Obtaining Version and AAA Debug Information for Cisco Secure ACS for Windows

Document ID: 6434

Contents

Introduction

This document explains how to view the Cisco Secure ACS for Windows version and how to set up and obtain authentication, authorization, and accounting (AAA) debug information.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

There are no specific prerequisites for this document.

Components Used

The information in this document is based on Cisco Secure ACS for Windows 2.6.

Obtaining Cisco Secure for Windows Version Information

You can view version information by using the DOC commmand line or by using the GUI.

Using the DOS Command Line

To view the version number of Cisco Secure ACS for Windows through the command line option in DOS, use **cstacacs** or **csradius** followed by the **−v** for RADIUS and **−x** for TACACS+. See the examples below:

```
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
```

You may also see the version number of the Cisco Secure ACS program in the Windows registry. For example:

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

Using the GUI

To view the version with the Cisco Secure ACS GUI, go to the ACS home page. You can do this at any time by clicking the Cisco Systems logo in the top left corner of the screen. The lower half of the home page will display the full version.

Setting Cisco Secure ACS for Windows Debugging Levels

The following is an explanation of the different debugging options that are needed to obtain the maximum debugging information.

How to Set the Logging Level to Full in the ACS GUI

You will need to set ACS to log all messages. To do this, follow the steps listed below:

1. From the ACS home page, go to **Systems Configuration > Service Control**.
2. Under the Service Log File Configuration heading, set the level of detail to **Full**.

   You can modify the Generate New File and Manage Directory sections if needed.

System Configuration

How to Set Dr. Watson Logging

At the command prompt type **drwtsn32** and the Dr. Watson window will appear. Make sure that the options for **Dump All Thread Contexts** and **Dump Symbol Table** are checked.
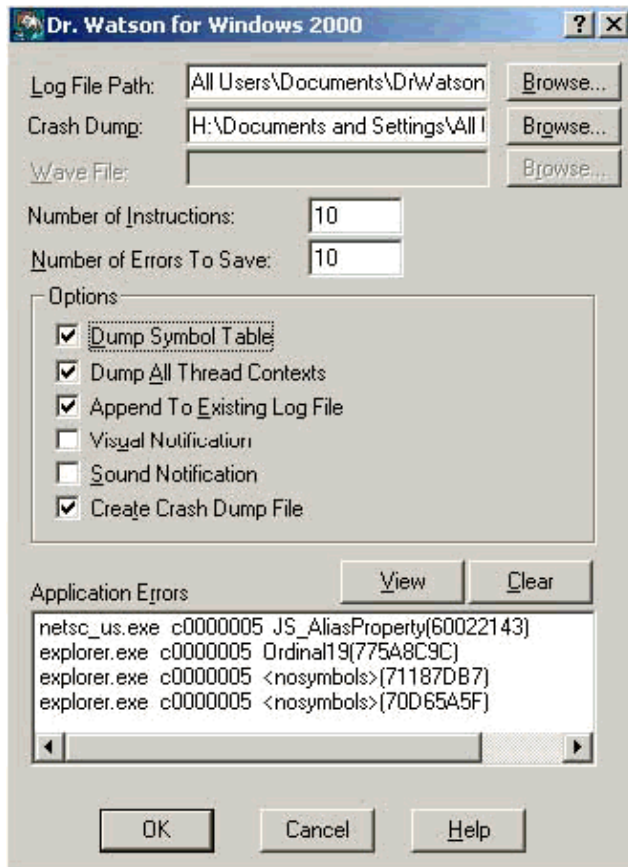
Creating a package.cab File

What Is the package.cab?

The package.cab is a Zip file that contains all the necessary files needed to troubleshoot ACS efficiently. You can use the CSSupport.exe utility to create the package.cab, or you can collect the files manually.

Creating a package.cab File with the CSSupport.exe Utility

If you are having an ACS problem for which you need to collect information, run the CSSupport.exe file as soon as possible after you see the problem. Use the DOS command line or Windows Explorer GUI to run CSSupport from C:\program files\Cisco Secure ACS v2.6\Utils>CSSupport.exe.

When you execute the CSSupport.exe file, the following window appears.

