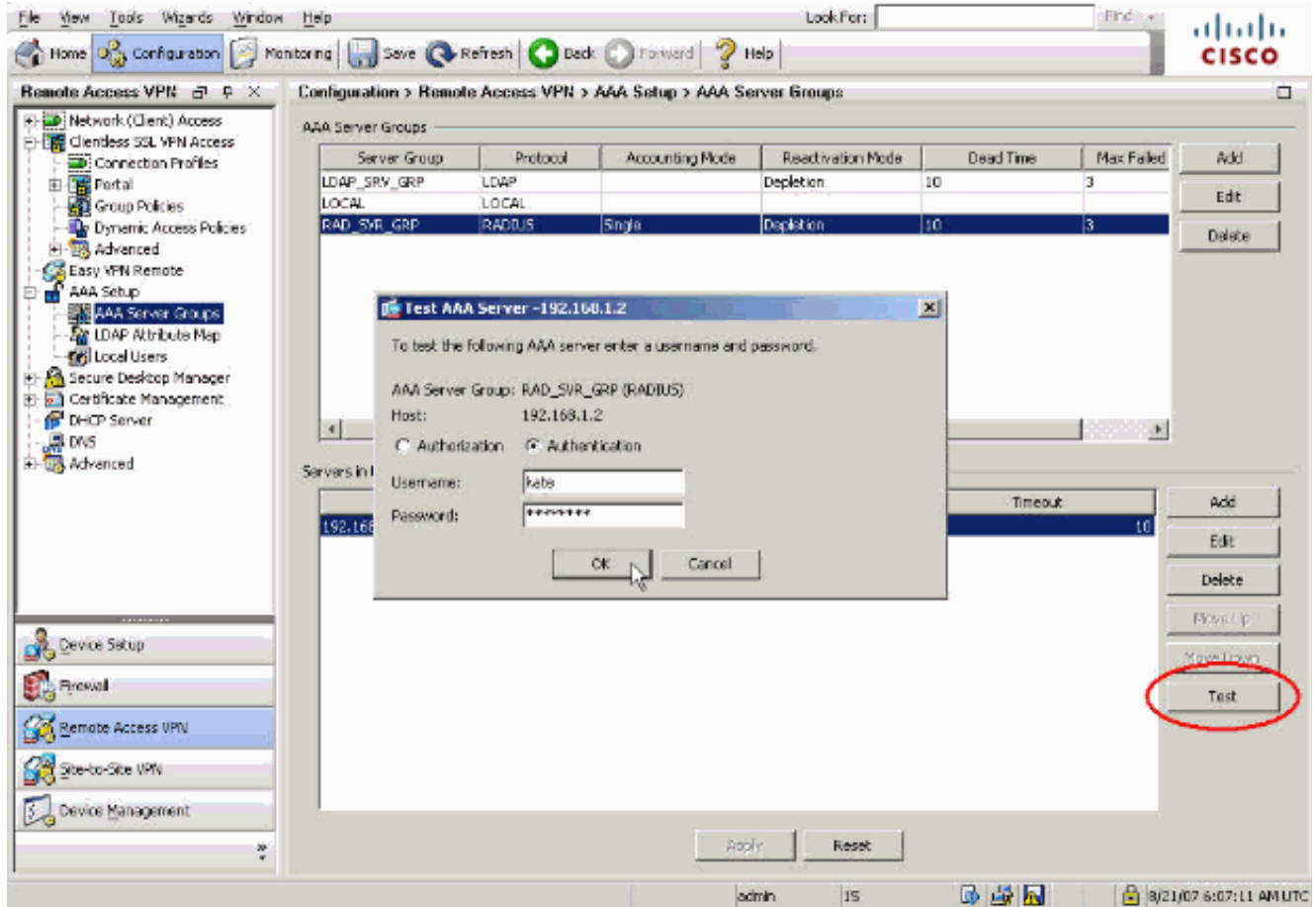
## Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

