

獲取適用於Windows的Cisco Secure ACS的版本和AAA調試資訊

目錄

[簡介](#)

[開始之前](#)

[慣例](#)

[必要條件](#)

[採用元件](#)

[獲取Cisco Secure for Windows版本資訊](#)

[使用DOS命令列](#)

[使用GUI](#)

[為Windows調試級別設定Cisco Secure ACS](#)

[如何在ACS GUI中將日誌記錄級別設定為Full](#)

[如何設定Dr. Watson日誌記錄](#)

[建立package.cab檔案](#)

[包裹是什麼？](#)

[使用CSSupport.exe實用程式建立package.cab檔案](#)

[手動收集package.cab檔案](#)

[獲取Cisco Secure for Windows NT AAA調試資訊](#)

[獲取Cisco Secure for Windows NT AAA複製調試資訊](#)

[離線測試使用者身份驗證](#)

[確定Windows 2000/NT資料庫失敗的原因](#)

[範例](#)

[RADIUS良好驗證](#)

[RADIUS錯誤驗證](#)

[TACACS+良好驗證](#)

[TACACS+錯誤驗證 \(摘要\)](#)

[相關資訊](#)

簡介

本文說明如何檢視適用於Windows的Cisco Secure ACS版本，以及如何設定和取得驗證、授權和計量(AAA)偵錯資訊。

開始之前

慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

[必要條件](#)

本文件沒有特定先決條件。

[採用元件](#)

本檔案中的資訊是根據適用於Windows 2.6的Cisco Secure ACS。

[獲取Cisco Secure for Windows版本資訊](#)

可以使用DOC命令列或使用GUI檢視版本資訊。

[使用DOS命令列](#)

要通過DOS中的命令列選項檢視Cisco Secure ACS for Windows的版本號，請使用**cstacacs**或**csradius**，然後使用**-v** for RADIUS和**-x** for TACACS+。請參閱以下示例：

```
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
```

您還可以在Windows登錄檔中看到Cisco Secure ACS程式的版本號。例如：

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

[使用GUI](#)

要使用Cisco Secure ACS GUI檢視版本，請轉到ACS首頁。您可以隨時按一下螢幕左上角的思科系統徽標。首頁的下半部分將顯示完整版本。

[為Windows調試級別設定Cisco Secure ACS](#)


以下是獲得最大調試資訊所需的不同調試選項的說明。


[如何在ACS GUI中將日誌記錄級別設定為Full](#)

您需要設定ACS以記錄所有消息。為此，請遵循下列步驟：

1. 在ACS首頁中，轉至**Systems Configuration > Service Control**。
2. 在「服務日誌檔案配置」標題下，將詳細級別設定為**完全**。如果需要，可以修改「生成新檔案」和「管理目錄」部分。

