

Obtención de la información de la depuración de AAA y de la versión para Secure ACS de Cisco para Windows

Contenido

[Introducción](#)

[Antes de comenzar](#)

[Convenciones](#)

[Prerequisites](#)

[Componentes Utilizados](#)

[Obtención de Cisco Secure para la información de versión de Windows](#)

[Uso de la línea de comandos de DOS](#)

[Uso de la interfaz GUI](#)

[Configuración de Cisco Secure ACS para niveles de depuración de Windows](#)

[Cómo configurar el nivel de registro a Completo en ACS GUI](#)

[Cómo configurar el registro de Dr. Watson](#)

[Creación de un archivo package.cab](#)

[¿Qué es package.cab?](#)

[Creación de un archivo package.cab con la utilidad CSSupport.exe](#)

[Recolección manual de un archivo .cab de paquete](#)

[Obtención de información de depuración AAA de Cisco Secure para Windows NT](#)

[Obtención de información de depuración de reiteración de AAA de Cisco Secure para Windows NT](#)

[Prueba de autenticación del usuario sin conexión](#)

[Determinación de las razones de las fallas de la base de datos de Windows 2000/NT](#)

[Examples](#)

[Autenticación de RADIUS correcta](#)

[Autenticación incorrecta de RADIUS](#)

[Buena autenticación de TACACS+](#)

[Autenticación TACACS+ que resultó mal \(condensada\)](#)

[Información Relacionada](#)

[Introducción](#)

Este documento explica cómo ver la versión de ACS Secure de Cisco para Windows, y cómo configurar y obtener información de depuración de Autenticación, autorización y contabilidad (AAA).

[Antes de comenzar](#)

[Convenciones](#)

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de Consejos Técnicos de Cisco](#).

[Prerequisites](#)

No hay requisitos previos específicos para este documento.

[Componentes Utilizados](#)

La información que contiene este documento se basa en Cisco Secure ACS para Windows 2.6.

[Obtención de Cisco Secure para la información de versión de Windows](#)

Puede ver la información de la versión utilizando la línea de comandos DOC o la GUI.

[Uso de la línea de comandos de DOS](#)

Para ver el número de versión de Cisco Secure ACS para Windows a través de la opción de la línea de comandos en DOS, utilice `cstacacs` o `csradius` seguido de `-v` para RADIUS y `-x` para TACACS+. Vea los ejemplos siguientes:

```
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
```

También puede ver el número de versión del programa Cisco Secure ACS en el registro de Windows. Por ejemplo:

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

[Uso de la interfaz GUI](#)

Para ver las versiones con la GUI de Cisco Secure ACS, visite la página Web de ACS. Puede hacer esto en cualquier momento con sólo hacer doble clic en el logotipo de Cisco Systems que se encuentra en el margen superior izquierdo de la pantalla. La mitad inferior de la página principal mostrará la versión completa.

[Configuración de Cisco Secure ACS para niveles de depuración de Windows](#)

Lo siguiente es una explicación de las diferentes opciones de depuración que son necesarias


para obtener la máxima información de depuración.


[Cómo configurar el nivel de registro a Completo en ACS GUI](#)

Necesitará configurar ACS para registrar todos los mensajes. Para hacerlo, siga los pasos enumerados a continuación:

1. Desde la página de inicio de ACS, vaya a Systems Configuration (Configuración de sistemas) > Service Control (Control de servicio).
2. Bajo el título Service Log File Configuration (Configuración del archivo de registro de servicios), establezca el nivel de detalles en Full (completo). Puede modificar las secciones Generate New File (Generar nuevo archivo) y Manage Directory (Administrar directorio) si es

