Windows용 Cisco Secure ACS의 버전 및 AAA 디버그 정보 가져오기

목차

소개

이 문서에서는 Windows용 Cisco Secure ACS 버전을 보는 방법과 AAA(Authentication, Authorization, and Accounting) 디버그 정보를 설정하고 가져오는 방법에 대해 설명합니다.

시작하기 전에

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

사전 요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Windows 2.6용 Cisco Secure ACS를 기반으로 합니다.

Cisco Secure for Windows 버전 정보 가져오기

DOC 명령줄을 사용하거나 GUI를 사용하여 버전 정보를 볼 수 있습니다.

DOS 명령줄 사용

DOS의 명령줄 옵션을 통해 Windows용 Cisco Secure ACS의 버전 번호를 보려면 RADIUS의 경우 **cstacacs** 또는 **csradius**와 TACACS+의 경우 **-v**를 사용하고 TACACS+의 경우 **-x**를 사용합니다. 아래 예를 참조하십시오.

```
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
```

Windows 레지스트리에서 Cisco Secure ACS 프로그램의 버전 번호를 볼 수도 있습니다. 예를 들면 다음과 같습니다.

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

GUI 사용

Cisco Secure ACS GUI로 버전을 보려면 ACS 홈 페이지로 이동하십시오. 언제든지 화면 왼쪽 상단에 있는 Cisco Systems 로고를 클릭하여 이 작업을 수행할 수 있습니다. 홈 페이지의 하단에는 전체 버전이 표시됩니다.