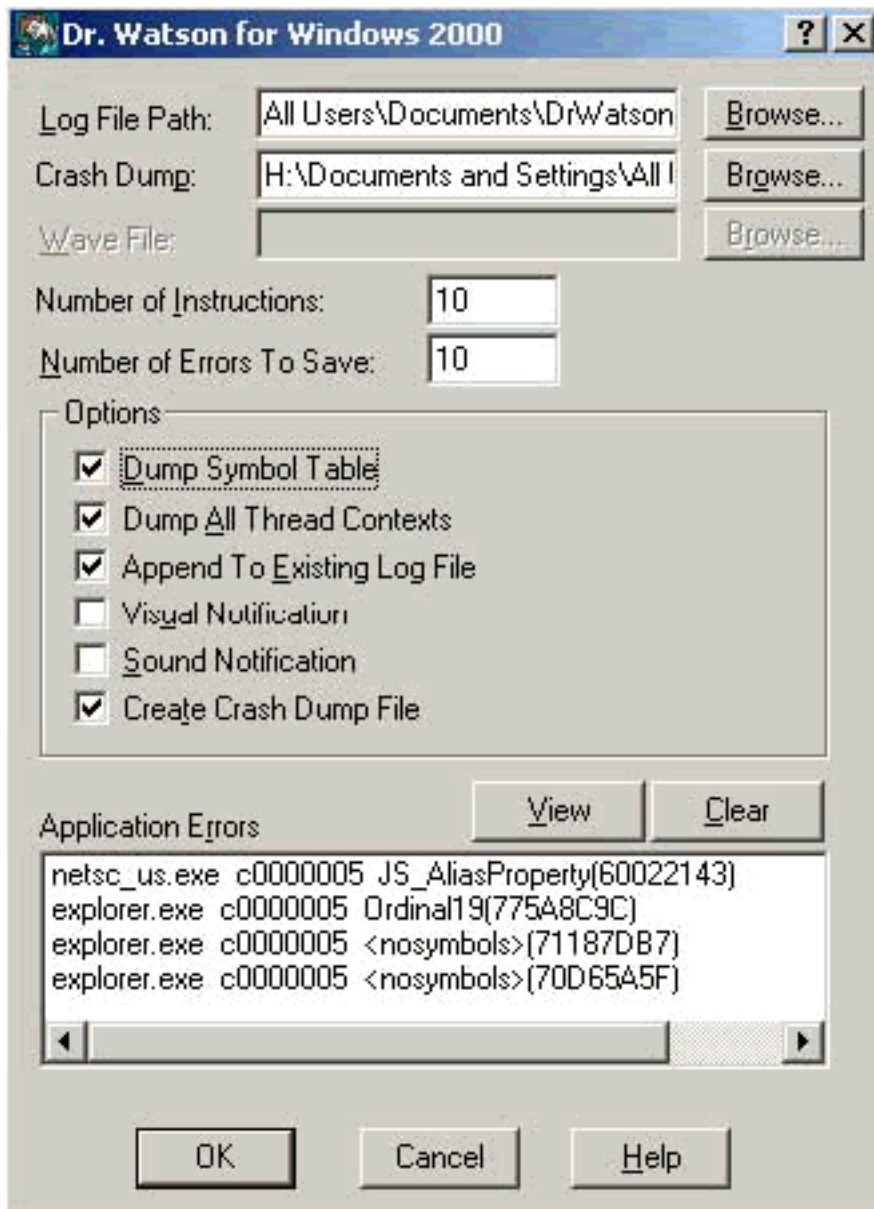
System Configuration

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	

[如何設定Dr. Watson日誌記錄](#)

在命令提示符下鍵入drwtsn32，將顯示Dr. Watson視窗。確保選中轉儲所有執行緒上下文和轉儲符號表的選項。



建立package.cab檔案

包裹是什麼？

package.cab是一個Zip檔案，其中包含對ACS進行高效故障排除所需的所有必要檔案。您可以使用CSSupport.exe實用程式建立package.cab，也可以手動收集檔案。

使用CSSupport.exe實用程式建立package.cab檔案

如果您的ACS問題需要收集資訊，請在發現問題後儘快運行CSSupport.exe檔案。使用DOS命令列或Windows資源管理器GUI從C:\program files\Cisco Secure ACS v2.6\Utils>CSSupport.exe運行CSSupport。

