

获取 Cisco Secure ACS for Windows 的版本和 AAA 调试信息

目录

[简介](#)

[开始使用前](#)

[规则](#)

[先决条件](#)

[使用的组件](#)

[获取Cisco Secure for Windows版本信息](#)

[使用DOS命令行](#)

[使用GUI](#)

[为Windows调试级别设置Cisco Secure ACS](#)

[如何在ACS GUI中将日志记录级别设置为“完全”](#)

[如何设置Dr. Watson日志记录](#)

[创建package.cab文件](#)

[包.cab是什么？](#)

[使用CSSupport.exe实用程序创建package.cab文件](#)

[手动收集package.cab文件](#)

[获取Cisco Secure for Windows NT AAA调试信息](#)

[获取Cisco Secure for Windows NT AAA复制调试信息](#)

[离线测试用户身份验证](#)

[确定Windows 2000/NT数据库故障的原因](#)

[Examples](#)

[RADIUS良好身份验证](#)

[RADIUS错误身份验证](#)

[TACACS+良好身份验证](#)

[TACACS+错误身份验证 \(总结 \)](#)

[相关信息](#)

[简介](#)

本文档介绍如何查看Cisco Secure ACS for Windows版本，以及如何设置和获取身份验证、授权和记帐(AAA)调试信息。

[开始使用前](#)

[规则](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

[先决条件](#)

本文档没有任何特定的前提条件。

[使用的组件](#)

本文档中的信息基于Cisco Secure ACS for Windows 2.6。

[获取Cisco Secure for Windows版本信息](#)

您可以使用DOC命令行或使用GUI查看版本信息。

[使用DOS命令行](#)

要通过DOS中的命令行选项查看Cisco Secure ACS for Windows的版本号，请使用**cstacacs**或**csradius**，后跟**-v**和**-x**来查看RADIUS和TACACS+。请参阅以下示例：

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

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

您还可以在Windows注册表中看到Cisco Secure ACS程序的版本号。例如：

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

[使用GUI](#)

要使用思科安全ACS GUI查看版本，请转至ACS主页。您可以随时单击屏幕左上角的思科系统徽标执行此操作。主页的下半部分将显示完整版本。

[为Windows调试级别设置Cisco Secure ACS](#)


以下是获取最大调试信息所需的不同调试选项的说明。


[如何在ACS GUI中将日志记录级别设置为“完全”](#)

您需要设置ACS以记录所有消息。为此，请执行以下步骤：

1. 从ACS主页，转到Systems Configuration > Service Control。
2. 在“服务日志文件配置”标题下，将详细级别设置为“完整”。如果需要，可以修改“生成新文件”和“管理目录”部分。