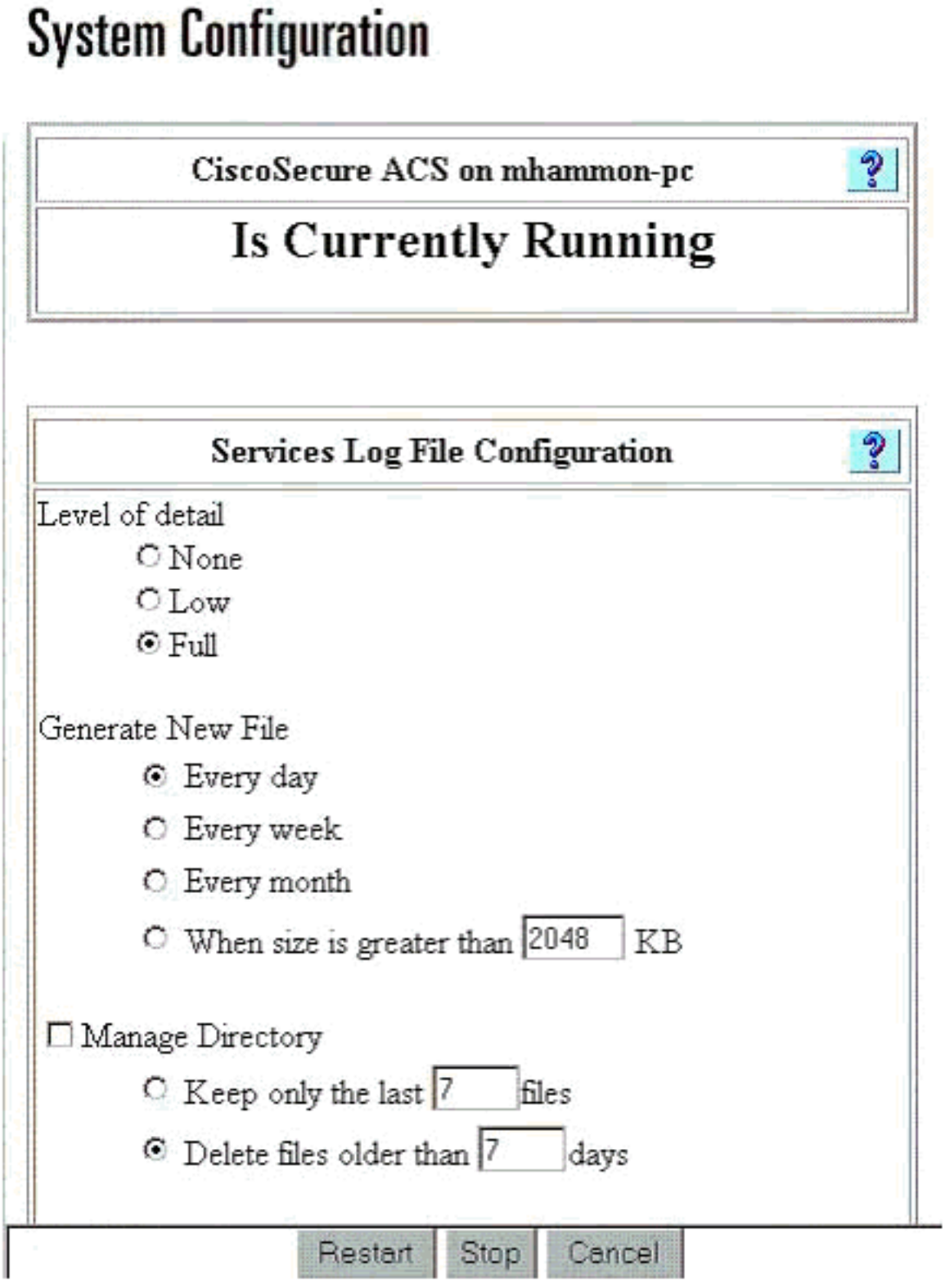
Windows용 Cisco Secure ACS 디버깅 수준 설정

다음은 최대 디버깅 정보를 얻는 데 필요한 여러 디버깅 옵션에 대한 설명입니다.

ACS GUI에서 로깅 레벨을 전체로 설정하는 방법

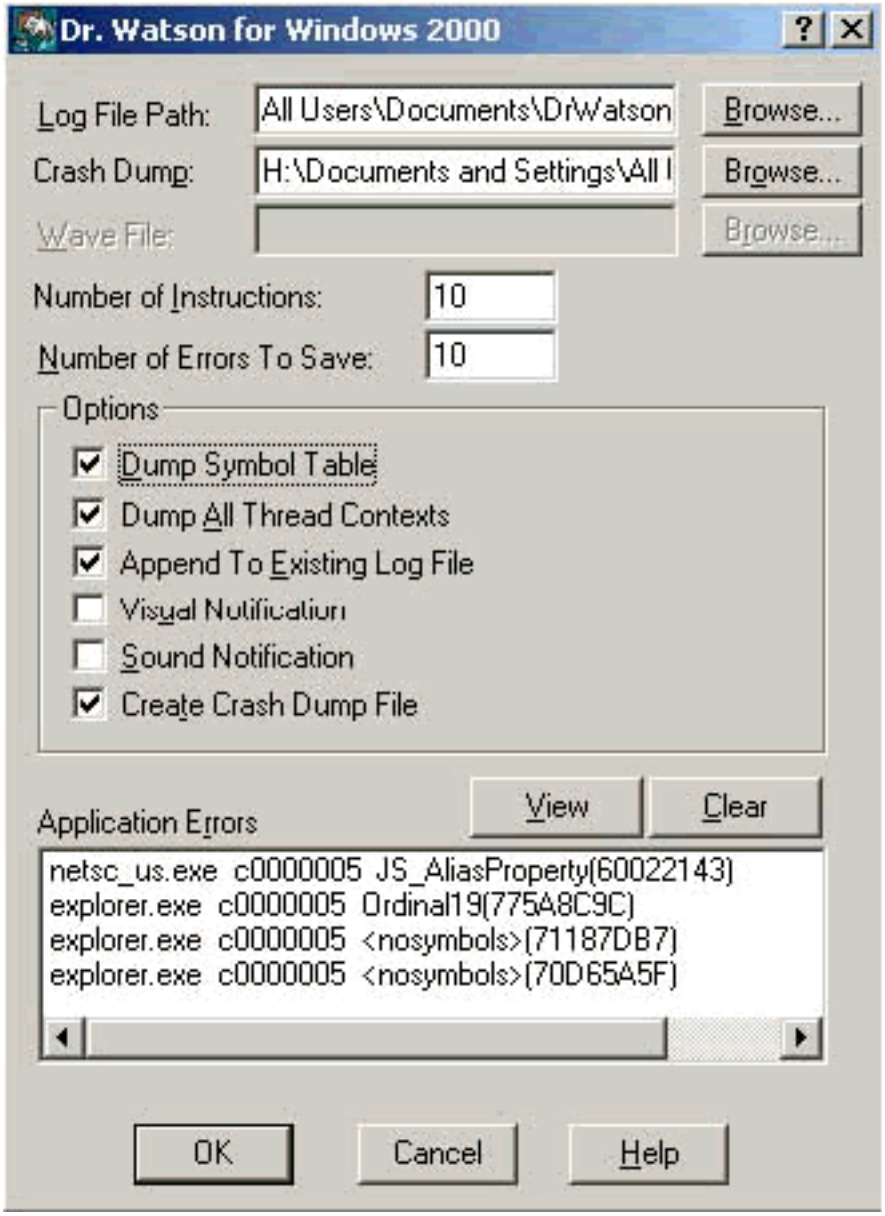
모든 메시지를 기록하도록 ACS를 설정해야 합니다. 이렇게 하려면 아래 나열된 단계를 수행하십시오.

1. ACS 홈 페이지에서 Systems Configuration(시스템 컨피그레이션) **> Service Control(서비스 제어)으로 이동합니다**.
2. Service Log File Configuration(서비스 로그 파일 컨피그레이션) 헤딩에서 세부 정보 레벨을 **Full(전체)**로 **설정합니다**.필요한 경우 새 파일 생성 및 디렉토리 관리 섹션을 수정할 수 있습니다.