當您執行CSSupport.exe檔案時，將出現以下視窗。



在此螢幕中，有兩個主要選項：

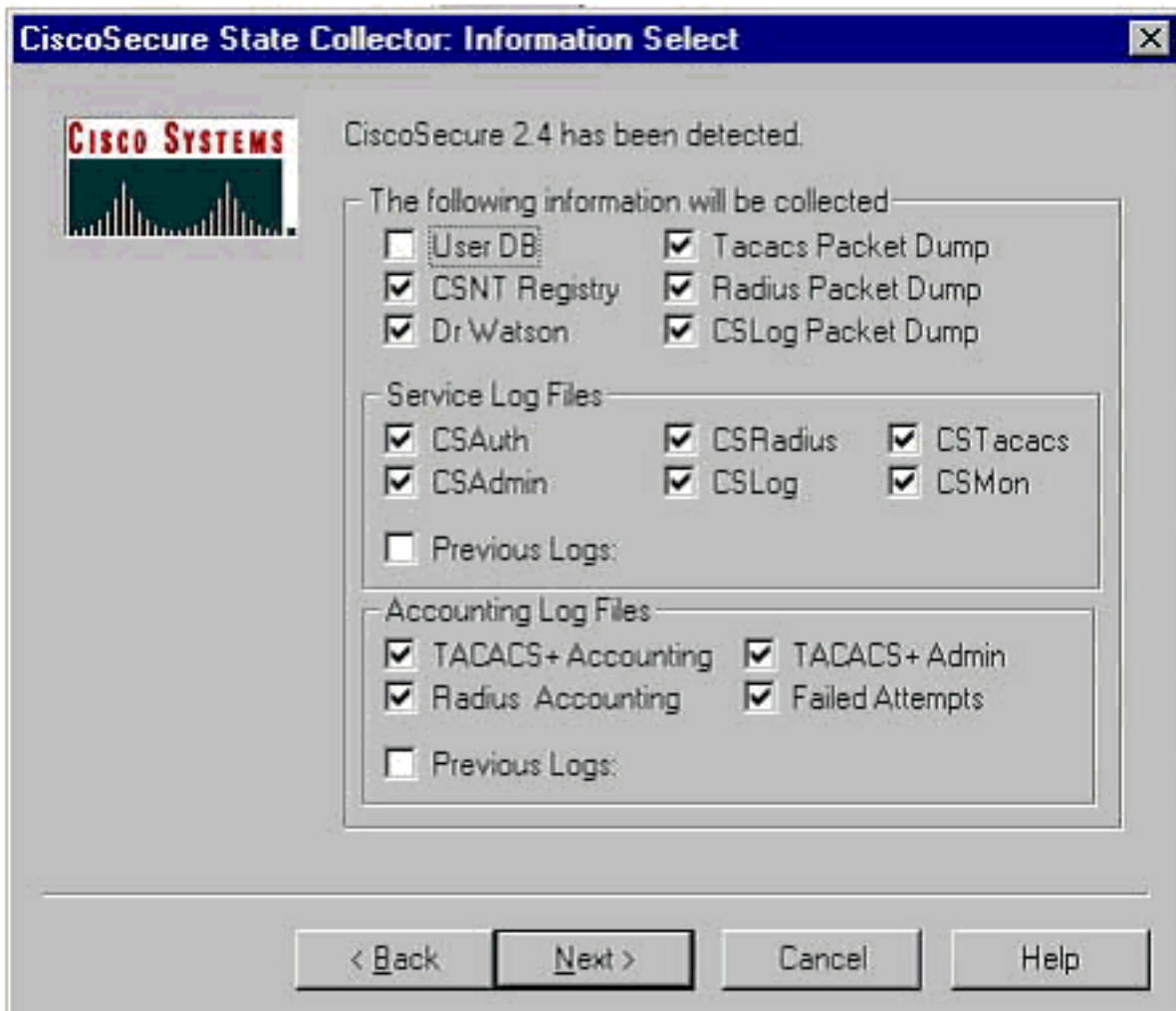
- [運行嚮導](#)，該嚮導引導您完成一系列四個步驟：思科安全狀態收集器：資訊選擇思科安全狀態收集器：安裝選擇思科安全狀態收集器：日誌詳細程度Cisco Secure State Collector (實際集合) 或
- [僅設定日誌級別](#)，這允許您跳過前幾個步驟並直接轉到Cisco安全狀態收集器：日誌詳細程度螢幕

對於首次設定，請選擇**運行嚮導**繼續執行設定日誌所需的步驟。初始設定後，可以使用**Set Log Levels Only**選項調整日誌記錄級別。進行選擇，然後按一下**下一步**。