From this screen, you have two main options:

- Run Wizard, which leads you through a series of four steps:

  - ♦ Cisco Secure State Collector: Information Select
  - ♦ Cisco Secure State Collector: Installation Select
  - ♦ Cisco Secure State Collector: Log Verbosity
  - ♦ Cisco Secure State Collector (the actual collection)

  or
- Set Log Level Only, which allows you to skip the first few steps and go directly to the Cisco Secure State Collector: Log Verbosity screen

For a first−time setup, select **Run Wizard** to proceed through the steps needed to set the log. After the initial setup, you can use the **Set Log Levels Only** option to adjust the logging levels. Make your selection, and click **Next**.

Run Wizard

The following explains how to select information using the Run Wizard option.

1. **Cisco Secure State Collector: Information** Select

   All options should be selected by default except for User DB and Previous Logs. If you think that your problem is the user or group database, then select **User DB**. If you would like to have old logs included, select the option for **Previous Logs**. Click **Next** when you are finished.
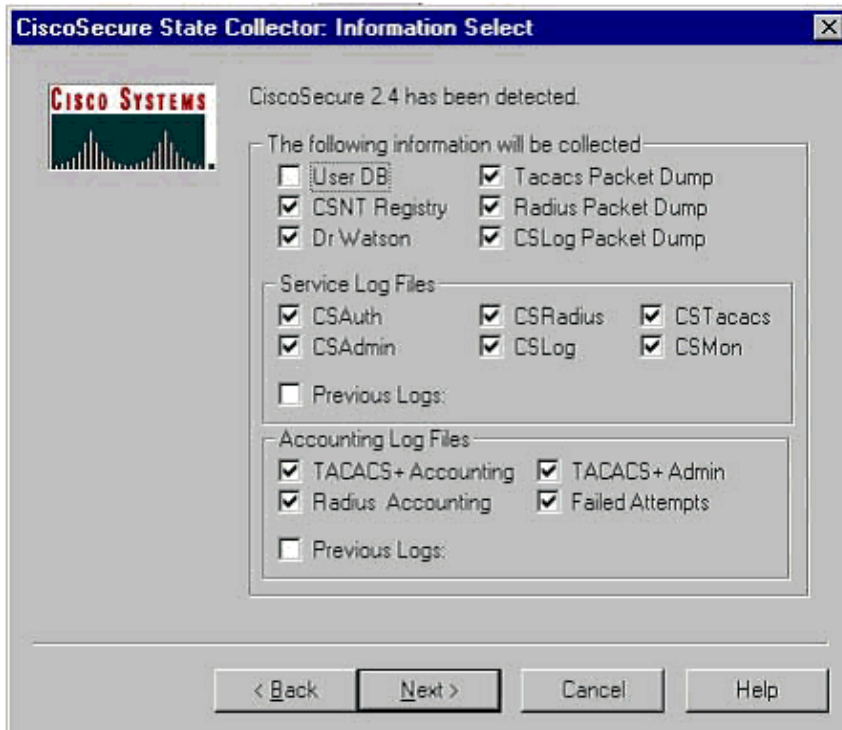
2. **Cisco Secure State Collector: Installation Select**

Choose the directory into which you want to place the package.cab. The default is C:\Program Files\Cisco Secure ACS v.26\Utils\Support. You may change this location if you desire. Make sure that the correct location of your Dr. Watson is specified. Running CSSupport requires that you start and stop the services. If you are sure that you want to stop and start the Cisco Secure services, click **Next** to continue.
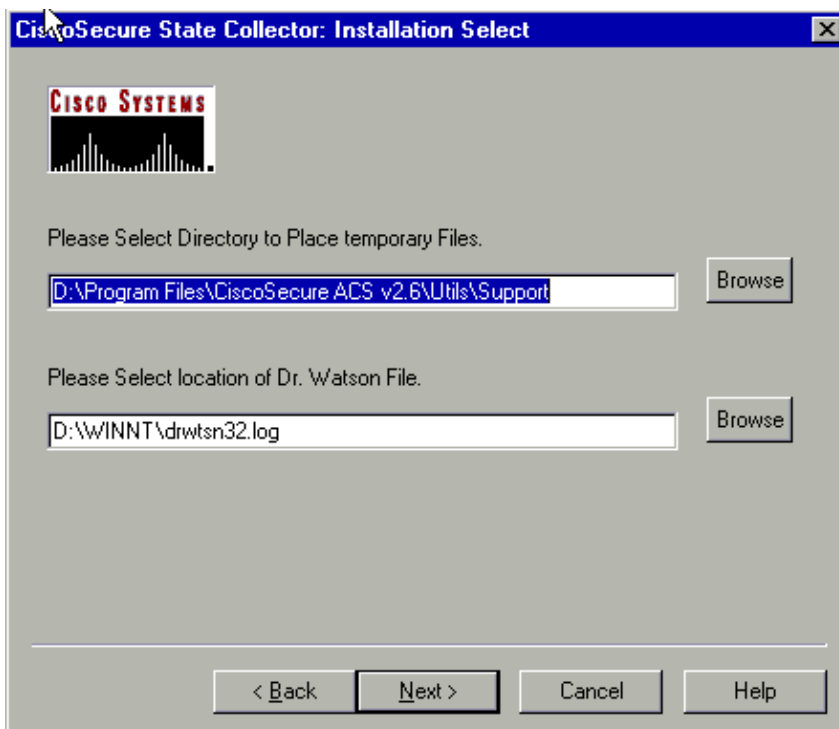
3. **Cisco Secure State Collector: Log Verbosity**