Dr. Watson 로깅을 설정하는 방법

명령 프롬프트에서 drwtsn32를 입력하면 Dr. Watson 창이 나타납니다. 모든 스레드 컨텍스트 **덤프** 및 **덤프 기호 테이블** 옵션이 선택되어 있는지 확인합니다.



package.cab 파일 만들기

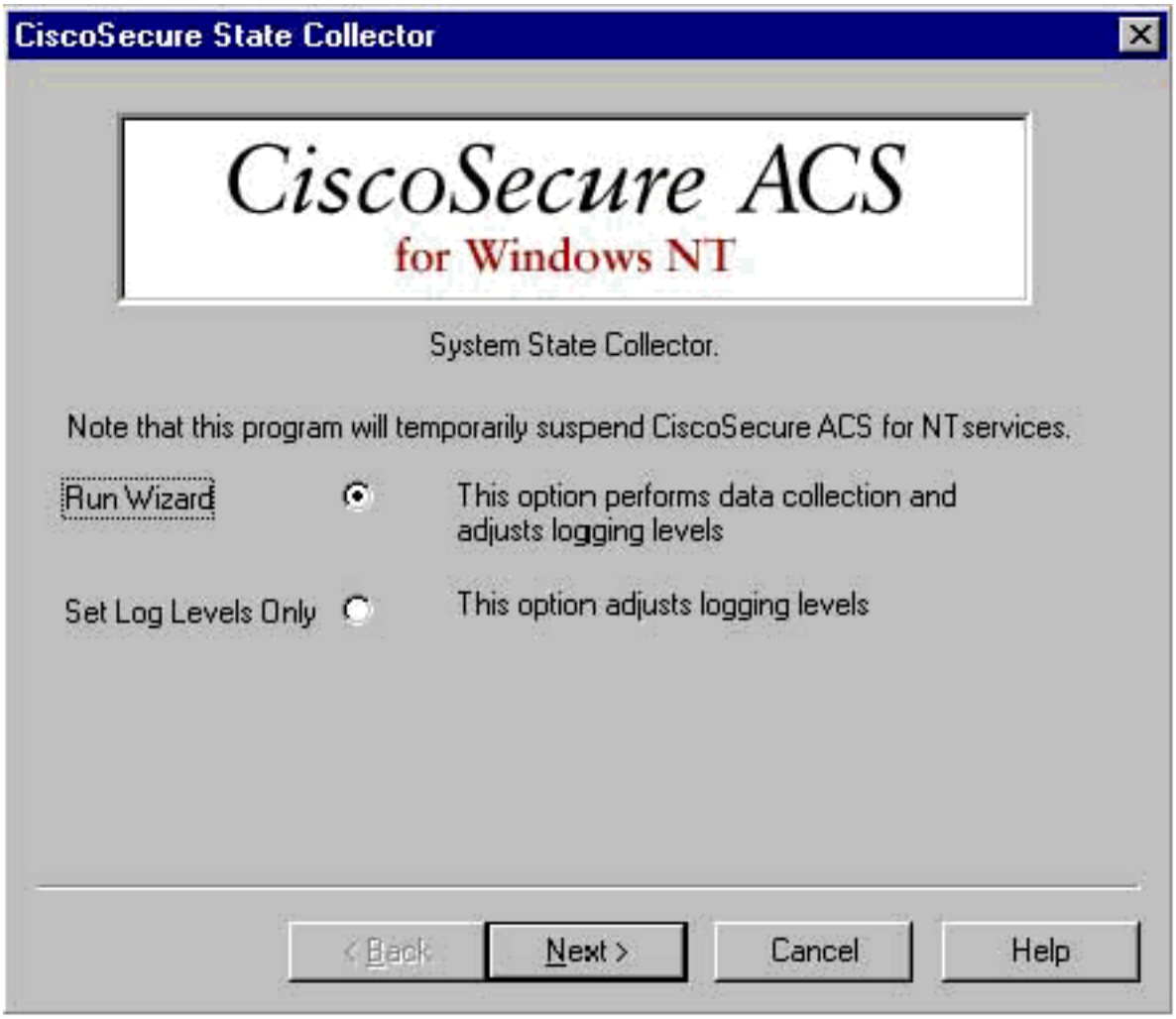
패키지.cab가 뭐죠?

package.cab는 ACS의 효율적인 문제 해결에 필요한 모든 파일을 포함하는 Zip 파일입니다. CSSupport.exe 유틸리티를 사용하여 package.cab를 만들거나 파일을 수동으로 수집할 수 있습니다.