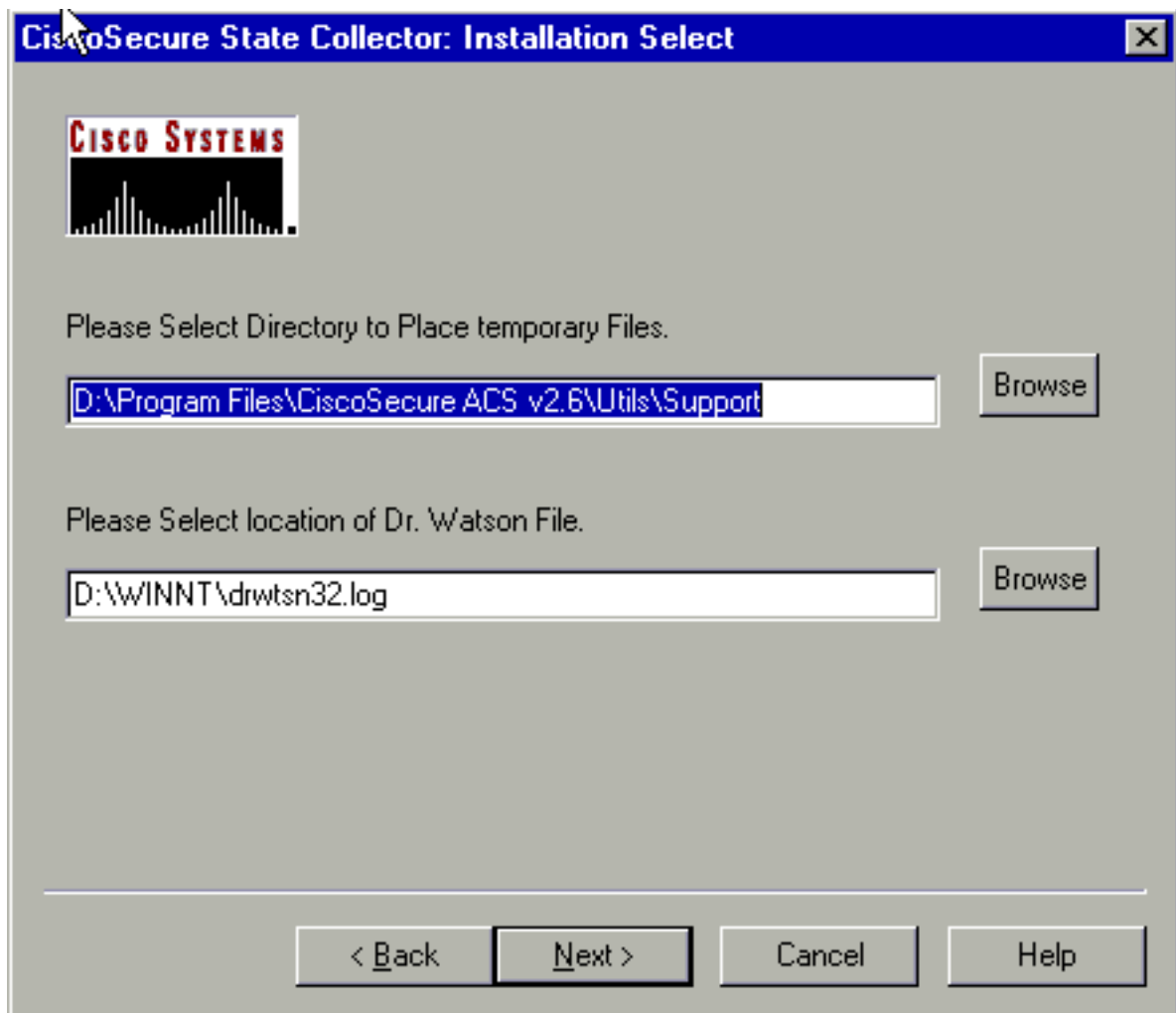
[運行嚮導](#)

