

Het verkrijgen van versie en AAA debug informatie voor Cisco Secure ACS voor Windows

Inhoud

[Inleiding](#)

[Voordat u begint](#)

[Conventies](#)

[Voorwaarden](#)

[Gebruikte componenten](#)

[Informatie over Cisco Secure voor Windows versie verkrijgen](#)

[De DOS-opdrachtregel gebruiken](#)

[De GUI gebruiken](#)

[Cisco Secure ACS instellen voor Windows-afvoerniveaus](#)

[Hoe het Logging-niveau in de ACS-GUI volledig instellen](#)

[Hoe stelt u Dr. Watson Logging in](#)

[Een pakket.taxi-bestand maken](#)

[Wat is het pakket.taxi?](#)

[Een bestand met een pakket.cab maken met het hulpprogramma CSSSupport.exe](#)

[Een pakket.cab-bestand handmatig verzamelen](#)

[Cisco Secure voor Windows NT AAA-debug informatie verkrijgen](#)

[Informatie over debug van Cisco Secure voor Windows NT AAA-replicatie verkrijgen](#)

[Verificatie door gebruiker offline testen](#)

[Redenen voor Windows 2000/NT Database-fouten bepalen](#)

[Voorbeelden](#)

[RADIUS-goede verificatie](#)

[RADIUS-slechte verificatie](#)

[TACACS+ goede verificatie](#)

[TACACS+ slechte verificatie \(samengevat\)](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document legt uit hoe u de Cisco Secure ACS voor Windows versie kunt bekijken en hoe u verificatie, autorisatie en accounting (AAA) kunt instellen en verkrijgen.

[Voordat u begint](#)

[Conventies](#)

Zie de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

Voorwaarden

Er zijn geen specifieke voorwaarden van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Secure ACS voor Windows 2.6.

Informatie over Cisco Secure voor Windows versie verkrijgen

U kunt versieinformatie bekijken door de DOC-opdrachtregel te gebruiken of door de GUI te gebruiken.

De DOS-opdrachtregel gebruiken

Als u het versienummer van Cisco Secure ACS voor Windows via de opdrachtregel in DOS wilt bekijken, gebruikt u **functies** of **Straal** gevolgd door de **-v** voor RADIUS en **-x** voor TACACS+. Zie de onderstaande voorbeelden:

```
C:\Program Files\CiscoSecure ACS v2.6\CSTacacs>cstacacs -s  
CSTacacs v2.6.2, Copyright 2001, Cisco Systems Inc
```

```
C:\Program Files\CiscoSecure ACS v2.6\CSRADIUS>csradius -v  
CSTacacs v2.6.2), Copyright 2001, Cisco Systems Inc
```