System Configuration

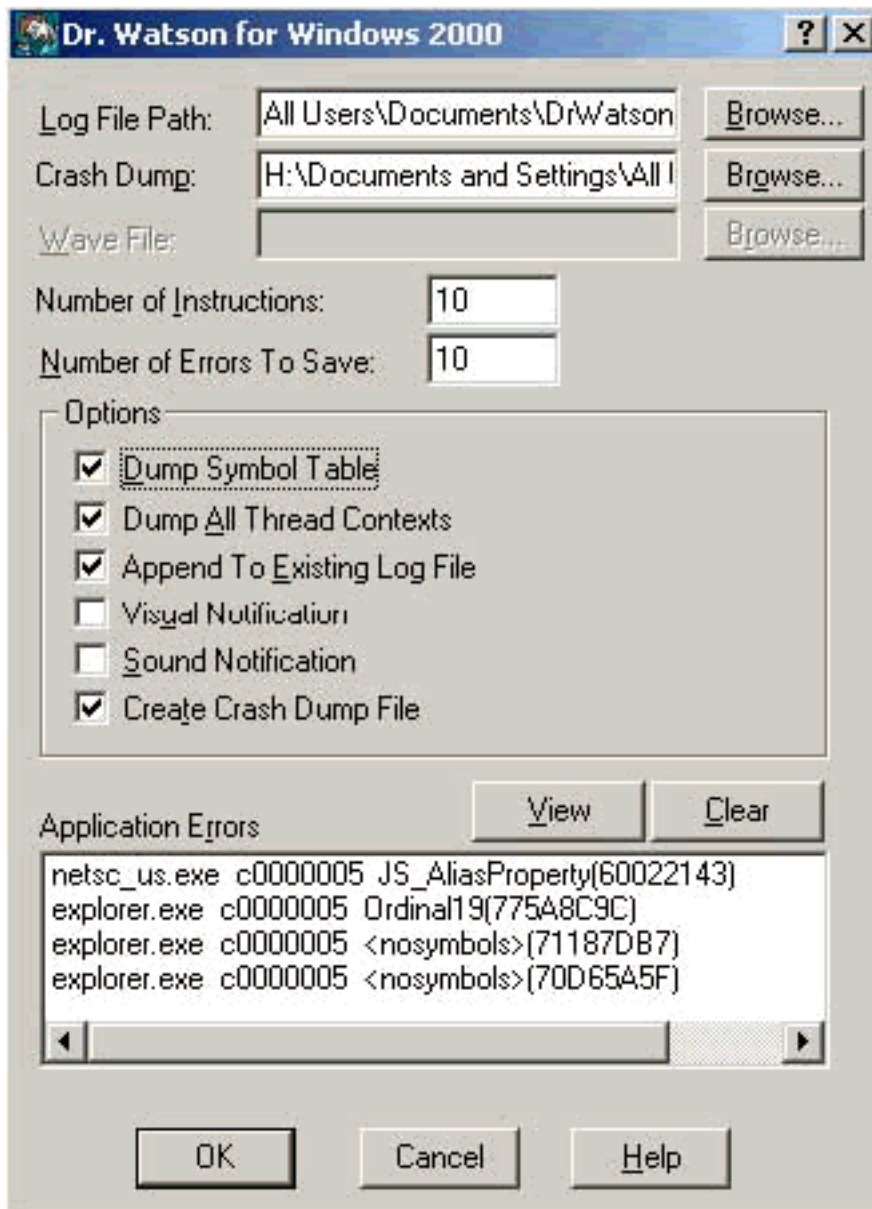
CiscoSecure ACS on mhammon-pc 	
Is Currently Running	

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	

necesario.

[Cómo configurar el registro de Dr. Watson](#)

En la solicitud de comando, escriba `drwtsn32` y aparecerá la ventana Dr. Watson. Asegúrese de que se encuentren seleccionadas las opciones para Dump All Thread Contexts (Vaciar todos los contextos de cadenas) y Dump Symbol Table (Vaciar tabla de símbolos).



[Creación de un archivo package.cab](#)

[¿Qué es package.cab?](#)

Package.cab es un archivo Zip que contiene todos los archivos necesarios para solucionar los problemas de ACS de manera eficiente. Puede usar la utilidad CSSupport.exe para crear el package.cab o puede recolectar los archivos en forma manual.

[Creación de un archivo package.cab con la utilidad CSSupport.exe](#)

Si tiene un problema de ACS para el que necesita recopilar información, ejecute el archivo CSSupport.exe lo antes posible después de ver el problema. Utilice la línea de comandos DOS o la GUI del Explorador de Windows para ejecutar CSSupport desde C:\program files\Cisco Secure ACS v2.6\Utils>CSSupport.exe.