下面說明了如何使用「運行嚮導」選項選擇資訊。

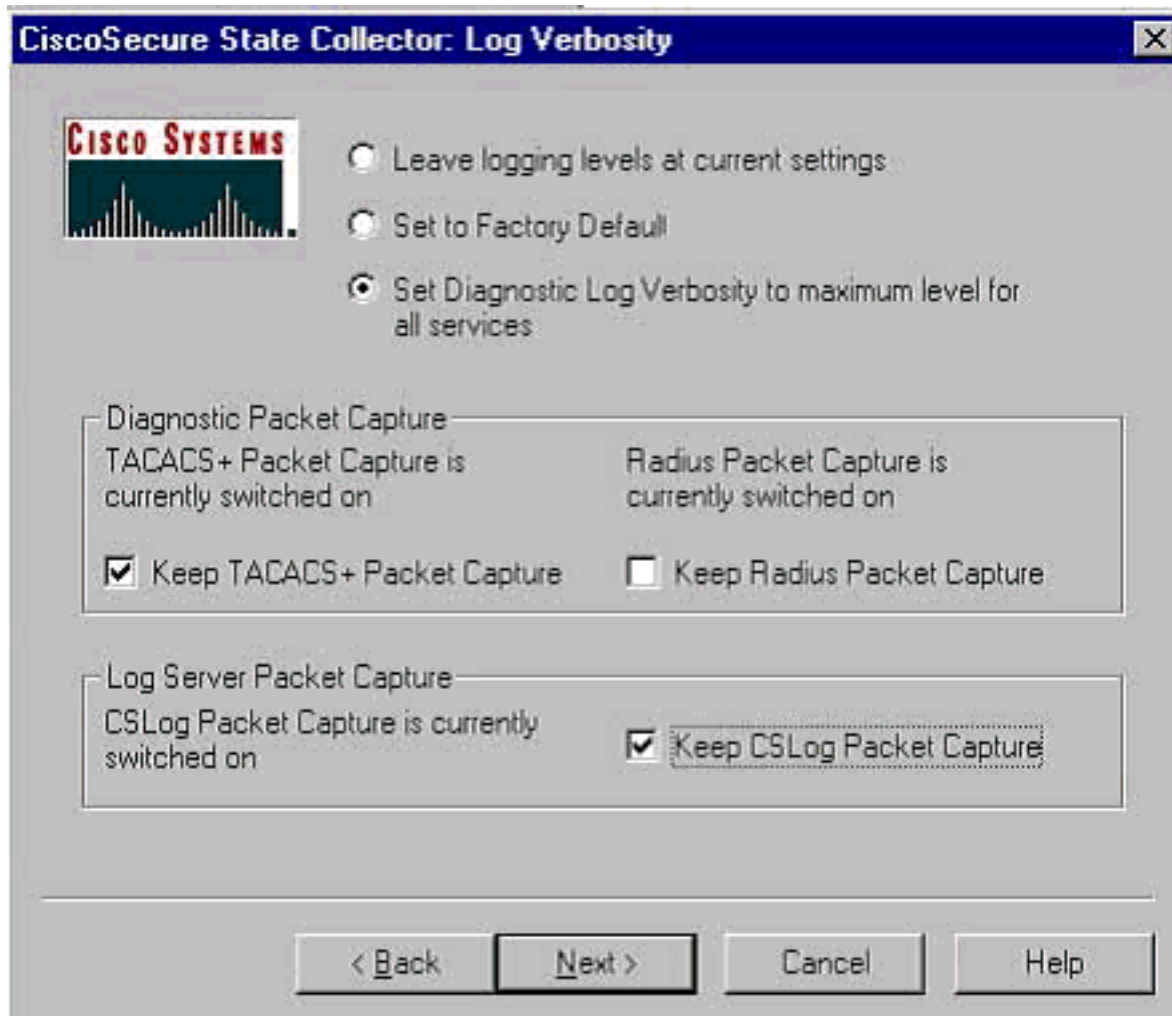
1. **思科安全狀態收集器：資訊選擇**預設情況下應選擇除「使用者資料庫」和「以前的日誌」之外的所有選項。如果您認為您的問題是使用者或組資料庫，請選擇**使用者資料庫**。如果您希望包含舊日誌，請選擇**Previous Logs**的**選項**。完成後按一下**Next**。