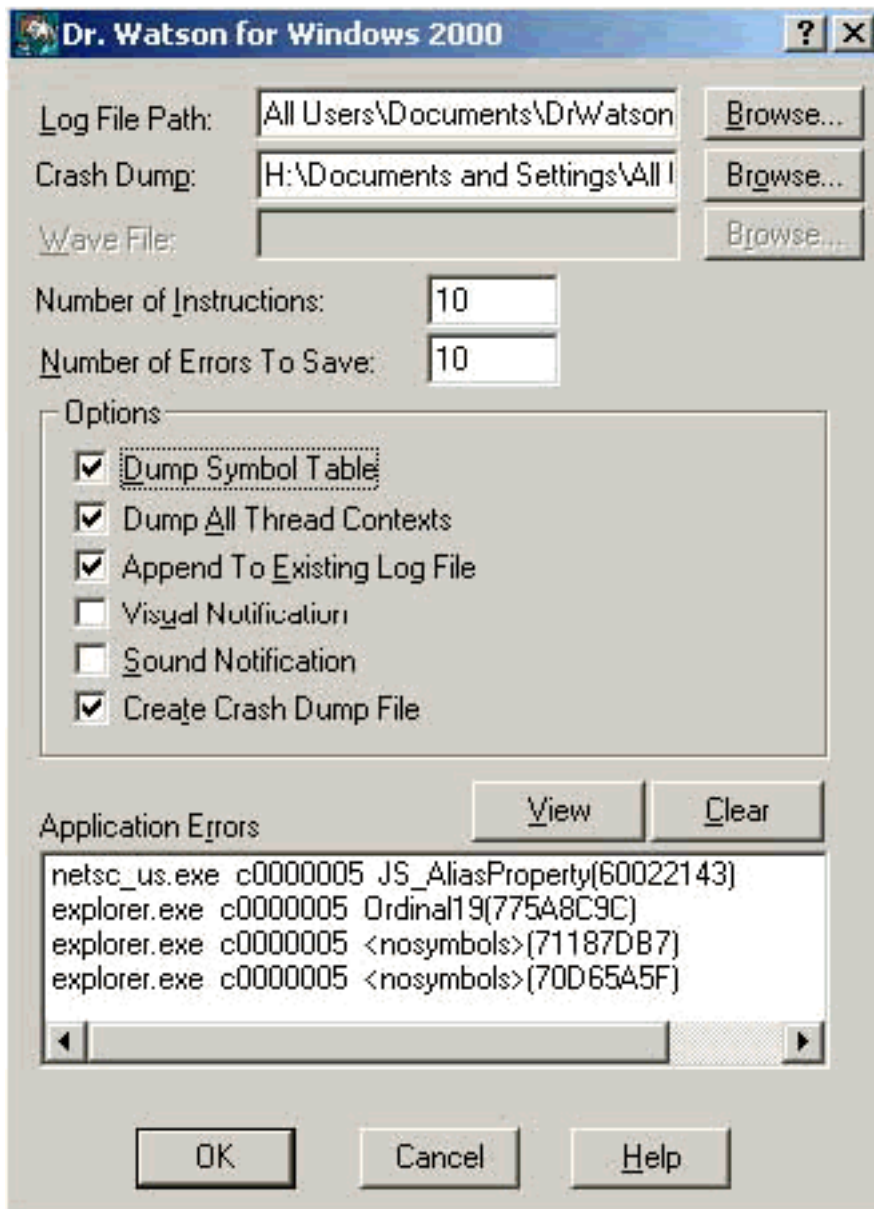
System Configuration

CiscoSecure ACS on mhammon-pc 	
Is Currently Running	

Services Log File Configuration 	
Level of detail	
<input type="radio"/> None	
<input type="radio"/> Low	
<input checked="" type="radio"/> Full	
Generate New File	
<input checked="" type="radio"/> Every day	
<input type="radio"/> Every week	
<input type="radio"/> Every month	
<input type="radio"/> When size is greater than <input type="text" value="2048"/> KB	
<input type="checkbox"/> Manage Directory	
<input type="radio"/> Keep only the last <input type="text" value="7"/> files	
<input checked="" type="radio"/> Delete files older than <input type="text" value="7"/> days	

[如何设置Dr. Watson日志记录](#)

在命令提示符下，键入`drwtsn32`，并出现“Dr. Watson(Dr. Watson)”窗口。确保选中了“转储所有线程上下文”和“转储符号表”选项。



[创建package.cab文件](#)

[包.cab是什么？](#)

package.cab是一个Zip文件，包含有效排除ACS故障所需的所有必要文件。可以使用CSSupport.exe 实用程序创建 package.cab，也可以手动收集文件。

[使用CSSupport.exe实用程序创建package.cab文件](#)

如果您遇到需要收集信息的ACS问题，请在您看到问题后尽快运行CSSupport.exe文件。使用DOS命令行或Windows资源管理器GUI从C:\program files\Cisco Secure ACS v2.6\Utils>CSSupport.exe运行CSSupport。