U kunt ook het versienummer van het Cisco Secure ACS-programma in het Windows-register zien. Bijvoorbeeld:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAAv2.1\CSAuth]  
Version=2.6(2)
```

De GUI gebruiken

Om de versie met de Cisco Secure ACS GUI te bekijken, gaat u naar de ACS-startpagina. U kunt dit op elk moment doen door te klikken op het Cisco Systems-logo in de linker bovenhoek van het scherm. De onderste helft van de startpagina geeft de volledige versie weer.

Cisco Secure ACS instellen voor Windows-afvoerniveaus


Het volgende is een uitleg van de verschillende opties voor het debuggen die nodig zijn om de maximale zuiveringsinformatie te krijgen.

Hoe het Logging-niveau in de ACS-GUI volledig instellen


U moet ACS instellen om alle berichten te loggen. Volg daartoe de onderstaande stappen:

1. Ga vanuit de startpagina ACS naar **Systems Configuration > Service Control**.
2. Stel onder de optie Service Log File Configuration het detailniveau in op **volledig**. U kunt de secties Generate New File en Manager indien nodig

System Configuration

CiscoSecure ACS on mhammon-pc 

Is Currently Running

Services Log File Configuration 

Level of detail

None

Low

Full

Generate New File

Every day

Every week

Every month

When size is greater than KB

Manage Directory

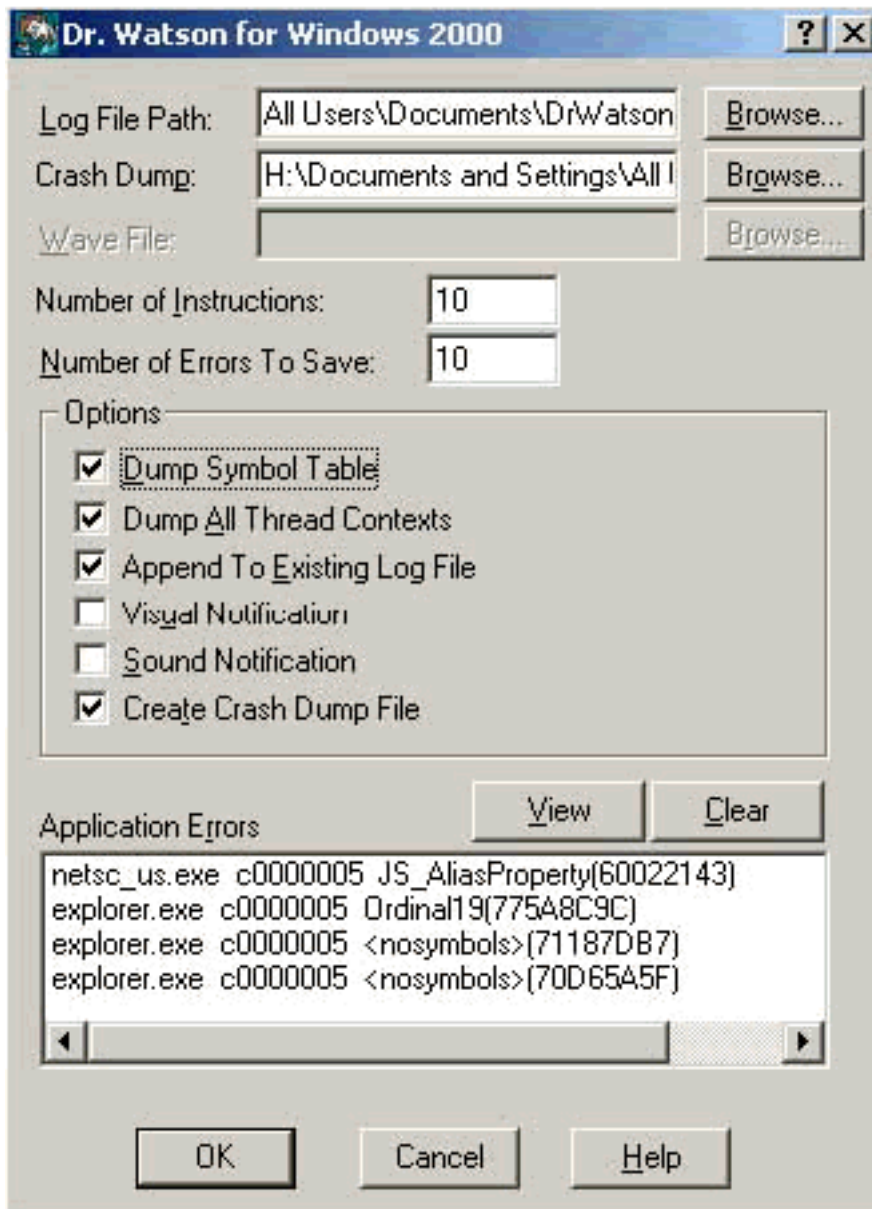
Keep only the last files

Delete files older than days

wijzigen.

[Hoe stelt u Dr. Watson Logging in](#)

In het opdrachtprompt type **drwtsn32** en het Dr. Watson venster verschijnt. Controleer of de opties voor **pomp** voor **alle draadcontexten** en **tabel met het symbool van de pomp** zijn ingeschakeld.



[Een pakket.taxi-bestand maken](#)

[Wat is het pakket.taxi?](#)

The Packet.cab is een Zip-bestand dat alle benodigde bestanden bevat om de ACS-bestanden efficiënt te kunnen oplossen. U kunt de voorziening CSSsupport.exe gebruiken om het pakket.cab te maken, of u kunt [de bestanden handmatig verzamelen](#).

[Een bestand met een pakket.cab maken met het hulpprogramma CSSSupport.exe](#)