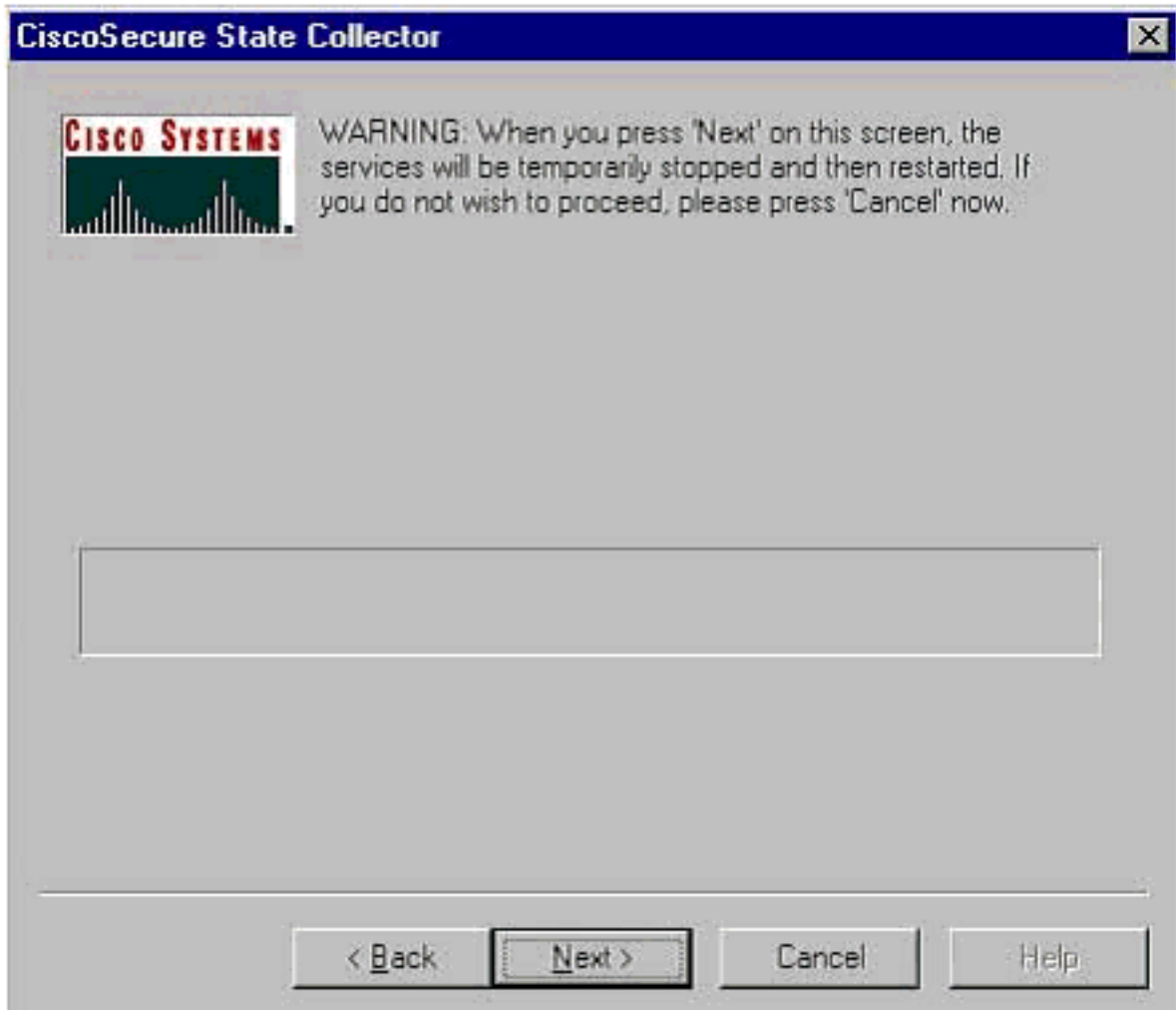
2. 思科安全狀態收集器：安裝選擇選擇要將package.cab放入的目錄。預設值為C:\Program Files\Cisco Secure ACS v.26\Utils\Support。如果需要，可以更改此位置。確保指定了您的Dr. Watson的正確位置。運行CSSupport需要啟動和停止服務。如果您確定要停止並啟動思科安全服務，請按一下下一步繼續。



3. 思科安全狀態收集器：日誌詳細程度選擇Set Diagnostic Log Verbosity to maximum level for all services的選項。在Diagnostic Packet Capture (診斷資料包捕獲) 標題下，選擇TACACS+或RADIUS (取決於您正在運行的專案)。選擇Keep CSLog Packet Capture選項。完成後，按一下下一步。**注意**：如果要具有前幾天的日誌，必須在步驟1中選擇Previous Logs選項，然後設定要返回的天數。