Al ejecutar el archivo CSSupport.exe, aparece la siguiente ventana.



En esta pantalla tiene dos opciones principales:

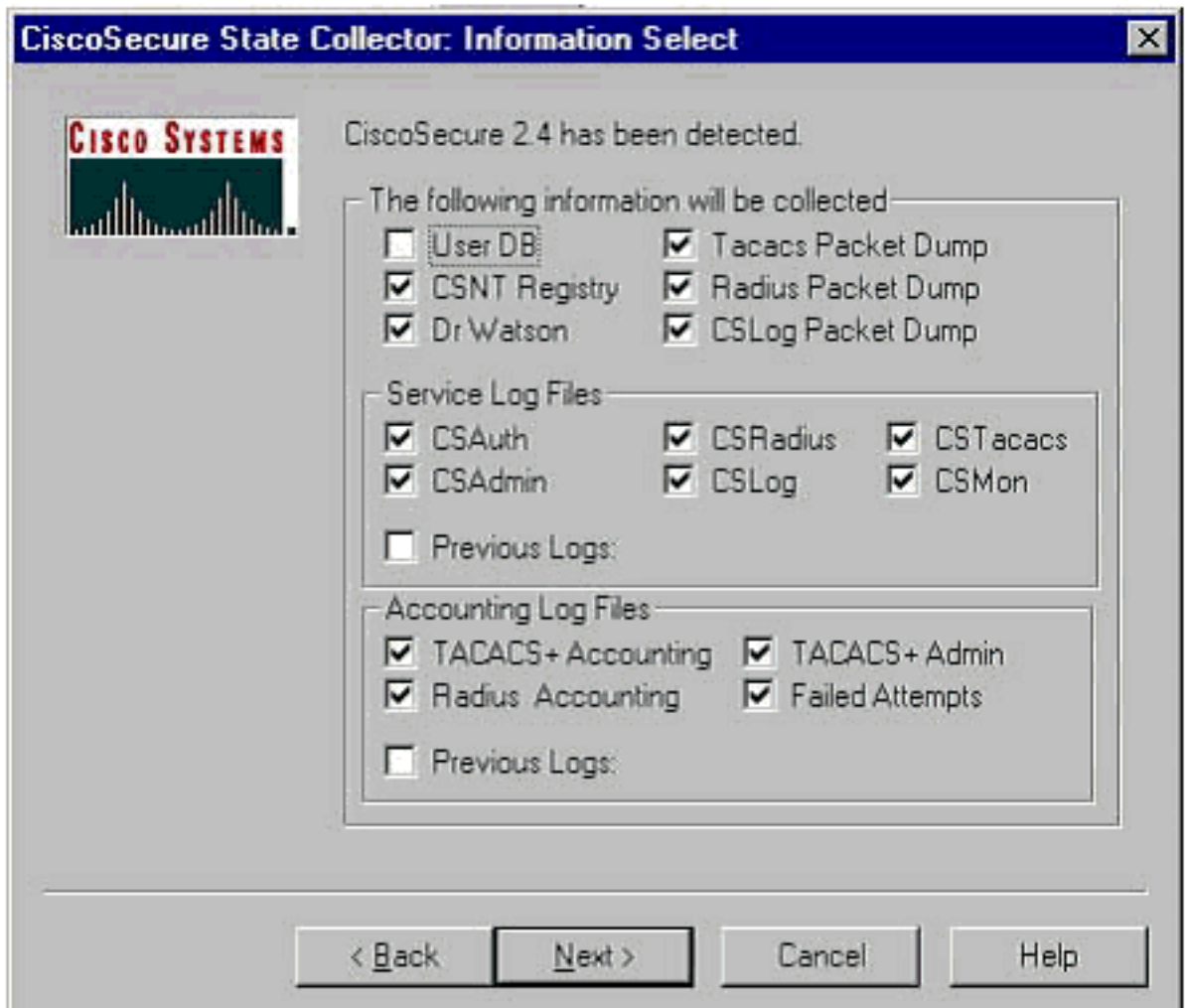
- [Ejecutar el asistente](#), que le guía por una serie de cuatro pasos: Cisco Secure State Collector: Selección de información Cisco Secure State Collector: Selección de instalación Cisco Secure State Collector: Verbosidad de registro Cisco Secure State Collector (la colección real) or
- [Establecer sólo nivel de registro](#), que le permite omitir los primeros pasos e ir directamente al Cisco Secure State Collector: Pantalla Log Verbosity (Registrar verbosidad)