执行CSSupport.exe文件时，将显示以下窗口。



在此屏幕中，您有两个主要选项：

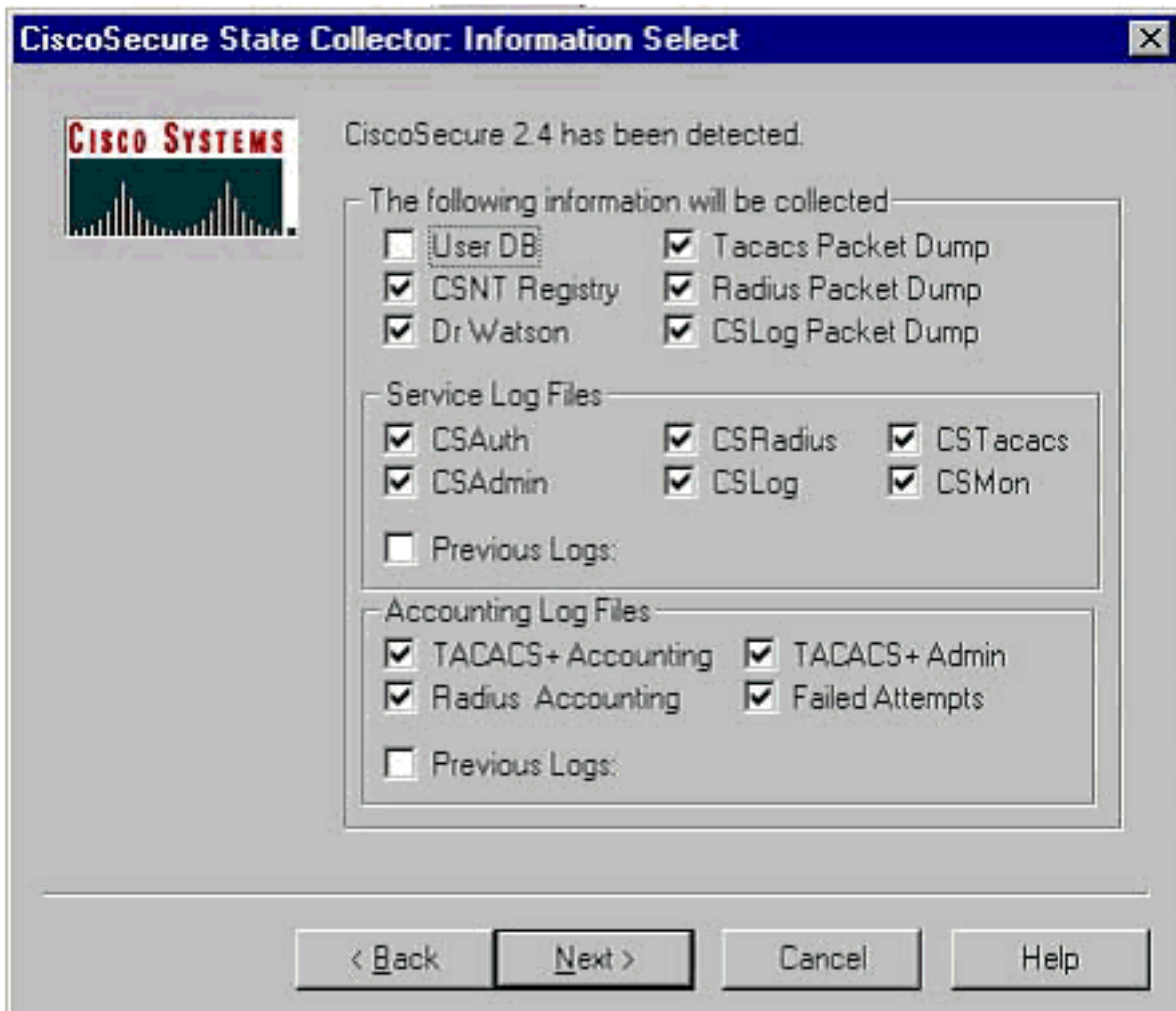
- [运行向导](#)，引导您完成一系列四个步骤：思科安全状态收集器：信息选择思科安全状态收集器：安装选择思科安全状态收集器：日志详细程度思科安全状态收集器（实际收集）或
- [Set Log Level Only](#)（仅设置日志级别），允许您跳过前几个步骤并直接转到Cisco Secure State Collector:日志详细性屏幕

对于首次设置，请选择“[运行向导](#)”以继续执行设置日志所需的步骤。在初始设置后，您可以使用“[仅设置日志级别](#)”选项来调整日志记录级别。进行选择，然后单击“[下一步](#)”。