Als u een ACS-probleem hebt waarvoor u informatie moet verzamelen, voert u het bestand CSSsupport.exe zo snel mogelijk uit nadat u het probleem hebt gezien. Gebruik de DOS-opdrachtregel voor Windows Verkenner GUI om CSS-ondersteuning uit C:\program files\Cisco Secure ACS v2.6\Utils>CSS Support.exe te uitvoeren.

Wanneer u het bestand CSSsupport.exe uitvoert, verschijnt het volgende venster.



Van dit scherm hebt u twee belangrijke opties:

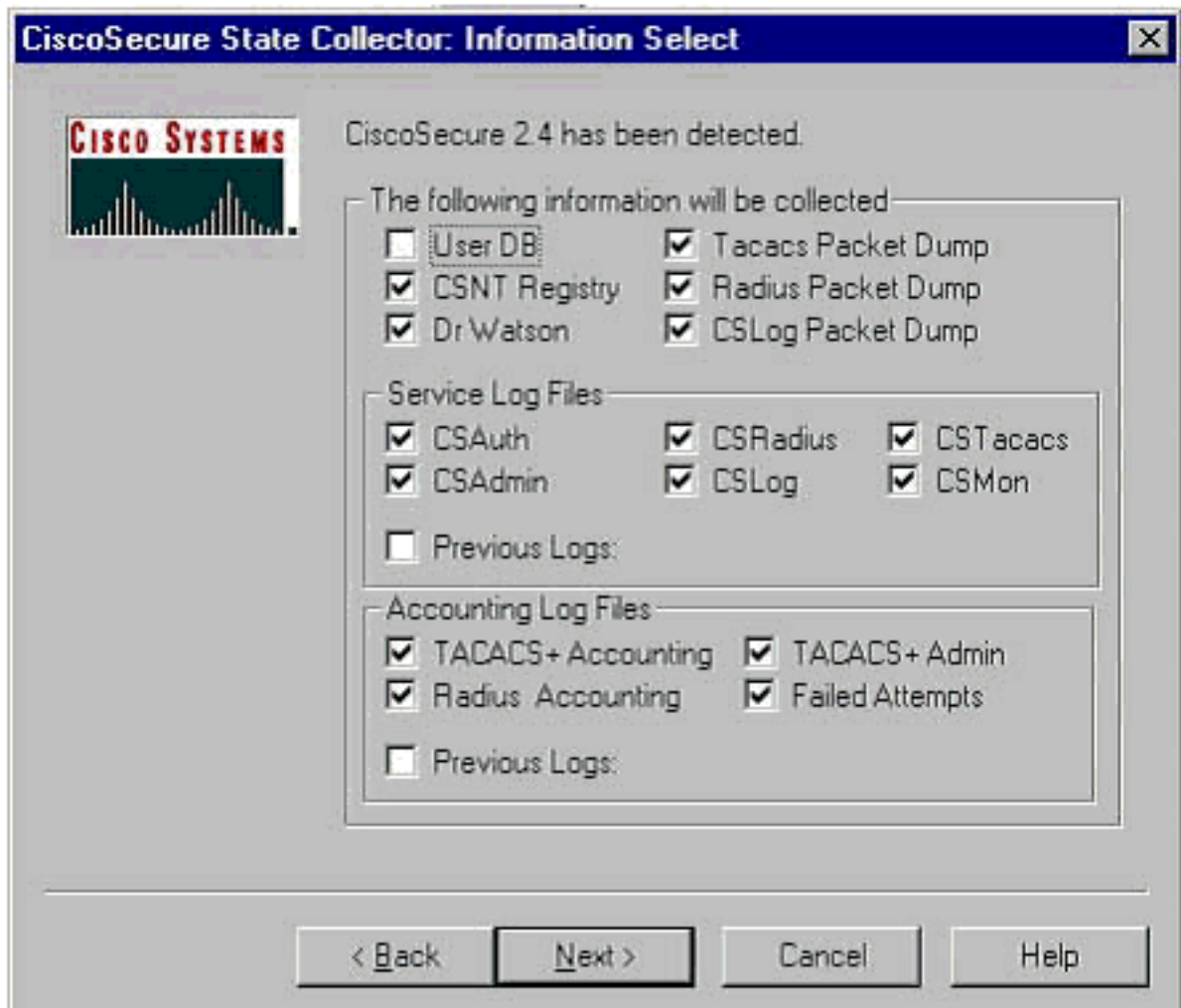
- [Draai de wizard](#), die u in vier stappen voert: Cisco Secure State Collector: Selectie informatie Cisco Secure State Collector: Installatieselectie Cisco Secure State Collector: Logversie Cisco Secure State Collector (de eigenlijke verzameling) of
- [Stel alleen het niveau voor Log in](#), zodat u de eerste stappen kunt overslaan en direct naar de Cisco Secure State Collector kunt gaan: Scherm met inlogversie

Selecteer de **Wizard uitvoeren** om door de stappen te gaan die nodig zijn om het logbestand in te stellen. Na de eerste instelling kunt u de optie **Alleen logniveaus instellen** om de logniveaus aan te passen. Maak uw selectie en klik op **Volgende**.

[Wizard uitvoeren](#)

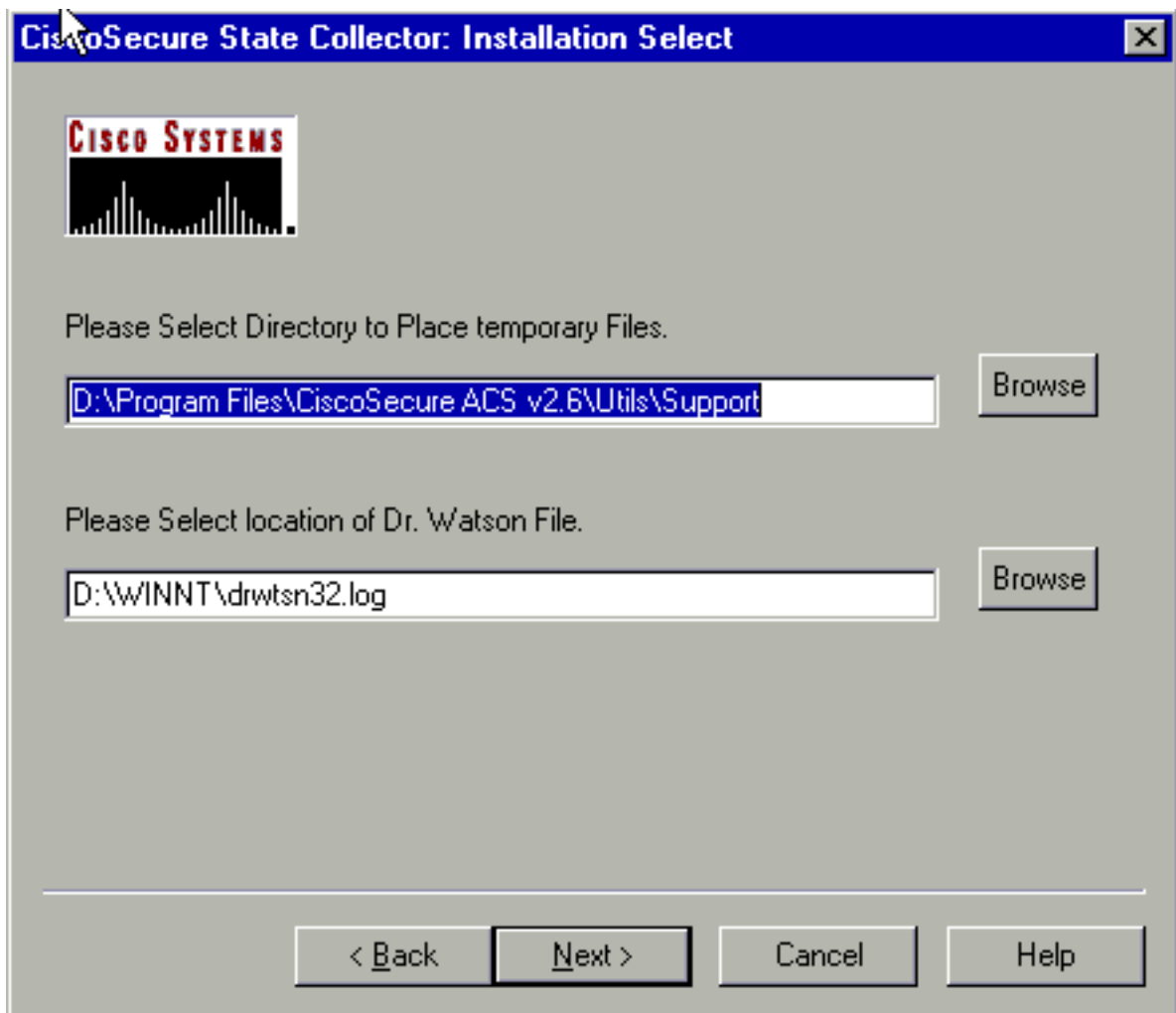
Hieronder wordt uitgelegd hoe u informatie kunt selecteren met de optie Wizard uitvoeren.

1. **Cisco Secure State Collector**: Selecteer **informatie** Alle opties moeten standaard worden geselecteerd, behalve voor gebruikersDB en vorige bestanden. Als u denkt dat uw probleem de gebruiker of de groepsdatabase is, selecteert u **Gebruiker DB**. Als u oude logbestanden wilt laten opnemen, selecteert u de optie voor **vorige logbestanden**. Klik op **Volgende** wanneer u klaar



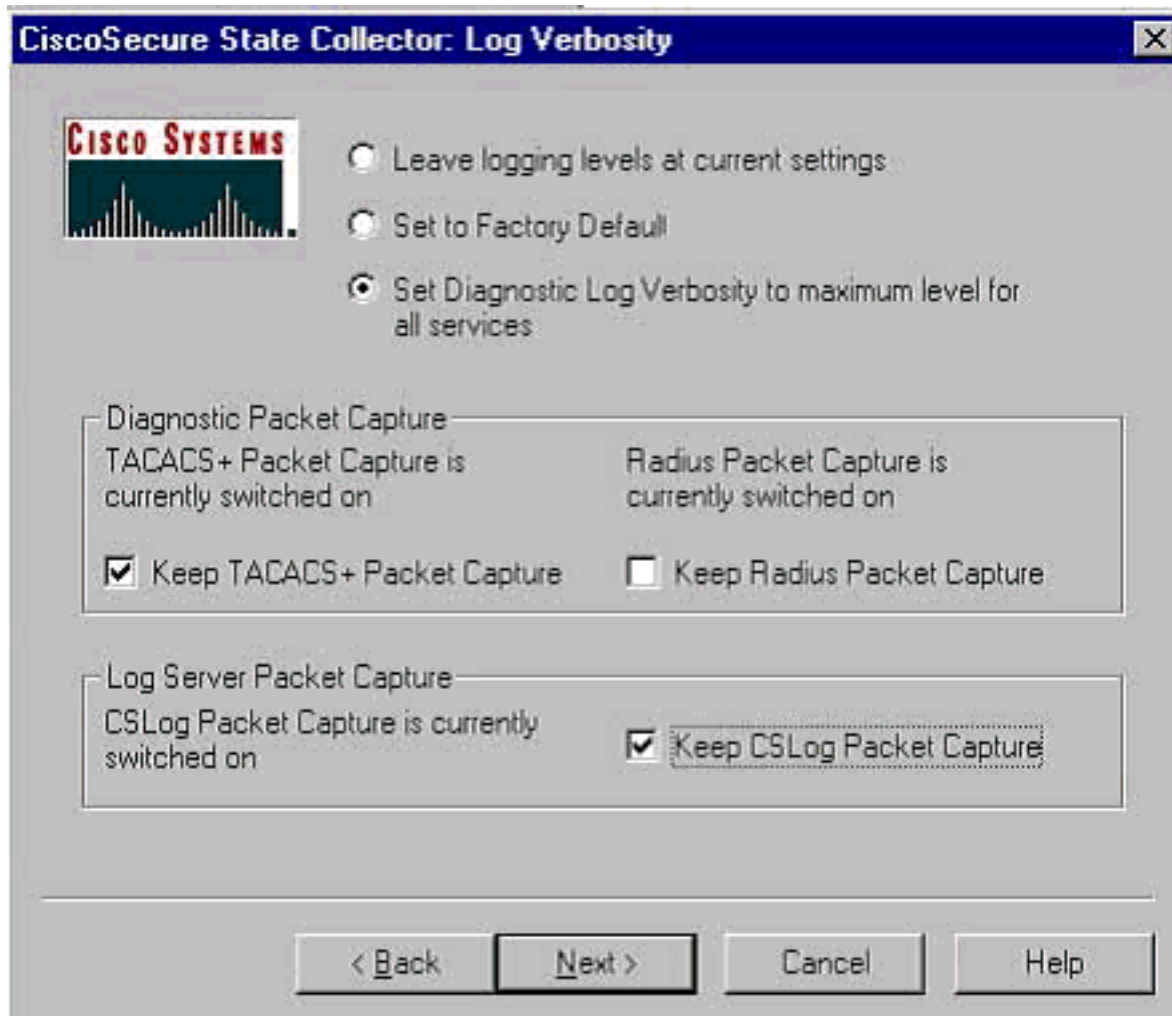
bent.

2. **Cisco Secure State Collector: Installatieselectie** Kies de map waarin u het Package.cab wilt plaatsen. De standaard is C:\Program Files\Cisco Secure ACS v.26\Utils\Support. U kunt deze locatie desgewenst wijzigen. Zorg ervoor dat de juiste locatie van uw Dr. Watson is aangegeven. Voor het uitvoeren van CSS-ondersteuning moet u de services starten en stoppen. Als u zeker bent dat u de Cisco Secure-services wilt stoppen en starten, klikt u op **Volgende** om verder te

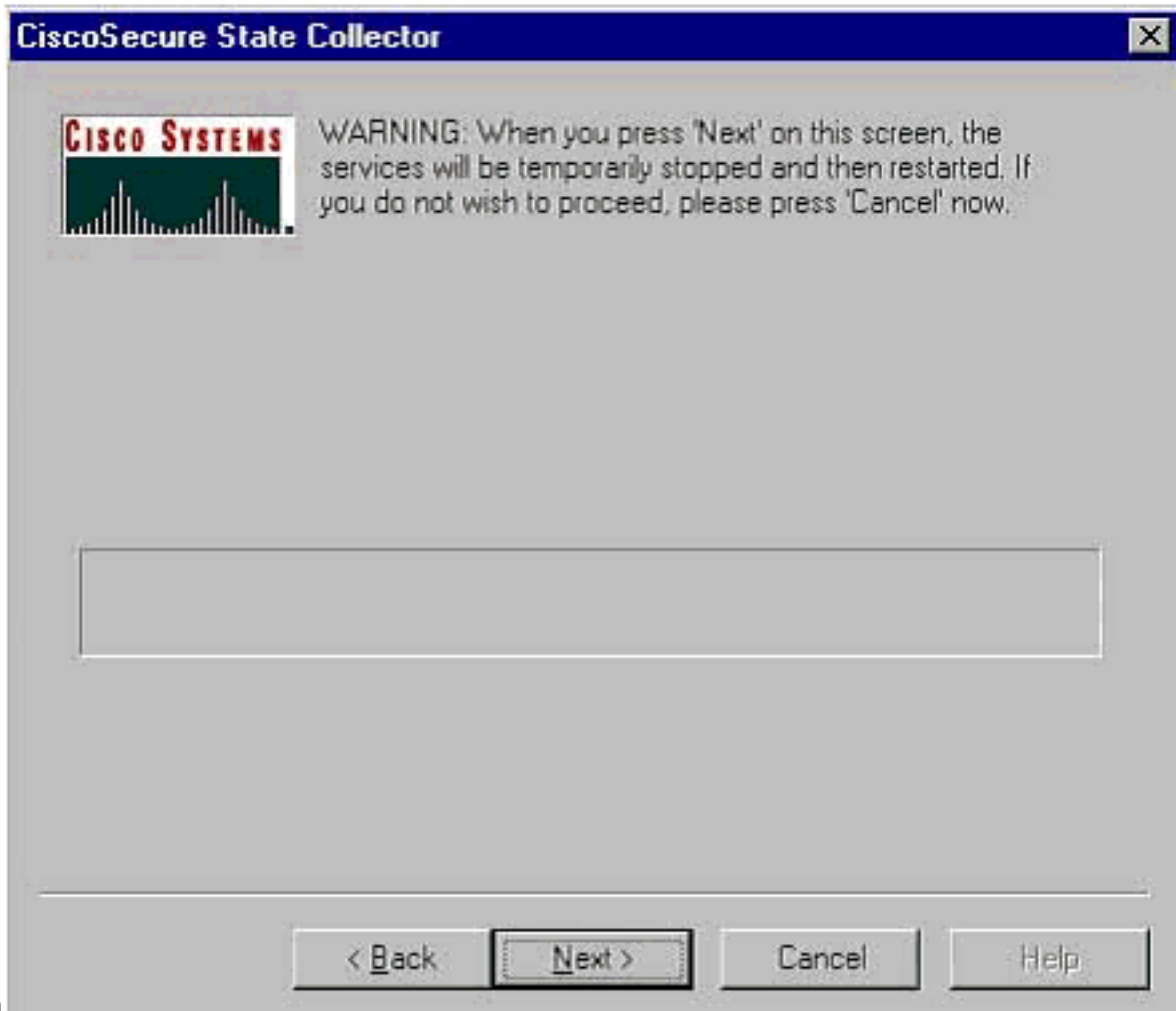


gaan.