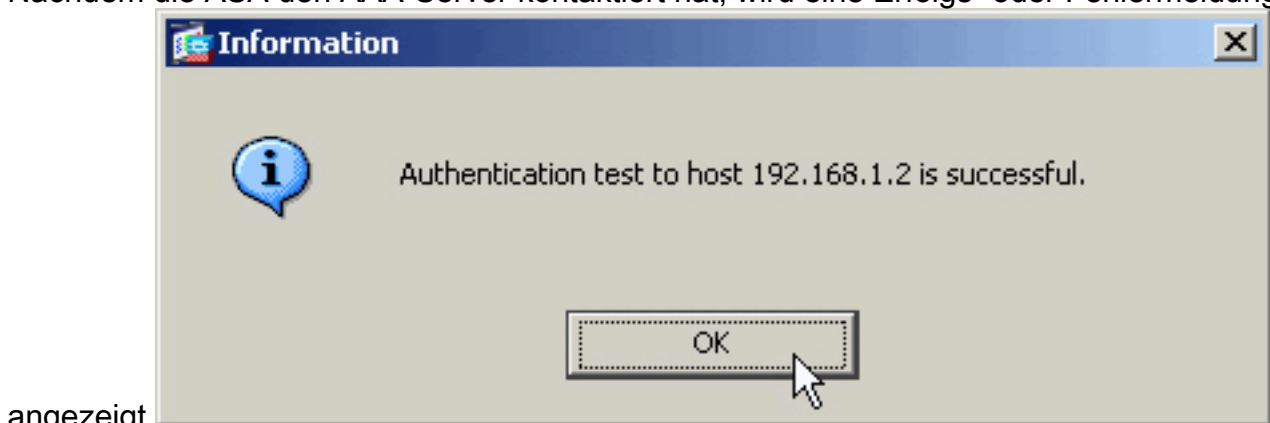
## Test mit ASDM

Überprüfen Sie Ihre RADIUS-Konfiguration mit der Schaltfläche **Test** im Konfigurationsbildschirm AAA-Servergruppen. Sobald Sie einen Benutzernamen und ein Kennwort eingegeben haben, können Sie über diese Schaltfläche eine Testauthentifizierungsanfrage an den ACS-Server senden.

1. Wählen Sie **Configuration > Remote Access VPN > AAA Setup > AAA Server Groups** aus.
2. Wählen Sie im oberen Teilfenster die gewünschte AAA-Servergruppe aus.
3. Wählen Sie im unteren Bereich den AAA-Server aus, den Sie testen möchten.
4. Klicken Sie auf die Schaltfläche **Test** rechts neben dem unteren Bereich.
5. Klicken Sie im sich öffnenden Fenster auf das Optionsfeld **Authentifizierung** und geben Sie die Anmeldeinformationen an, mit denen Sie testen möchten. Klicken Sie abschließend auf **OK**.



6. Nachdem die ASA den AAA-Server kontaktiert hat, wird eine Erfolgs- oder Fehlermeldung



angezeigt.

## Test mit CLI

Sie können den **Test**-Befehl in der Befehlszeile verwenden, um Ihre AAA-Konfiguration zu testen. Eine Testanforderung wird an den AAA-Server gesendet, und das Ergebnis wird in der Befehlszeile angezeigt.

```
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

## Fehlerbehebung

Der Befehl **debug radius** kann Ihnen helfen, Authentifizierungsprobleme in diesem Szenario zu beheben. Dieser Befehl ermöglicht das Debuggen von RADIUS-Sitzungen sowie die RADIUS-Paketdekodierung. Bei jeder angegebenen Debugausgabe ist das erste dekodierte Paket das Paket, das von der ASA an den ACS-Server gesendet wird. Das zweite Paket ist die Antwort vom ACS-Server.

**Hinweis:** Beachten Sie [vor der](#) Verwendung von **Debug**-Befehlen die [Informationen](#) zu [Debug-Befehlen](#).

Wenn die Authentifizierung erfolgreich ist, sendet der RADIUS-Server eine Meldung zur Annahme des Zugriffs.

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
```

Wenn die Authentifizierung fehlschlägt, sendet der ACS-Server eine Meldung zur Ablehnung des Zugriffs.



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
```

## [Zugehörige Informationen](#)

- [RADIUS \(Remote Authentication Dial-In User Service\)](#)
- [Anforderungen für Kommentare \(RFCs\)](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)