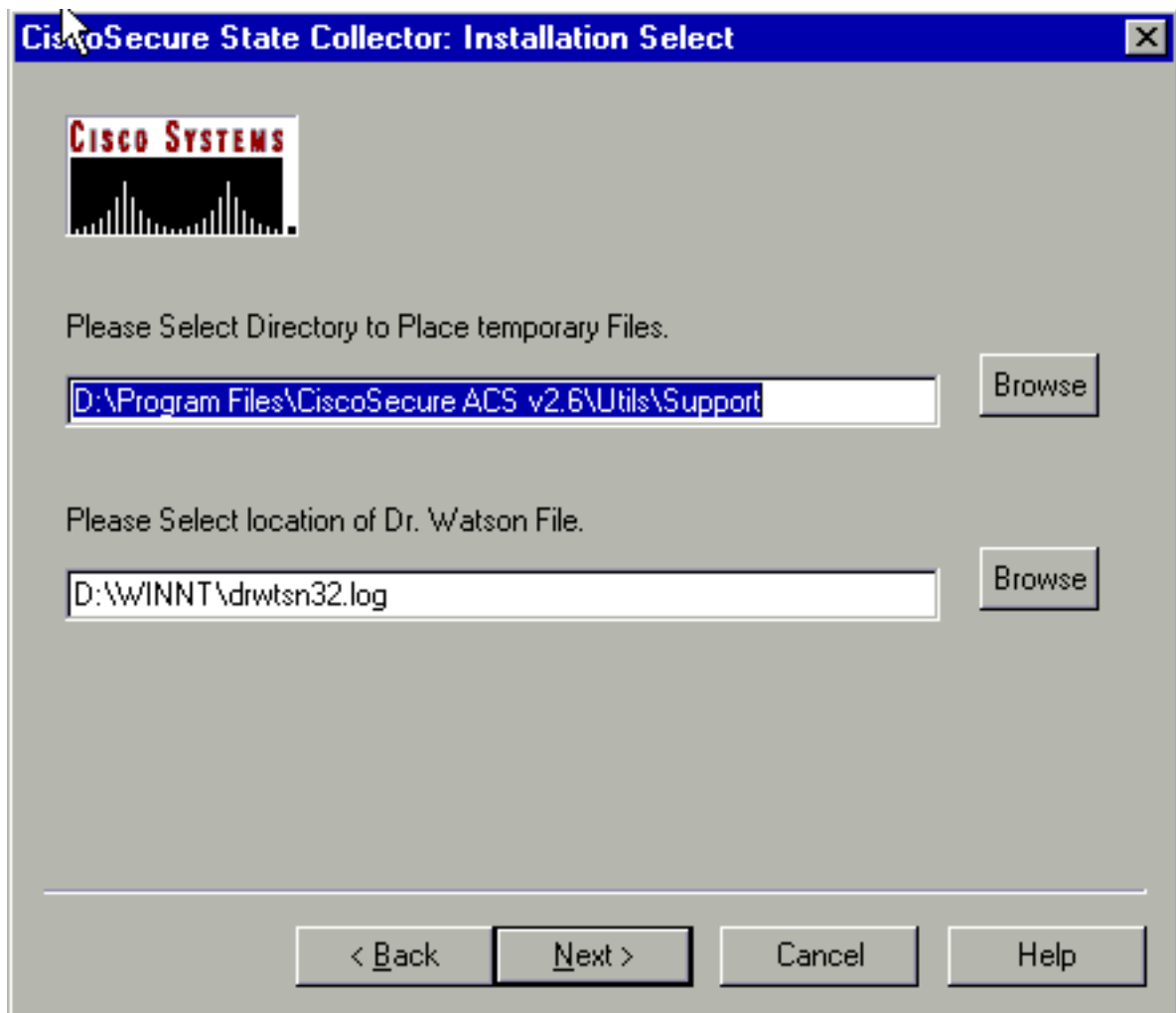
[运行向导](#)