Select the option for **Set Diagnostic Log Verbosity to maximum level for all services**. Under the Diagnostic Packet Capture heading, select either TACACS+ or RADIUS, depending on what you are running. Select the **Keep CSLog Packet Capture** option. When you are finished, click **Next**.

Note: If you want to have logs from previous days, you must select the option for **Previous Logs** option in step 1 and then set the number of days you want to go back.
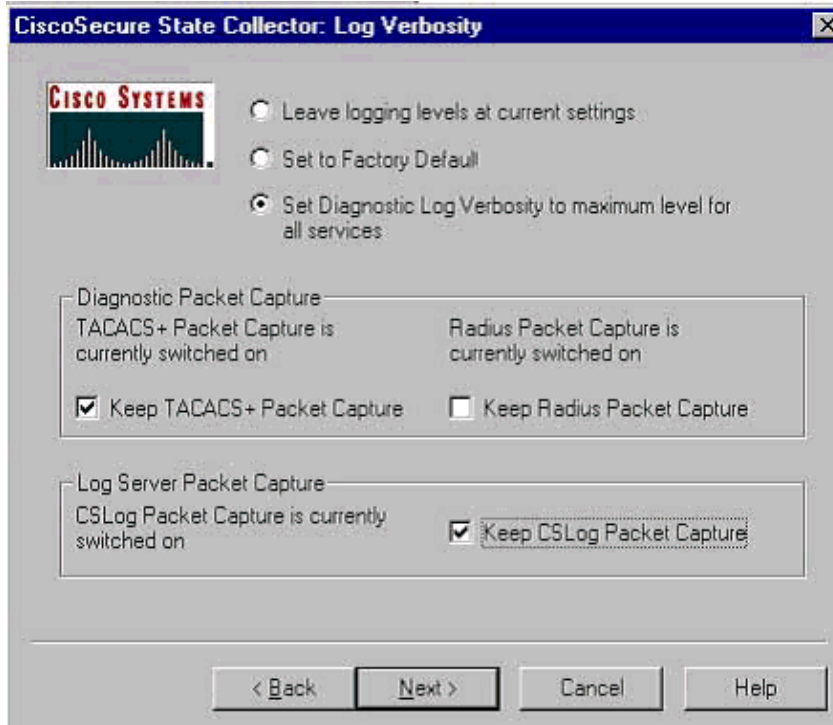
4. **Cisco Secure State Collector**