CSSupport.exe 유틸리티를 사용하여 package.cab 파일 만들기

정보를 수집해야 하는 ACS 문제가 있는 경우 문제가 표시되면 가능한 빨리 CSSupport.exe 파일을 실행합니다. DOS 명령줄 또는 Windows 탐색기 GUI를 사용하여 C:\program files\Cisco Secure ACS v2.6\Utils>CSSupport.exe에서 CSSsupport를 실행합니다.

CSSupport.exe 파일을 실행하면 다음 창이 나타납니다.



이 화면에는 두 가지 기본 옵션이 있습니다.

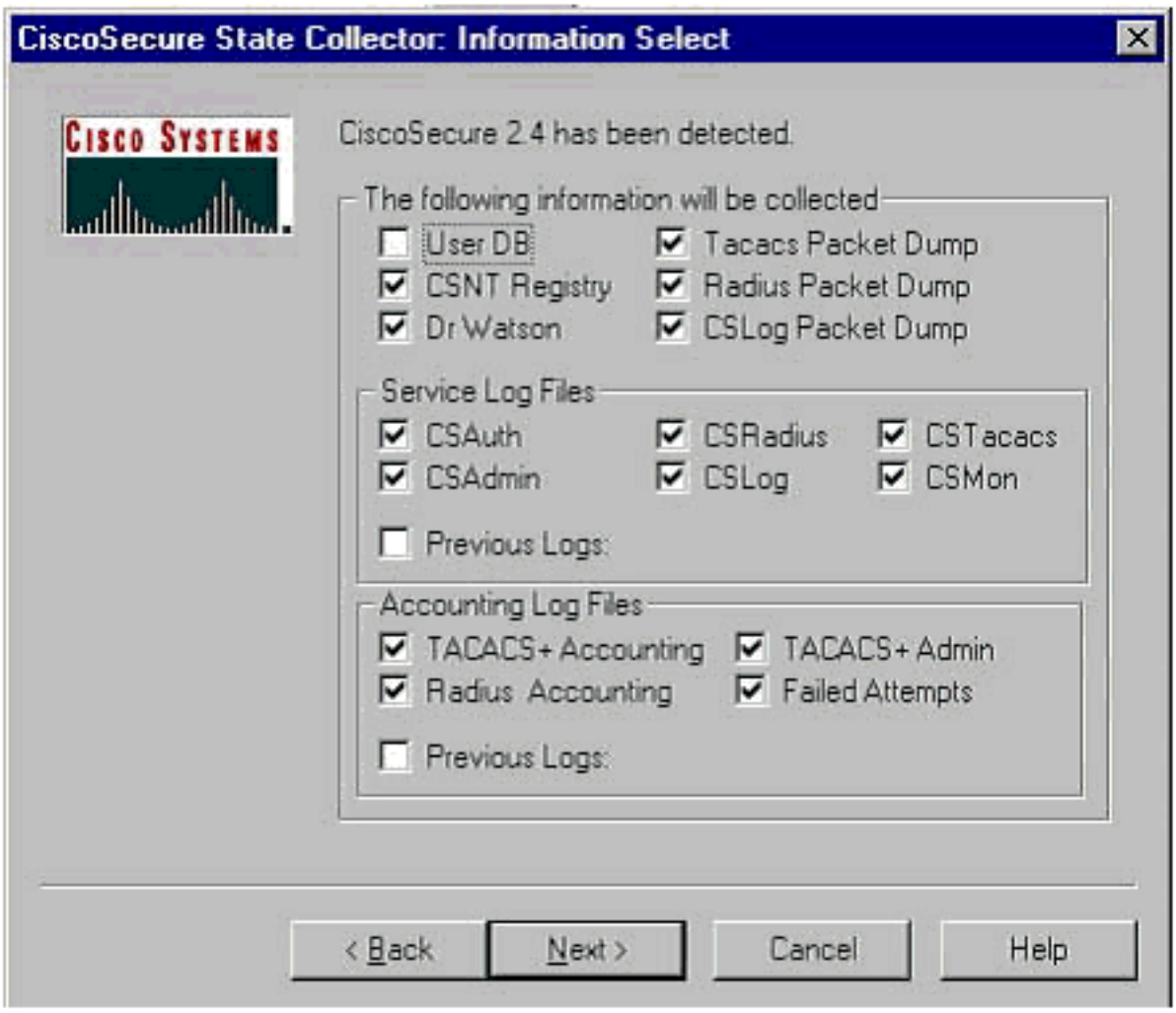
- 마법사를 실행하여 다음과 같은 네 가지 단계를 안내합니다.Cisco Secure State Collector: 정보 선택Cisco Secure State Collector: 설치 선택Cisco Secure State Collector: 로그 세부 정보 표시Cisco Secure State Collector(실제 수집)또는
- Set Log Level Only(로그 레벨만 설정)를 선택하면 처음 몇 단계를 건너뛰고 Cisco Secure State Collector로 바로 이동할 수 있습니다. 자세한 정보 표시 화면

최초 설치의 경우 **마법사 실행**을 선택하여 로그 설정에 필요한 단계를 진행합니다. 초기 설정 후 **Set Log Levels Only** 옵션을 사용하여 로깅 레벨을 조정할 수 있습니다. 선택한 후 **다음**을 클릭합니다.