3. **Cisco Secure State Collector: Logversie** Selecteer de optie voor **het instellen van de diagnostische inlogfout op het maximale niveau voor alle services**. Selecteer onder de optie Diagnostic Packet Capture, ofwel TACACS+ of RADIUS, afhankelijk van wat u hebt. Selecteer de optie **CSL-pakketvastlegging behouden**. Klik op **Volgende** als u klaar bent. **N.B.:** Als u logbestanden van vorige dagen wilt hebben, moet u de optie voor **vorige logbestanden** in stap 1 selecteren en vervolgens het aantal dagen instellen dat u wilt teruggaan.



4. **Cisco Secure State Collector**U ziet een waarschuwing dat wanneer u verdergaat, uw diensten worden stopgezet en dan opnieuw worden gestart. Deze onderbreking is nodig voor CSS ondersteuning om alle benodigde bestanden te pakken. De uitlooptijd moet minimaal zijn. U kunt het servicetaneel bekijken en op dit venster opnieuw starten. Klik op **Volgende** om verder te



gaan

Wa

Wanneer de services opnieuw worden gestart, kan Packet.cab gevonden worden op de gespecificeerde locatie. Klik op **Voltoeien** en uw Packet.cab-bestand is klaar. Bladeren naar de locatie die u voor het Packet.cab hebt opgegeven en verplaatsen naar een map waarin het kan worden opgeslagen. Uw technische helpdeskmedewerker kan uw vraag op elk moment tijdens het proces voor het oplossen van problemen indienen.

[Alleen logniveaus instellen](#)

Als u eerder de State Collector hebt uitgevoerd en alleen de logniveaus hoeft te wijzigen, kunt u de optie Alleen inlogniveau instellen om naar de [Cisco Secure State Collector](#) te overslaan: [Log veelzijdig](#) scherm in, waar u de diagnostische pakketvastlegging instelt. Wanneer u op **Volgende** klikt, gaat u rechtstreeks naar de pagina Waarschuwing. Klik vervolgens nogmaals op **Volgende** om de service te stoppen, het bestand te verzamelen en de services opnieuw te starten.

[Een pakket.cab-bestand handmatig verzamelen](#)

Het volgende is een lijst van de bestanden die in een Package.cab worden gecompileerd. Als de CSS-ondersteuning niet goed werkt, kunt u deze bestanden verzamelen met Windows Verkenner.

Registry (ACS.reg)

Failed Attempts File

(C:\program files\Cisco Secure acs v2.6\Logs\Failed Attempts active.csv)

TACACS+ Accounting