Para una configuración inicial, seleccione **Ejecutar asistente** para continuar con los pasos necesarios para establecer el registro. Luego de la configuración inicial, puede utilizar la opción Set Log Levels Only para ajustar los niveles de registro. Realice la selección y haga clic en **Next**.

[Ejecutar Asistente](#)

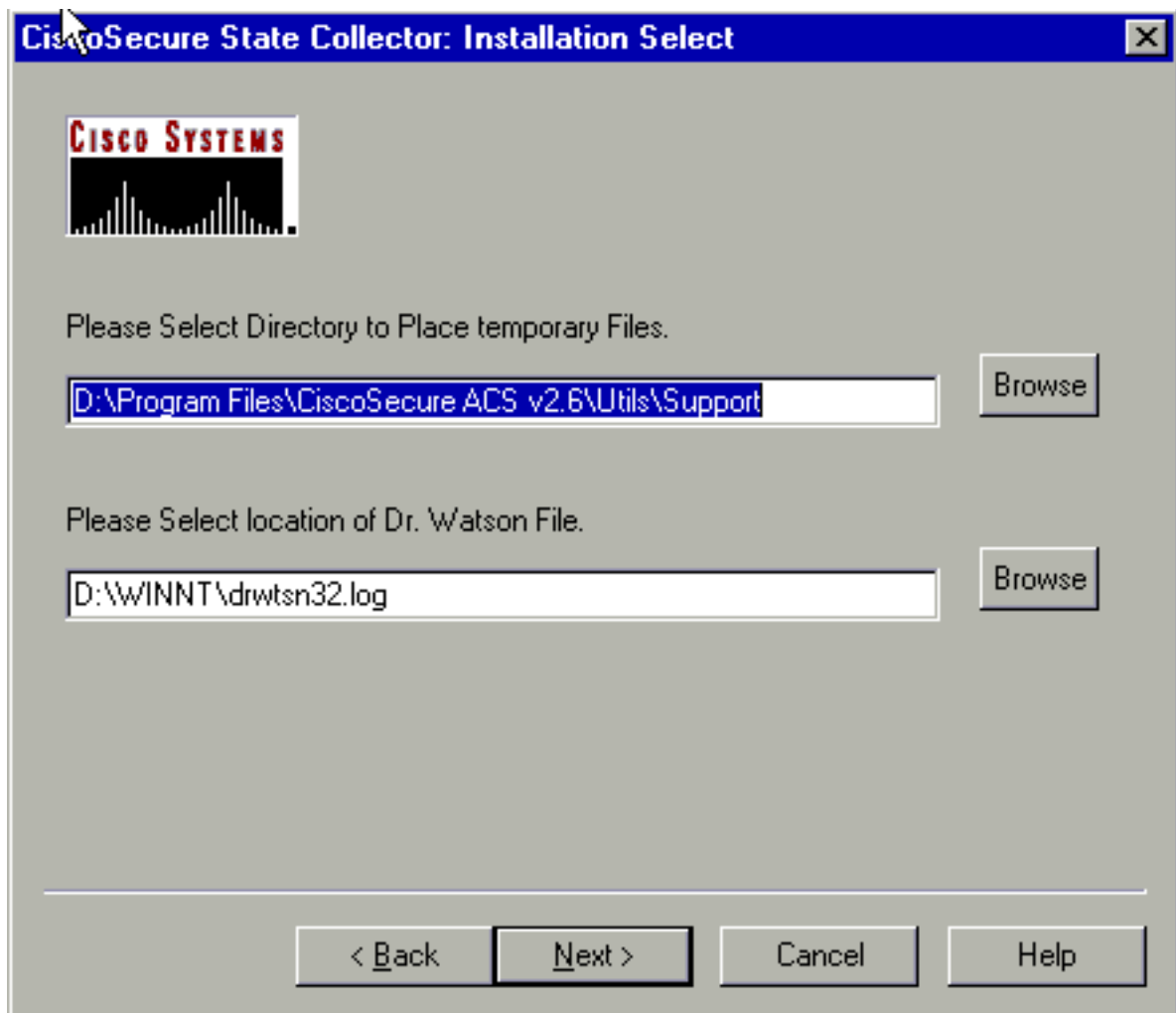
A continuación, se explica cómo seleccionar información mediante la opción Run Wizard (Ejecutar asistente).