You will see a warning that states that when you continue, your services will be stopped and then restarted. This interruption is necessary for CSSupport to grab all of the needed files. The down time should be minimal. You will be able to watch the services stop and restart on this window. Click **Next** to proceed.
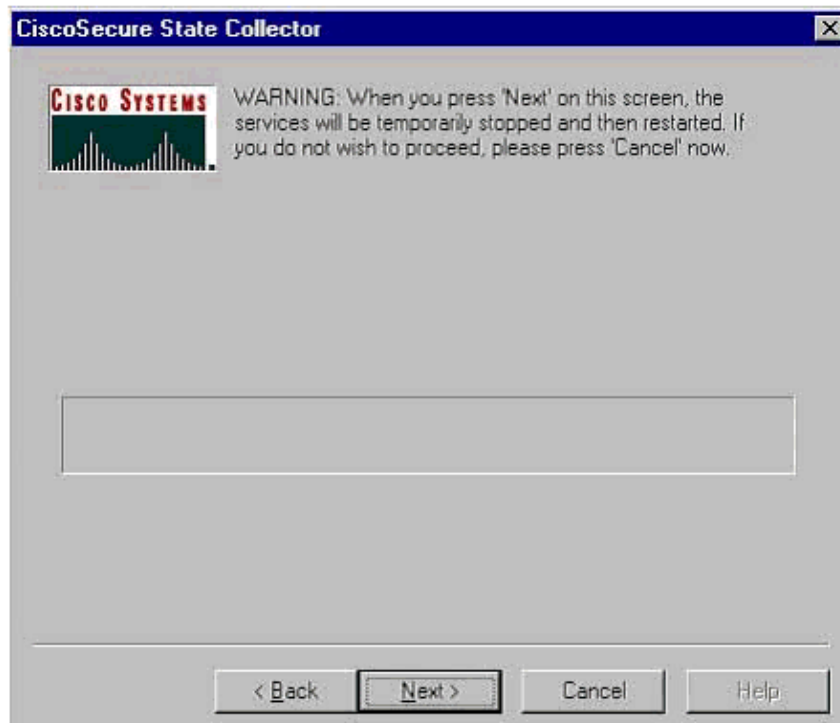
When the services restart, the package.cab can be found in the location specified. Click **Finish**, and your package.cab file is ready.

Browse to the location that you specified for the package.cab and relocate it to a directory where it can be saved. Your technical support engineer may request it at any time during the troubleshooting process.

Set Log Levels Only

If you have previously run the State Collector and only need to change the logging levels, you can use the Set Log Levels Only option to skip to the Cisco Secure State Collector: Log Verbosity screen, where you set the diagnostic packet capture. When you click **Next**, you will go directly to the Warning page. Then click **Next** again to stop the service, gather the file, and restart the services.

Collecting a package.cab File Manually

The following is a list of the files that are compiled into a package.cab. If the CSSupport is not functioning properly, you can gather these files using Windows Explorer.

```
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
```

Obtaining Cisco Secure for Windows NT AAA Debug Information

The Windows NT CSRadius, CSTacacs, and CSAuth services may be run in the command line mode when you are troubleshooting a problem.

Note: The GUI access is limited if any Cisco Secure for Windows NT services are running in the command line mode.

To obtain CSRadius, CSTacacs, or CSAuth debug information, open a DOS window and adjust the Windows property Screen Buffer height to 300.

Use the following commands for CSRadius:

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

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

Use the following commands for CSTacacs:

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

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

Obtaining Cisco Secure for Windows NT AAA Replication Debug Information

The Windows NT CSAuth services may be run in the command line mode when you are troubleshooting a replication problem.

Note: The GUI access is limited if any Cisco Secure for Windows NT services are running in the command line mode.

To obtain CSAuth replication debug information, open a DOS window and adjust the Windows property Screen Buffer height to 300.

Use the following commands for CSAuth on both the source and the target servers:

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

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

The debug is written to the command prompt window, and it also goes in the $BASE\csauth\logs\auth.log file.

Testing User Authentication Offline

User authentication may be tested through the command−line interface (CLI). RADIUS can be tested with "radtest," and TACACS+ can be tested with "tactest." This tests can be useful if the communicating device is not producing useful debug information, and if there is some question as to whether there is a Cisco Secure ACS Windows problem or a device problem. Both radtest and tactest are located in the $BASE\utils directory. The following are examples of each test.

Testing RADIUS User Authentication Offline with 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 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.
```

Testing TACACS+ User Authentication Offline with Tactest

```
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>
```

Determining Reasons for Windows 2000/NT Database Failures

If authentication is being passed to Windows 2000/NT but is failing, you can turn on the Windows audit facility by going to **Programs > Administrative Tools > User Manager for Domains, Policies > Audit**. Going to **Programs > Administrative Tools > Event Viewer** shows authentication failures. Failures found in the log of failed attempts are displayed in a format as shown in the example below.

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

These messages can be researched on Microsoft's website at Windows 2000 Event & Error Messages and Error Codes in Windows NT .

The 1300L error message is described as shown below.

```
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.

Examples

RADIUS Good Authentication

```
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 Bad Authentication

```
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+ Good Authentication

```
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+ Bad Authentication (Summarized)

```
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>
```

Related Information

- **Documentation for Cisco Secure ACS for Windows**
- **Technical Support – Cisco Systems**

Updated: Nov 11, 2002

Document ID: 6434