以下说明如何使用运行向导选项选择信息。

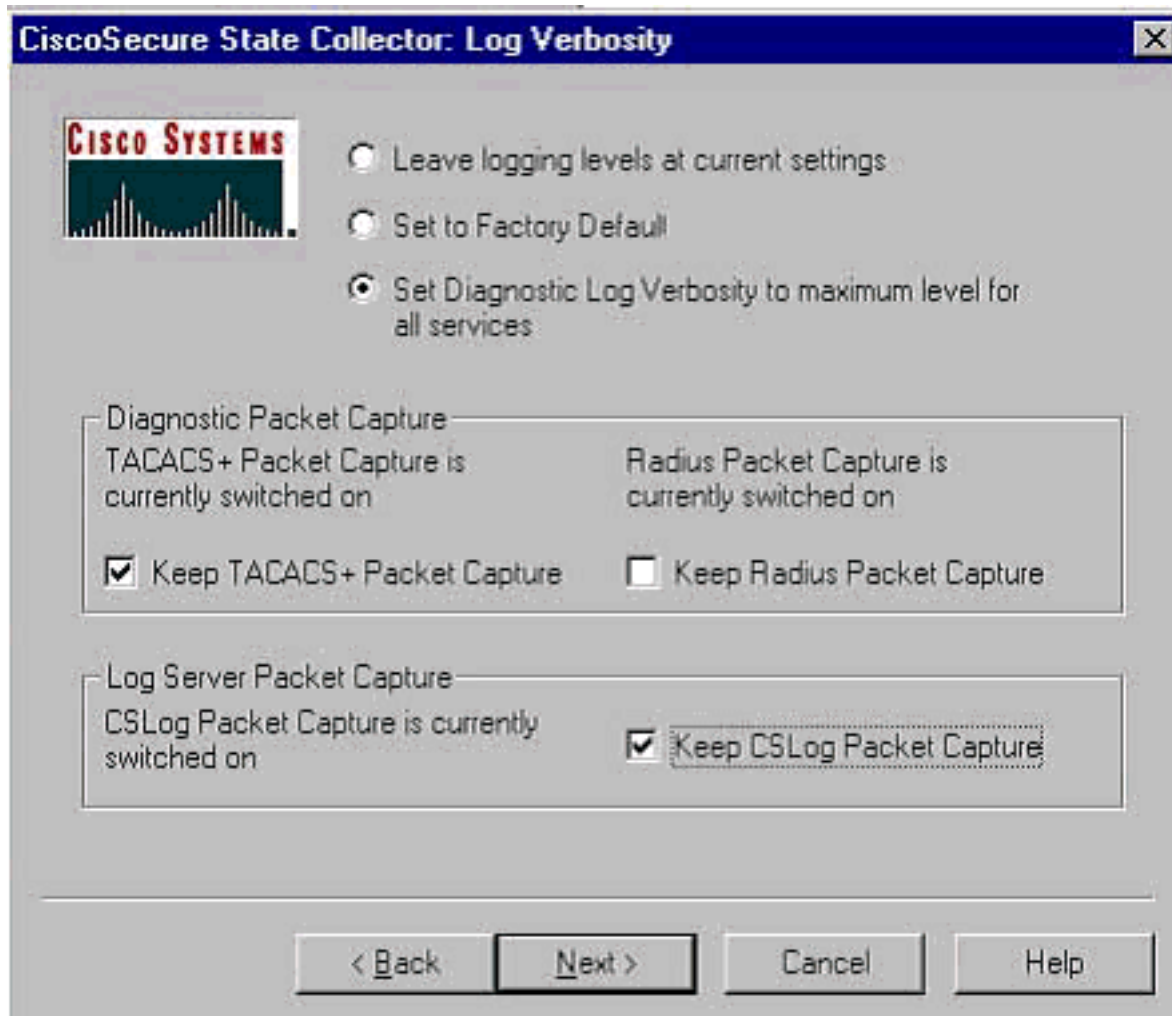
1. **思科安全状态收集器：信息选择**除用户数据库和以前的日志外，默认情况下应选择所有选项。如果您认为问题出在用户或组数据库上，则选择“**用户数据库**”。如果要包含旧日志，请选择“**Previous Logs**”选项。完成后单击“**下一步**”。