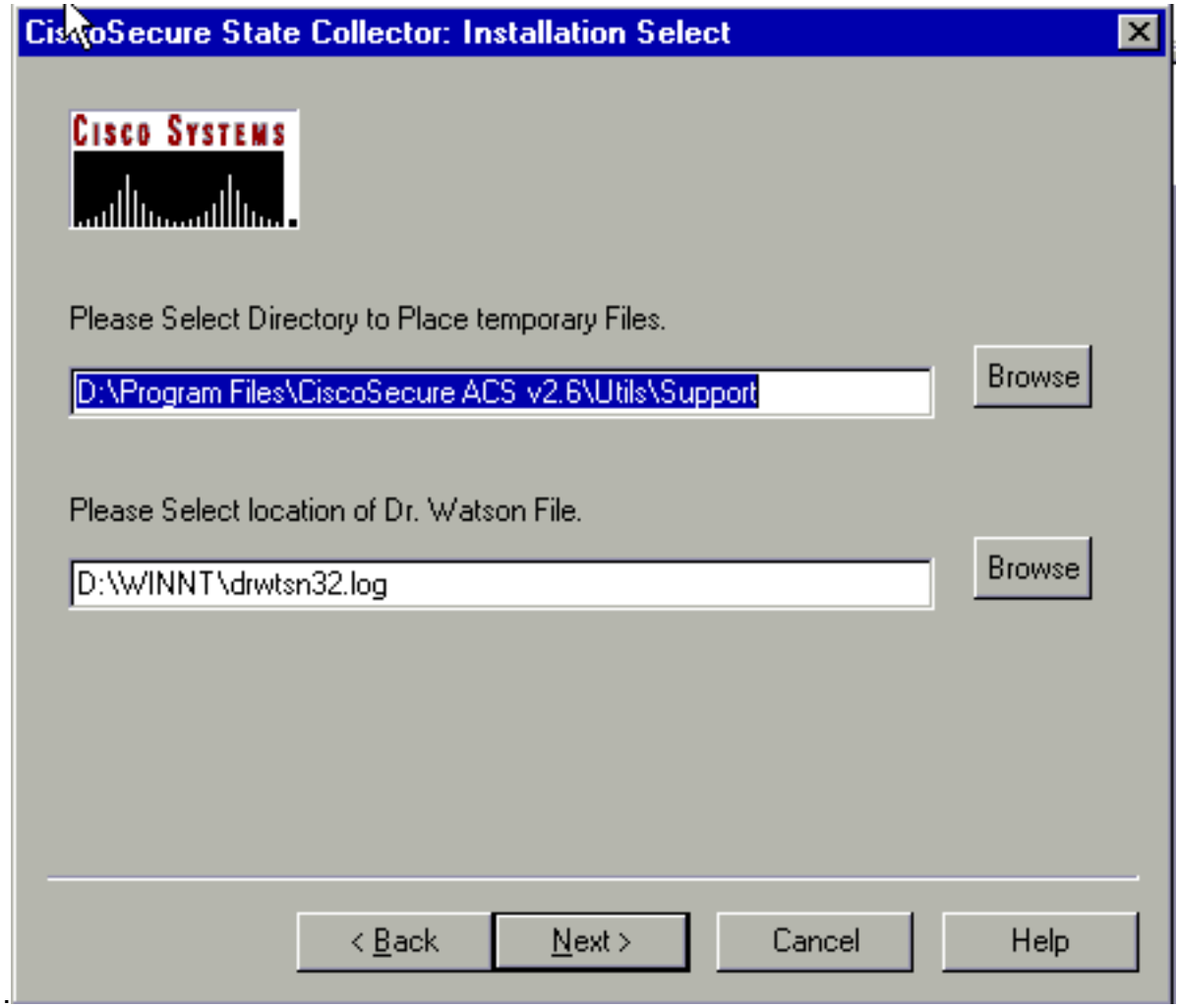
마법사 실행

다음은 마법사 실행 옵션을 사용하여 정보를 선택하는 방법에 대해 설명합니다.