```
(C:\program files\Cisco Secure acs v2.6\Logs\TACACS+ Accounting\  
TACACS+ Accounting active.csv)
```

RADIUS Accounting

```
(C:\program files\Cisco Secure acs v2.6\Logs\RADIUS Accounting\  
RADIUS Accounting active.csv)
```

TACACS+ Administration

```
(C:\program files\Cisco Secure acs v2.6\Logs\TACACS+ Administration\  
TACACS+ Administration active.csv)
```

Auth log

```
(C:\program files\Cisco Secure acs v2.6\CSAuth\Logs\auth.log)
```

RDS log

```
(C:\program files\Cisco Secure acs v2.6\CSRADIUS\Logs\RDS.log)
```

TCS log

```
(C:\program files\Cisco Secure acs v2.6\CSTacacs\Logs\TCS.log)
```

ADMN log

```
(C:\program files\Cisco Secure acs v2.6\CSAdmin\Logs\ADMIN.log)
```

Cslog log

```
(C:\program files\Cisco Secure acs v2.6\CSLog\Logs\cslog.log)
```

Csmon log

```
(C:\program files\Cisco Secure acs v2.6\CSMon\Logs\csmon.log)
```

DrWatson

```
(drwtsn32.log) See section 3 for further details
```

[Cisco Secure voor Windows NT AAA-debug informatie verkrijgen](#)

De services van Windows NT CSRADIUS, CSTACS en CSAUTH kunnen in de modus van de opdrachtregel worden uitgevoerd wanneer u een probleem-probleem oplossen.

Opmerking: De GUI-toegang is beperkt als Cisco Secure voor Windows NT-services actief zijn in de opdrachtregelmodus.

Om CSRADIUS, CSTACS, of CSAUTH te verkrijgen debug-informatie, opent u een DOS-venster en past u de vensterbufferhoogte aan 300 aan.

Gebruik de volgende opdrachten voor CSRADIUS:

```
c:\program files\ciscosecure acs v2.1\csradius>net stop csradius
```

```
c:\program files\ciscosecure acs v2.1\csradius>csradius -d -p -z
```

Gebruik de volgende opdrachten voor CSTACS:

```
c:\program files\ciscosecure acs v2.1\cstacacs>net stop cstacacs
```

```
c:\program files\ciscosecure acs v2.1\cstacacs>cstacacs -e -z
```

Informatie over debug van Cisco Secure voor Windows NT AAA-replicatie verkrijgen

De Windows NT Quality-of-Service kan in de modus van de opdrachtregel worden uitgevoerd wanneer u een replicatieprobleem hebt opgelost.

Opmerking: De GUI-toegang is beperkt als Cisco Secure voor Windows NT-services actief zijn in de opdrachtregelmodus.

Om CSAuth replicatie te verkrijgen debug informatie, opent u een DOS-venster en past u de hoogte van de Buffer van het Scherm van Windows aan 300 aan.

Gebruik de volgende opdrachten voor CSAuth op zowel de bron als de doelservers:

```
c:\program files\ciscosecure acs v2.6\csauth>net stop csauth
```

```
c:\program files\ciscosecure acs v2.1\csauth>csauth -p -z
```

Het debug wordt in het venster van de opdrachtmelding geschreven en ook in het bestand \$BASE\csauth\logs\auth.log.

Verificatie door gebruiker offline testen

Gebruikersverificatie kan worden getest via de opdrachtregel-interface (CLI). RADIUS kan worden getest met behulp van 'radtest' en TACACS+ kan worden getest met behulp van 'tactest'. Deze testen kunnen nuttig zijn als het communicerende apparaat geen nuttige debug informatie produceert en als er enige vraag is of er een Cisco Secure ACS Windows probleem of een apparaatprobleem is. Zowel radtest als tactest vinden plaats in de \$BASE\utils folder. De volgende voorbeelden zijn voorbeelden van elke test.

RADIUS-gebruikersverificatie offline testen met Radtest

```
SERVER TEST PROGRAM
```

```
1...Set Radius IP, secret & timeout
2...Authenticate user
3...Authenticate from file
4...Authenticate with CHAP
5...Authenticate with MSCHAP
6...Replay log files
7...Drive authentication and accounting from file
8...Accounting start for user
9...Accounting stop for user
A...Extended Setup
B...Customer Packet Builder
0...Exit
```

```
Defaults server:172.18.124.99 secret:secret_value timeout:2000mSec
      auth:1645 acct:1646 port:999 cli:999
```

```
Choice>2
```

```

User name><>abcde
User password><>abcde
Cli><999>
NAS port id><999>
State><>
User abcde authenticated
Request from host 172.18.124.99:1645 code=2, id=0, length=44 on port 1645
    [080] Signature          value: A6 10 00 96 6F C2 AB 78 B6 9F CA D9 01 E3 D7 C6
    [008] Framed-IP-Address value: 10.1.1.5

Hit Return to continue.

```

Testen van TACACS+ gebruikersverificatie offline met tastbare resultaten

```

tactest -H 127.0.0.1 -k secret
TACACS>
Commands available:
    authen action type service port remote [user]
           action <login,sendpass,sendauth>
           type <ascii,pap,chap,mschap,arap>
           service <login,enable,ppp,arap,pt,rcmd,x25>
    author arg1=value1 arg2=value2 ...
    acct arg1=value1 arg2=value2 ...
TACACS> authen login ascii login tty0 abcde
Username: abcde
Password: abcde
Authentication succeeded :
TACACS>

```

Redenen voor Windows 2000/NT Database-fouten bepalen

Als de authenticatie wordt doorgegeven aan Windows 2000/NT maar faalt, kunt u de Windows-auditfaciliteit inschakelen door naar **Programma's > Administratieve Gereedschappen > Gebruikersbeheer voor domeinen, beleid > Audit**. Het gaan naar **Programma's > Administratieve Gereedschappen > Het evenementenvenster** toont echtheidsfouten. Fouten in het logbestand van mislukte pogingen worden weergegeven in een bestandsindeling zoals in het onderstaande voorbeeld.

NT/2000 authentication FAILED (error 1300L)

Deze berichten kunnen worden onderzocht op de website van Microsoft op [Windows 2000 Event & Error Messages](#) en [Error Codes in Windows NT](#) .

De 1300L foutmelding wordt hieronder beschreven.

Code	Name	Description
1300L	ERROR_NOT_ALL_ASSIGNED	Indicates not all privileges referenced are assigned to the caller. This allows, for example, all privileges to be disabled without having to know exactly which privileges are assigned.

Voorbeelden

RADIUS-goede verificatie

```
F:\Program Files\Cisco Secure ACS v2.6\CSRADIUS>csradius -p -z
CSRADIUS v2.6(2.4), Copyright 1997-1999, Cisco Systems Inc
Debug logging on
Command line mode
===== SERVICE STARTED =====
Version is 2.6(2.4)
Server variant is Default
10 auth threads, 20 acct threads
NTlib The local computer name is YOUR-PC
NTlib We are NOT a domain controller
NTlib We are a member of the RTP-APPS domain
NTlib An additional domain list is defined: \LOCAL,RTP-APPS,somedomain
Winsock initialised ok
Created shared memory
ExtensionPoint: Base key is [SOFTWARE\Cisco\CiscoAAAv2.6\CSRADIUS\ExtensionPoint
s]
ExtensionPoint: Entry [001] for supplier [Cisco Aironet] via dll [AironetEAP.dll
]
ExtensionPoint: Looking for vendor associations for supplier [Cisco Aironet]
ExtensionPoint: Found vendor association [RADIUS (Cisco Aironet)] for supplier [
Cisco Aironet]
ExtensionPoint: Supplier [Cisco Aironet] is disabled, ignoring...
CSAuth interface initialised
About to retrieve user profiles from CSAuth
Profile 0, Subset for vendor 1 - RADIUS (Cisco IOS/PIX)
    [026] Vendor-Specific                vsa id: 9
        [103] cisco-h323-return-code     value: 01
Profile 0, Subset for vendor 8 - RADIUS (Cisco Aironet)
    [026] Vendor-Specific                vsa id: 9
        [103] cisco-h323-return-code     value: 01
Starting auth/acct worker threads
RADIUS Proxy: Proxy Cache successfully initialized.
Hit any key to stop