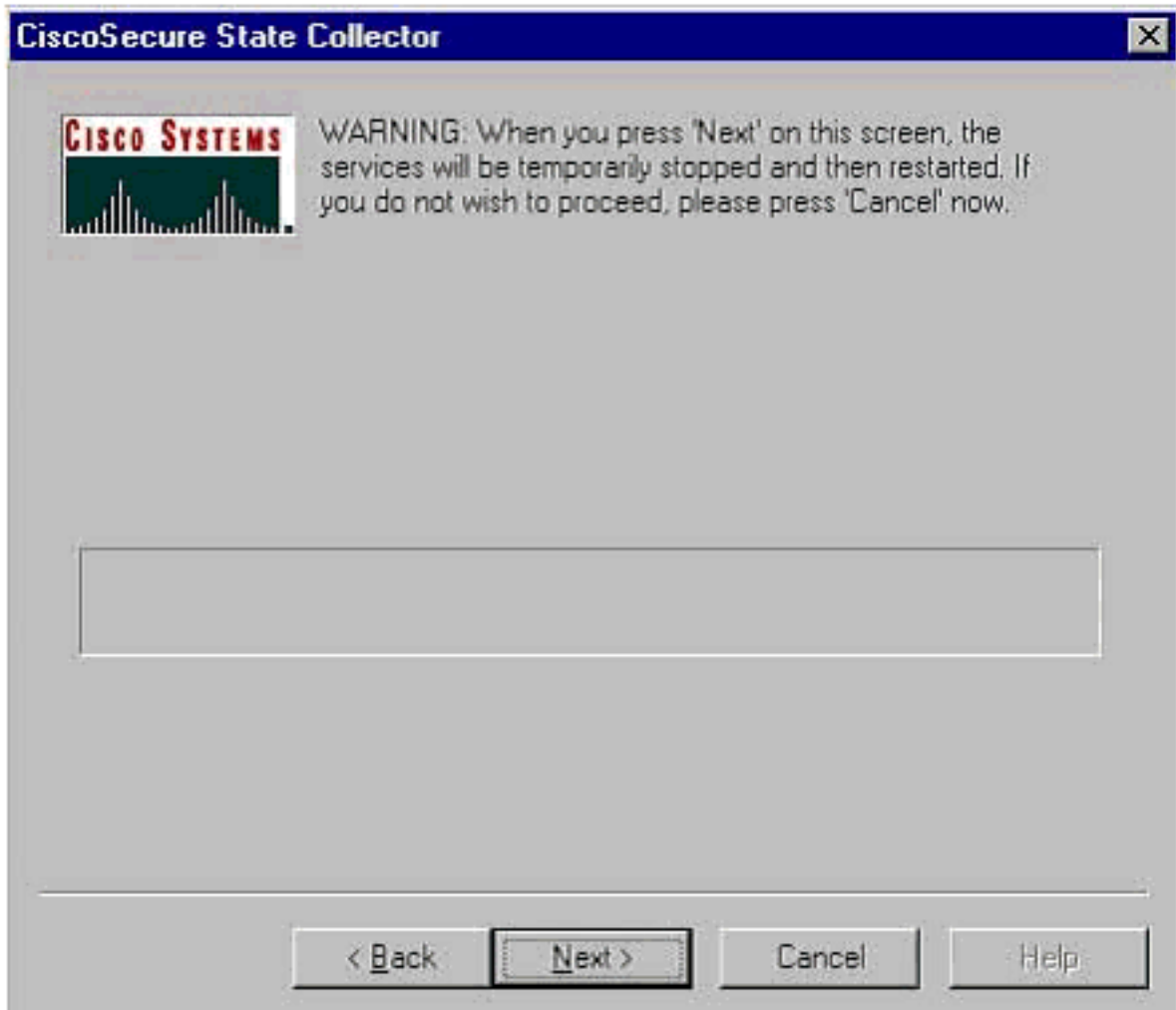
2. **思科安全状态收集器：安装选择**选择要将package.cab放入的目录。默认值为C:\Program Files\Cisco Secure ACS v.26\Utils\Support。如果需要，可以更改此位置。确保指定了Dr. Watson的正确位置。运行CSSupport需要启动和停止服务。如果确定要停止并启动思科安全服务，请单击“下一步”继续。