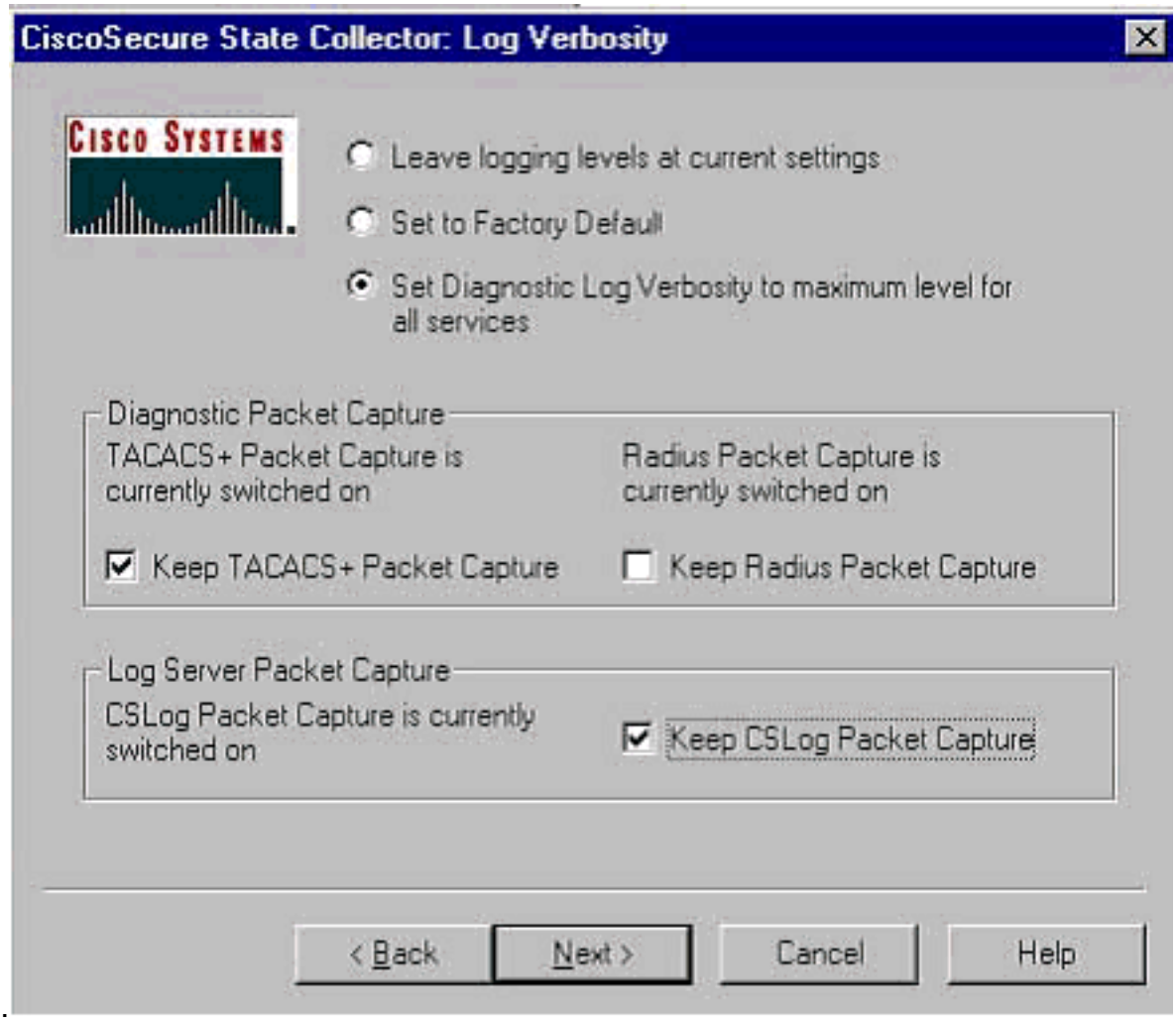
1. **Cisco Secure State Collector: 정보** 선택사용자 DB 및 이전 로그를 제외한 모든 옵션은 기본적으로 선택해야 합니다. 문제가 사용자 또는 그룹 데이터베이스라고 생각되면 **사용자 DB**를 선택합니다. 이전 로그를 포함하려면 Previous Logs(이전 로그) 옵션을 **선택합니다**. 완료되면 **Next**를 클릭합니다