Dispatch thread ready on Radius Auth Port [1645]
Dispatch thread ready on Radius Auth Port [1812]
Dispatch thread ready on Radius Acct Port [1646]
Dispatch thread ready on Radius Acct Port [1813]
Request from host 172.18.124.154:1645 code=1, id=6, length=55 on port 1645
    [001] User-Name                       value: roy
    [004] NAS-IP-Address                  value: 172.18.124.154
    [002] User-Password                   value: BF 37 6D 76 76 22 55 88 83
AD 6F 03 2D FA 92 D0
    [005] NAS-Port                        value: 5
Sending response code 2, id 6 to 172.18.124.154 on port 1645
    [008] Framed-IP-Address               value: 255.255.255.255

RADIUS Proxy: Proxy Cache successfully closed.
Calling CMFini()
CMFini() Complete
===== SERVICE STOPPED=====
Server stats:
Authentication packets : 1
    Accepted             : 1
```

```
Rejected          : 0
Still in service  : 0
Accounting packets : 0
Bytes sent        : 26
Bytes received    : 55
UDP send/rcv errors : 0
```

F:\Program Files\Cisco Secure ACS v2.6\CSRADIUS>

RADIUS-slechte verificatie

```
F:\Program Files\Cisco Secure ACS v2.6\CSRADIUS>
F:\Program Files\Cisco Secure ACS v2.6\CSRADIUS>csradius -p -z
CSRADIUS v2.6(2.4), Copyright 1997-1999, Cisco Systems Inc
Debug logging on
Command line mode
===== SERVICE STARTED =====
Version is 2.6(2.4)
Server variant is Default
10 auth threads, 20 acct threads
NTlib The local computer name is YOUR-PC
NTlib We are NOT a domain controller
NTlib We are a member of the RTP-APPS domain
NTlib An additional domain list is defined: \LOCAL,RTP-APPS,somedomain
Winsock initialised ok
Created shared memory
ExtensionPoint: Base key is [SOFTWARE\Cisco\CiscoAAAv2.6\CSRADIUS\ExtensionPoints]
ExtensionPoint: Entry [001] for supplier [Cisco Aironet] via dll [AironetEAP.dll]
ExtensionPoint: Looking for vendor associations for supplier [Cisco Aironet]
ExtensionPoint: Found vendor association [RADIUS (Cisco Aironet)] for supplier [Cisco Aironet]
ExtensionPoint: Supplier [Cisco Aironet] is disabled, ignoring...
CSAuth interface initialised
About to retrieve user profiles from CSAuth
Profile 0, Subset for vendor 1 - RADIUS (Cisco IOS/PIX)
  [026] Vendor-Specific          vsa id: 9
  [103] cisco-h323-return-code   value: 01
Profile 0, Subset for vendor 8 - RADIUS (Cisco Aironet)
  [026] Vendor-Specific          vsa id: 9
  [103] cisco-h323-return-code   value: 01
Starting auth/acct worker threads
RADIUS Proxy: Proxy Cache successfully initialized.
Hit any key to stop

Dispatch thread ready on Radius Auth Port [1645]
Dispatch thread ready on Radius Auth Port [1812]
Dispatch thread ready on Radius Acct Port [1646]
Dispatch thread ready on Radius Acct Port [1813]
Request from host 172.18.124.154:1645 code=1, id=7, length=55 on port 1645
  [001] User-Name                value: roy
  [004] NAS-IP-Address           value: 172.18.124.154
  [002] User-Password            value: 47 A3 BE 59 E3 46 72 40 B3
  AC 40 75 B3 3A B0 AB
  [005] NAS-Port                 value: 5
User:roy - Password supplied for user was not valid
Sending response code 3, id 7 to 172.18.124.154 on port 1645
Request from host 172.18.124.154:1645 code=1, id=8, length=55 on port 1645
  [001] User-Name                value: roy
  [004] NAS-IP-Address           value: 172.18.124.154
```

```

[002] User-Password          value: FE AF C0 D1 4D FD 3F 89 BA
0A C7 75 66 DC 48 27
[005] NAS-Port              value: 5
User:roy - Password supplied for user was not valid
Sending response code 3, id 8 to 172.18.124.154 on port 1645
Request from host 172.18.124.154:1645 code=1, id=9, length=55 on port 1645
[001] User-Name            value: roy
[004] NAS-IP-Address       value: 172.18.124.154
[002] User-Password       value: 79 1A 92 14 D6 5D A5 3E D6
7D 09 D2 A5 8E 65 A5
[005] NAS-Port            value: 5
User:roy - Password supplied for user was not valid
Sending response code 3, id 9 to 172.18.124.154 on port 1645
Request from host 172.18.124.154:1645 code=1, id=10, length=55 on port 1645
[001] User-Name            value: roy
[004] NAS-IP-Address       value: 172.18.124.154
[002] User-Password       value: 90 4C 6D 39 66 D1 1C B4 F7
87 8B 7F 8A 29 60 9E
[005] NAS-Port            value: 5
User:roy - Password supplied for user was not valid
Sending response code 3, id 10 to 172.18.124.154 on port 1645

```

RADIUS Proxy: Proxy Cache successfully closed.

Calling CMFini()

CMFini() Complete

===== SERVICE STOPPED =====

Server stats:

```

Authentication packets : 4
  Accepted              : 0
  Rejected             : 4
  Still in service     : 0
Accounting packets     : 0
Bytes sent              : 128
Bytes received         : 220
UDP send/recv errors   : 0

```

F:\Program Files\Cisco Secure ACS v2.6\CSRADIUS>

[TACACS+ goede verificatie](#)

```

F:\Program Files\Cisco Secure ACS v2.6\CSTacacs>cstacacs -e -z
CSTacacs v2.6(2.4), Copyright 1997-1999, Cisco Systems Inc
CSTacacs server starting =====
Base directory is F:\Program Files\Cisco Secure ACS v2.6\CSTacacs
Log directory is F:\Program Files\Cisco Secure ACS v2.6\CSTacacs\Logs
CSTacacs version is 2.6(2.4)
Running as console application.
Doing Stats

```

```

**** Registry Setup ****
Single TCP connection operation enabled
Base Proxy enabled.
*****

```

```

TACACS+ server started
Hit any key to stop

```

```

Created new session f3f130 (count 1)
All sessions busy, waiting
Thread 0 waiting for work

```


Thread 0 allocated work

Waiting for packetRead AUTHEN/START size=38

Packet from NAS*****

CONNECTION: NAS 520b Socket 2d4

PACKET: version 192 (0xc0), type 1, seq no 1, flags 1

session_id 1381473548 (0x52579d0c), Data length 26 (0x1a)

End header

Packet body hex dump:

01 01 01 01 03 01 0e 00 72 6f 79 30 31 37 32 2e 31 38 2e 31 32 34 2e 31 35 34

type=AUTHEN/START, priv_lvl = 1

action = login

authen_type=ascii

service=login

user_len=3 port_len=1 (0x1), rem_addr_len=14 (0xe)

data_len=0

User: roy

port: 0

rem_addr: 172.18.124.154End packet*****

Created new Single Connection session num 0 (count 1/1)

All sessions busy, waiting

All sessions busy, waiting

Listening for packet.Single Connect thread 0 waiting for work

Single Connect thread 0 allocated work

thread 0 sock: 2d4 session_id 0x52579d0c seq no 1 AUTHEN:START login ascii login

roy 0 172.18.124.154

Authen Start request

Authen Start request

Calling authentication function

Writing AUTHEN/GETPASS size=28

Packet from CST*****

CONNECTION: NAS 520b Socket 2d4

PACKET: version 192 (0xc0), type 1, seq no 2, flags 1

session_id 1381473548 (0x52579d0c), Data length 16 (0x10)

End header

Packet body hex dump:

05 01 00 0a 00 00 50 61 73 73 77 6f 72 64 3a 20

type=AUTHEN status=5 (AUTHEN/GETPASS) flags=0x1

msg_len=10, data_len=0

msg: Password:

data:

End packet*****

Read AUTHEN/CONT size=22

Packet from NAS*****

CONNECTION: NAS 520b Socket 2d4

PACKET: version 192 (0xc0), type 1, seq no 3, flags 1

session_id 1381473548 (0x52579d0c), Data length 10 (0xa)

End header

Packet body hex dump:

00 05 00 00 00 63 69 73 63 6f

type=AUTHEN/CONT

user_msg_len 5 (0x5), user_data_len 0 (0x0) flags=0x0

User msg: cisco

User data: End packet*****

Listening for packet.login query for 'roy' 0 from 520b accepted

Writing AUTHEN/SUCCEED size=18

Packet from CST*****

CONNECTION: NAS 520b Socket 2d4

PACKET: version 192 (0xc0), type 1, seq no 4, flags 1

session_id 1381473548 (0x52579d0c), Data length 6 (0x6)

End header

```
Packet body hex dump:
01 00 00 00 00 00
type=AUTHEN status=1 (AUTHEN/SUCCEED) flags=0x0
msg_len=0, data_len=0
msg:
data:
End packet*****
Single Connect thread 0 waiting for work
520b: fd 724 eof (connection closed)
Thread 0 waiting for work
Release Host Cache
Close Proxy Cache
Calling CMFini()
CMFini() Complete
Closing Password Aging
Closing Finished
```

```
F:\Program Files\Cisco Secure ACS v2.6\CSTacacs>
```

TACACS+ slechte verificatie (samengevat)

```
F:\Program Files\Cisco Secure ACS v2.6\CSTacacs>
F:\Program Files\Cisco Secure ACS v2.6\CSTacacs>cstacacs -e -z
CSTacacs v2.6(2.4), Copyright 1997-1999, Cisco Systems Inc
CSTacacs server starting =====
Base directory is F:\Program Files\Cisco Secure ACS v2.6\CSTacacs
Log directory is F:\Program Files\Cisco Secure ACS v2.6\CSTacacs\Logs
CSTacacs version is 2.6(2.4)
Running as console application.
Doing Stats
```

```
**** Registry Setup ****
Single TCP connection operation enabled
Base Proxy enabled.
*****
```

```
TACACS+ server started
Hit any key to stop
```

```
Created new session f3f130 (count 1)
All sessions busy, waiting
Thread 0 waiting for work
Thread 0 allocated work
Waiting for packetRead AUTHEN/START size=38
```

```
Packet from NAS*****
CONNECTION: NAS 520b Socket 2d4
PACKET: version 192 (0xc0), type 1, seq no 3, flags 1
session_id 714756899 (0x2a9a5323), Data length 11 (0xb)
End header
Packet body hex dump:
00 06 00 00 00 63 69 73 63 6f 31
type=AUTHEN/CONT
user_msg_len 6 (0x6), user_data_len 0 (0x0) flags=0x0
User msg: cisco1
User data: End packet*****
Listening for packet.login query for 'roy' 0 from 520b rejected
Writing AUTHEN/FAIL size=18
```

Release Host Cache
Close Proxy Cache
Calling CMFini()
CMFini() Complete
Closing Password Aging
Closing Finished

F:\Program Files\Cisco Secure ACS v2.6\CSTacacs>

[Gerelateerde informatie](#)

- [Technische ondersteuning - Cisco-systemen](#)