1. **Cisco Secure State Collector: Selección de información** Deben seleccionarse todas las opciones predeterminadas, excepto User DB y Previous Logs (registros anteriores). Si piensa que su problema es la base de datos del grupo o el usuario, seleccione User DB (Usuario DB). Si desea incluir registros antiguos, seleccione la opción Previous Logs (Registros previos). Haga clic en Next (Siguiente) cuando

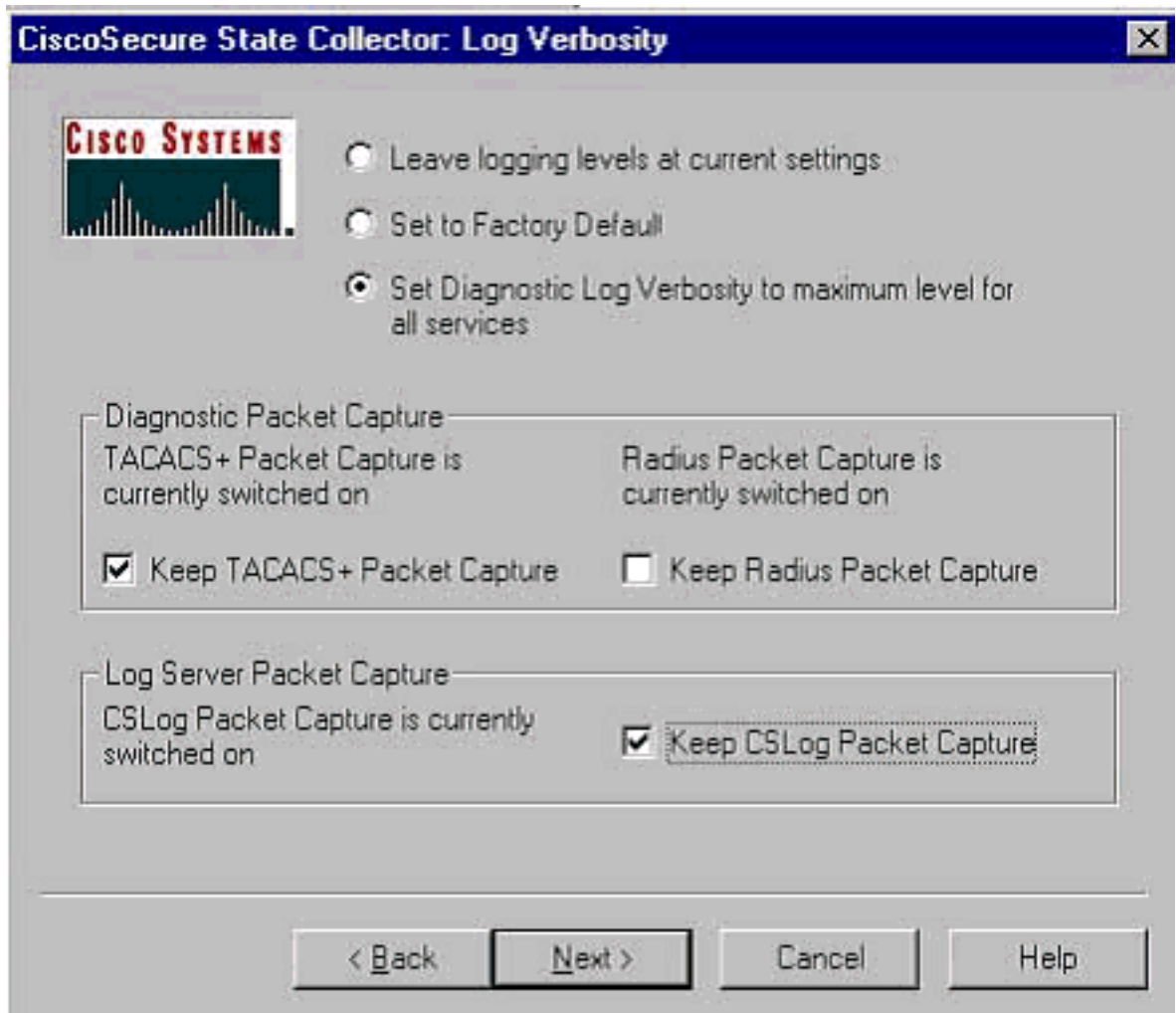


termine.

2. **Cisco Secure State Collector: Selección de instalación** Elija el directorio en el que desea colocar el package.cab. El valor predeterminado es C:\Program Files\Cisco Secure ACS v.26\Utils\Support. Puede cambiar esta ubicación si lo desea. Asegúrese de que la ubicación correcta del Dr. Watson se ha especificado. La ejecución de CSSupport requiere que inicie y detenga los servicios. Si está seguro de que desea detener e iniciar los servicios de Cisco Secure, haga clic en Next (Siguiente) para continuar.