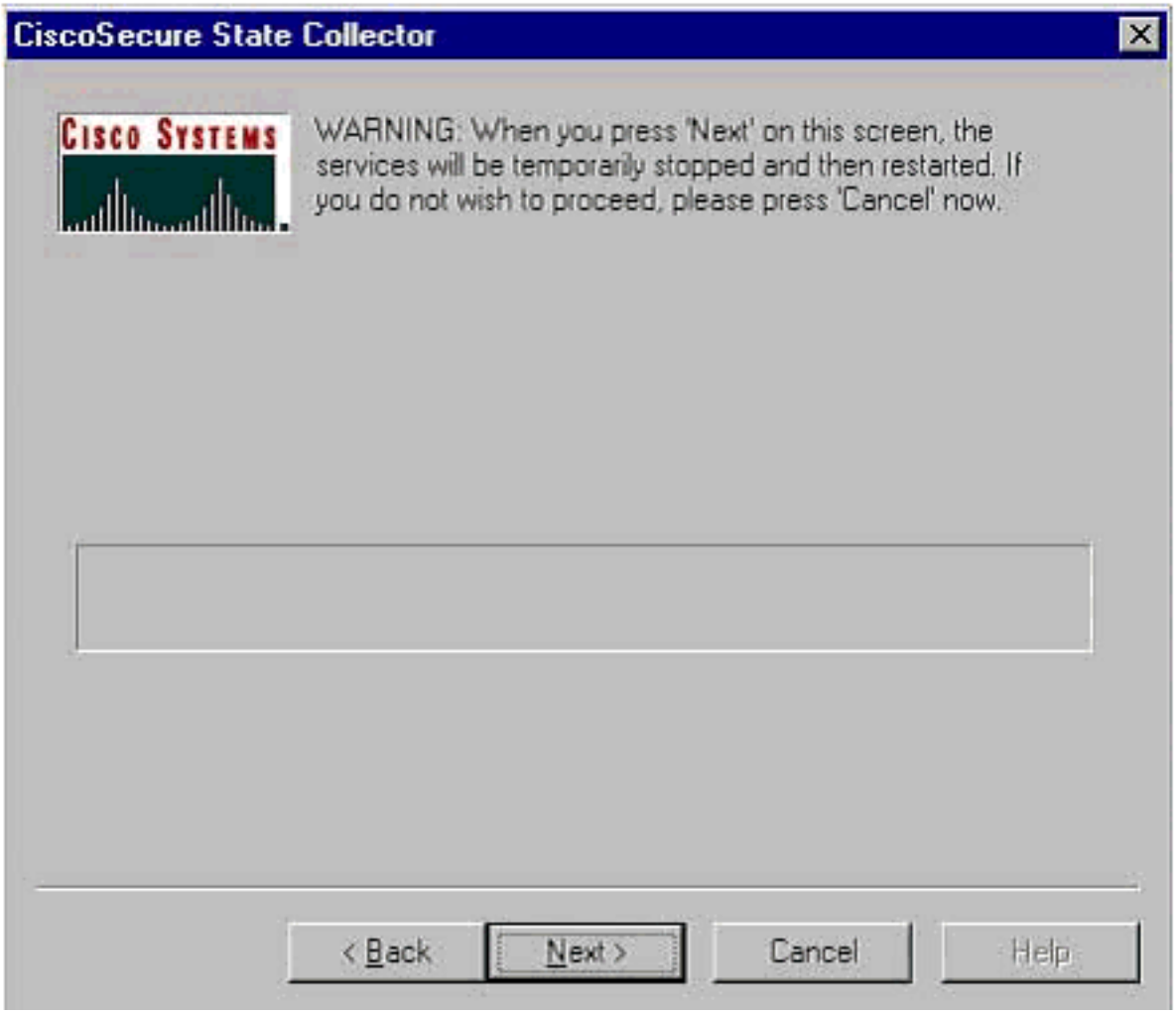
2. **Cisco Secure State Collector: 설치 선택**package.cab를 배치할 디렉토리를 선택합니다. 기본값은 C:\Program Files\Cisco Secure ACS v.26\Utils\Support입니다. 원하는 경우 이 위치를 변경할 수 있습니다. Dr. Watson의 올바른 위치가 지정되었는지 확인하십시오. CSSsupport를 실행하려면 서비스를 시작하고 중지해야 합니다. Cisco Secure Services를 중지하고 시작하려면 **다음**을 클릭하여 계속합니다



3. **Cisco Secure State Collector: 로그 세부 정보 표시모든 서비스**에 대해 **Set Diagnostic Log Verbosity(진단 로그 세부 정보 설정)** 옵션**을 최대 수준으로 설정합니다**. Diagnostic Packet Capture(진단 패킷 캡처) 제목 아래에서 실행 중인 항목에 따라 TACACS+ 또는 RADIUS를 선택합니다. Keep CSLog **Packet Capture** 옵션**을** 선택합니다. 완료되면 **다음**을 클릭합니다.**참고:** 이전 날짜의 로그를 사용하려면 단계 1에서 **이전 로그** 옵션을 선택한 다음 되돌릴 일 수를 설정해야 합니다



4. **Cisco Secure State 컬렉터**계속할 때 서비스가 중지되고 다시 시작된다는 경고가 표시됩니다. 이 중단은 CSSsupport에서 필요한 모든 파일을 가져오는 데 필요합니다. 다운 시간은 최소여야 합니다. 이 창에서 서비스를 중지하고 다시 시작할 수 있습니다. 계속하려면 **Next**를 클릭합



니다. 서비스를 다시 시작하면 지정된 위치에서 package.cab를 찾을 수 있습니다. **마침**을 클릭하면 package.cab 파일이 준비됩니다.package.cab에 대해 지정한 위치를 찾아 저장할 수 있는 디렉토리로 옮깁니다. 기술 지원 엔지니어가 문제 해결 프로세스 중에 언제든지 요청할 수 있습니다.