3. 思科安全状态收集器：日志详细程度选择将诊断日志详细性设置为所有服务的最大级别的选项。在Diagnostic Packet Capture标题下，根据您正在运行的内容选择TACACS+或RADIUS。选择Keep CSLog Packet Capture选项。完成后，单击“下一步”。注：如果要使用前几天的日志，则必须在步骤1中为“上一个日志”选项选择选项，然后设置要返回的天数。



4. **思科安全状态收集器**您将看到警告，指出当您继续时，服务将停止，然后重新启动。CSSupport需要此中断才能获取所有所需文件。停机时间应该最小。您将能够在此窗口中观看服务停止并重新启动。单击 Next (下一步) 继续。



重新启动

服务后，可在指定的位置找到package.cab。单击Finish，您的package.cab文件就绪。浏览到您为package.cab指定的位置，并将其重新定位到可以保存该位置的目录。在故障排除过程中，您的技术支持工程师可随时请求。

[仅设置日志级别](#)

如果您以前运行过状态收集器，并且只需更改日志记录级别，则可以使用“仅设置日志级别”选项跳至思科安全状态收集器：[Log Verbosity\(日志详细性\)](#)屏幕，在此设置诊断数据包捕获。单击“下一步”后，将直接转到“警告”页。然后再次单击“下一步”以停止服务、收集文件并重新启动服务。

[手动收集package.cab文件](#)

以下是编译到package.cab中的文件列表。如果CSSupport无法正常运行，您可以使用Windows资源管理器收集这些文件。

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
(drwtasn32.log) See section 3 for further details

[获取Cisco Secure for Windows NT AAA调试信息](#)

当您排除故障时，Windows NT CSRADIUS、CSTacacs和CSAuth服务可能会在命令行模式下运行。

注意：如果任何Cisco Secure for Windows NT服务在命令行模式下运行，则GUI访问受限。

要获取CSRADIUS、CSTacacs或CSAuth调试信息，请打开DOS窗口并将Windows属性的屏幕缓冲区高度调整为300。

对CSRADIUS使用以下命令：

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

对CSTacacs使用以下命令：

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

[获取Cisco Secure for Windows NT AAA复制调试信息](#)

在排除复制问题故障时，Windows NT CSAuth服务可能会在命令行模式下运行。

注意：如果任何Cisco Secure for Windows NT服务在命令行模式下运行，则GUI访问受限。

要获取CSAuth复制调试信息，请打开DOS窗口并将Windows属性的屏幕缓冲区高度调整为300。

在源服务器和目标服务器上对CSAuth使用以下命令：

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

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

调试将写入命令提示符窗口，并进入\$BASE\csauth\logs\auth.log文件。

[离线测试用户身份验证](#)

用户身份验证可通过命令行界面(CLI)进行测试。RADIUS可以使用“radtest”测试，TACACS+可以使用“tactest”测试。如果通信设备未生成有用的调试信息，并且对Cisco Secure ACS Windows问题或设备问题有疑问，则此测试非常有用。radtest和tactest都位于\$BASE\utils目录中。以下是每个测试的示例。

[使用Radtest离线测试RADIUS用户身份验证](#)

```
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.
```

[使用Tactest离线测试TACACS+用户身份验证](#)

```
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>
```

确定Windows 2000/NT数据库故障的原因

如果身份验证被传递到Windows 2000/NT但失败，您可以通过转到**程序>管理工具>域用户管理器、策略>审核**来打开Windows审核工具。转到**程序>管理工具>事件查看器**显示身份验证失败。失败尝试日志中发现的失败以如下例所示的格式显示。

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

这些消息可在Microsoft网站的Windows 2000 Event & Error Messages和[Error Codes in Windows NT\(Windows 2000事件和错误消息](#) 和[Windows NT中的错误代码](#))上进行研究。

1300L错误消息如下所示。

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良好身份验证

```
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/recvd errors  : 0
```

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

RADIUS错误身份验证

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\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=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/rcv errors    : 0

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

TACACS+良好身份验证

```
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+错误身份验证 \(总结\)](#)

```
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>
```

[相关信息](#)

- [技术支持 - Cisco Systems](#)