4. **思科安全狀態收集器**您將看到一條警告，指示當您繼續操作時，服務將停止然後重新啟動。CSSupport需要中斷才能獲取所有需要的檔案。停機時間應儘可能短。您將能夠在此視窗中看到服務停止和重新啟動。按一下**下一步**繼續。



服務重新啟動時，可以在指定的位置找到package.cab。按一下「Finish」，您的package.cab檔案就準備好了。瀏覽到為package.cab指定的位置，並將其重新定位到可以儲存該包的目錄。您的技術支援工程師可能會在故障排除過程中隨時提出請求。

僅設定日誌級別

如果您以前運行過狀態收集器，並且只需要更改日誌記錄級別，則可以使用「僅設定日誌級別」選項跳至[Cisco Secure State Collector:記錄詳細度](#)螢幕，可在其中設定診斷資料包捕獲。按一下下一步後，您將直接轉到「警告」頁面。然後再次按一下下一步以停止服務、收集檔案並重新啟動服務。

手動收集package.cab檔案

以下清單列出已編譯到package.cab中的檔案。如果CSSupport運行不正常，可以使用Windows資源管理器收集這些檔案。

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
```

[獲取Cisco Secure for Windows NT AAA調試資訊](#)

當您診斷問題時，Windows NT CSRADIUS、CSTacacs和CSAuth服務可能會在命令列模式下運行。

注意：如果任何Cisco Secure for Windows NT服務在命令列模式下運行，則GUI訪問會受到限制。

要獲取CSRADIUS、CSTacacs或CSAuth調試資訊，請開啟DOS視窗並將Windows屬性螢幕緩衝區高度調整為300。

對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
```

對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
```

[獲取Cisco Secure for Windows NT AAA複製調試資訊](#)

當您對複製問題進行故障排除時，Windows NT CSAuth服務可能在命令列模式下運行。

注意：如果任何Cisco Secure for Windows NT服務在命令列模式下運行，則GUI訪問會受到限制。

要獲取CSAuth複製調試資訊，請開啟DOS視窗並將Windows屬性螢幕緩衝區高度調整為300。

對源伺服器 and 目標伺服器上的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
```

debug會寫入命令提示符視窗，也會進入\$BASE\csauth\logs\auth.log檔案。

[離線測試使用者身份驗證](#)

使用者身份驗證可以通過命令列介面(CLI)進行測試。RADIUS可測試「radtest」，而TACACS+可測試「tactest」。如果通訊裝置沒有生成有用的調試資訊，並且存在有關Cisco Secure ACS Windows問題或裝置問題的問題，則此測試可能非常有用。radtest和tactest都位於\$BASE\utils目錄中。下面是每個測試的示例。

[使用Radtest離線測試RADIUS使用者身份驗證](#)

```
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離線測試TACACS+使用者身份驗證](#)

```
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>
```

確定Windows 2000/NT資料庫失敗的原因

如果正在將身份驗證傳遞到Windows 2000/NT但失敗，您可以通過轉至程式>管理工具>域的使用者管理器、策略>稽核來開啟Windows稽核工具。轉到Programs > Administrative Tools > Event Viewer會顯示身份驗證失敗。失敗嘗試日誌中發現的失敗以如下示例所示的格式顯示。

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

這些消息可以在Microsoft網站上研究，網址為[Windows 2000 Event & Error Messages](#) and [Error Codes in Windows NT](#)。

如下所示描述1300L錯誤消息。

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.

範例

RADIUS良好驗證

```
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
Winsoc 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/recv errors   : 0
```

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

RADIUS錯誤驗證

```
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/recv errors : 0

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

TACACS+良好驗證

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+錯誤驗證 (摘要)

```
F:\Program Files\Cisco Secure ACS v2.6\CSTacacs>
F:\Program Files\Cisco Secure ACS v2.6\CSTacacs>ctacacs -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: cisc01
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>
```

相關資訊

- [技術支援 - Cisco Systems](#)