로그 레벨만 설정

이전에 State Collector(상태 컬렉터)를 실행했으며 로깅 레벨만 변경해야 하는 경우 Set Log Levels Only(로그 레벨만 설정) 옵션을 사용하여 Cisco Secure State Collector(Cisco 보안 상태 컬렉터)로 건너뛸 수 있습니다. Log Verbosity 화면 - 진단 패킷 캡처를 설정합니다. **Next(다음)**를 클릭하면 Warning(경고) 페이지로 바로 이동합니다. 그런 다음 **Next(다음)**를 다시 클릭하여 서비스를 중지하고 파일을 수집하고 서비스를 다시 시작합니다.

package.cab 파일을 수동으로 수집

다음은 package.cab로 컴파일되는 파일의 목록입니다. CSSsupport가 제대로 작동하지 않으면 Windows 탐색기를 사용하여 이러한 파일을 수집할 수 있습니다.

```
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
```

Windows NT AAA용 Cisco Secure 디버그 정보 가져오기

문제를 해결하는 경우 명령줄 모드에서 Windows NT CSRadius, CSTacacs 및 CSAuth 서비스를 실행할 수 있습니다.

참고: Windows NT용 Cisco Secure 서비스가 명령줄 모드에서 실행 중인 경우 GUI 액세스가 제한됩니다.

CSRadius, CSTacacs 또는 CSAuth 디버그 정보를 얻으려면 DOS 창을 열고 Windows 속성 화면 버퍼 높이를 300으로 조정합니다.

CSRadius에 대해 다음 명령을 사용합니다.

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

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

CSTacacs에 대해 다음 명령을 사용합니다.

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

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

Windows NT AAA용 Cisco Secure 복제 디버그 정보 가져오기

복제 문제를 해결하는 경우 명령줄 모드에서 Windows NT CSAuth 서비스를 실행할 수 있습니다.

참고: Windows NT용 Cisco Secure 서비스가 명령줄 모드에서 실행 중인 경우 GUI 액세스가 제한됩니다.

CSAuth 복제 디버그 정보를 얻으려면 DOS 창을 열고 Windows 속성 화면 버퍼 높이를 300으로 조정합니다.

소스 및 대상 서버 모두에서 CSAuth에 다음 명령을 사용합니다.

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

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

debug는 명령 프롬프트 창에 기록되고 $BASE\csauth\logs\auth.log 파일에도 기록됩니다.

오프라인으로 사용자 인증 테스트

사용자 인증은 CLI(Command Line Interface)를 통해 테스트할 수 있습니다. RADIUS는 "radtest"로 테스트할 수 있으며 TACACS+는 "tactest"로 테스트할 수 있습니다. 이 테스트는 통신 디바이스에서 유용한 디버그 정보를 생성하지 않거나 Cisco Secure ACS Windows 문제가 있는지 디바이스 문제가 있는지 묻는 질문이 있는 경우 유용할 수 있습니다. radtest 및 tactest 모두 $BASE\utils 디렉토리에 있습니다. 다음은 각 테스트의 예입니다.

Radtest를 사용하여 오프라인으로 RADIUS 사용자 인증 테스트

```
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 pasword><>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.
```

Tactest를 사용하여 오프라인으로 TACACS+ 사용자 인증 테스트

```
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>
```

Windows 2000/NT 데이터베이스 실패 이유 결정

인증이 Windows 2000/NT로 전달되고 있지만 실패하는 경우 Programs(프로그램) > Administrative Tools(관리 도구) > User Manager for Domains(**도메인**의 **사용자 관리자), Policies(정책) > Audit(감사)**로 이동하여 Windows 감사 기능을 설정할 수 있습니다. Programs(**프로그램) > Administrative Tools(관리 툴) > Event Viewer(이벤트 뷰어)로** 이동하면 인증 실패가 표시됩니다. 실패한 시도 로그에서 발견된 실패는 아래 예와 같이 형식으로 표시됩니다.

```
NT/2000 authentication FAILED (error 1300L)
```

이러한 메시지는 Windows 2000 Event & Error Messages and Error Codes in Windows NT (Windows 2000 이벤트 및 오류 메시지 및 오류 코드)의 Microsoft 웹 사이트에서 조사할 수 있습니다.

1300L 오류 메시지는 아래와 같이 설명되어 있습니다.

```
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.
```

예

RADIUS 정상 인증

```
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 initialsed 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 retreive 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/recv errors   : 0
```

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

RADIUS 잘못된 인증

```
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 initialsed 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 retreive 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+ 양호한 인증

```
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+ 잘못된 인증(요약)

```
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>
```

관련 정보

- Technical Support - Cisco Systems