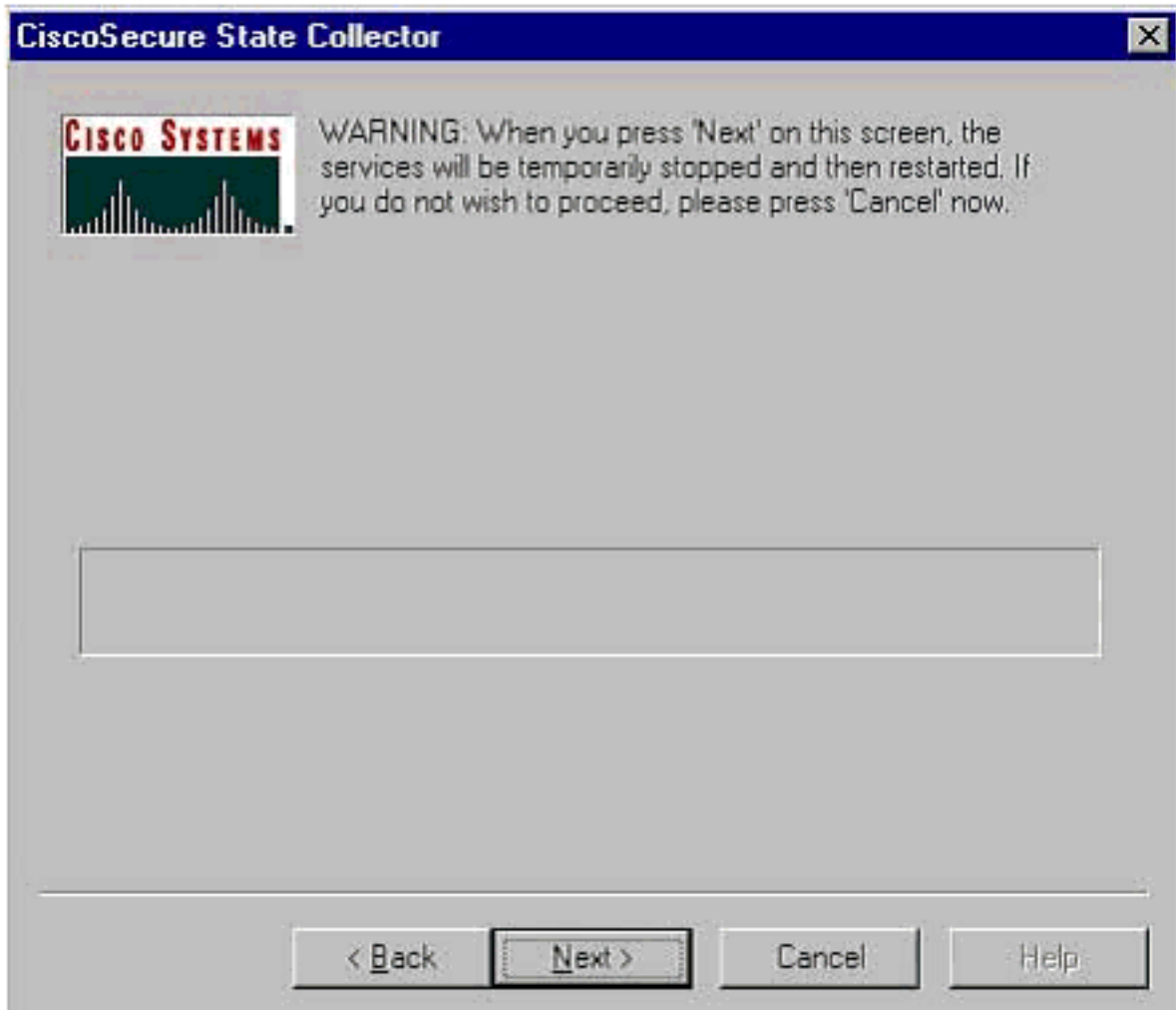


3. **Cisco Secure State Collector: Verbosidad de registro** Seleccione la opción **Establecer la verbosidad del registro de diagnóstico al nivel máximo para todos los servicios**. Bajo el encabezamiento **Diagnostic Packet Capture (Captura de paquete de diagnóstico)**, seleccione **TACACS+** o **RADIUS**, según cuál esté ejecutando. Seleccione la opción **Keep CSLog Packet Capture**. Cuando haya finalizado, haga clic en **Next (Siguiente)**. **Nota:** Si desea tener registros de días anteriores, debe seleccionar la opción **Registros anteriores** en el paso 1 y luego establecer el número de días que desea



volver.

4. **Cisco Secure State Collector** Verá una advertencia que indica que, cuando continúe, sus servicios se detendrán y luego se reiniciarán. Esta interrupción es necesaria para que CSSupport tome todos los archivos necesarios. El tiempo de caída debería ser mínimo. Podrá observar la detención del servicio y reiniciarlo en esta ventana. Para continuar, haga clic en Next (Siguiente).



Quando

se reinician los servicios, se puede encontrar package.cab en la ubicación especificada. Haga clic en Finish (Finalizar) y el archivo package.cab estará listo. Busque la ubicación especificada para package.cab y reubique en un directorio donde se pueda guardar. El ingeniero de soporte técnico podrá solicitarla en cualquier momento durante el proceso de resolución de problemas.

[Establecer sólo niveles de registro](#)

Si ejecutó State Collector anteriormente y sólo debe cambiar los niveles de registro, puede utilizar la opción Set Log Levels Only (Configurar niveles de registro únicamente) a fin de pasar a Cisco Secure State Collector: [La pantalla Log Verbosity \(Ingresar verbosidad\), donde configura la captura de paquetes de diagnóstico](#). Cuando hace clic en Siguiente, irá directamente a la página de Advertencia. Luego, haga clic en Next nuevamente para detener el servicio, reunir el archivo y reiniciar los servicios.

[Recolección manual de un archivo .cab de paquete](#)

A continuación se muestra una lista de los archivos compilados en package.cab. Si CSSupport no funciona correctamente, puede recopilar estos archivos con el Explorador de Windows.

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

[Obtención de información de depuración AAA de Cisco Secure para Windows NT](#)

Los servicios CSRADIUS, CSTacacs y CSAAuth de Windows NT pueden ejecutarse en el modo de línea de comando cuando se está resolviendo un problema.

Nota: El acceso a la GUI es limitado si algún servicio Cisco Secure para Windows NT se está ejecutando en el modo de línea de comandos.

Para obtener información de depuración CSRADIUS, CSTacacs o CSAAuth, abra una ventana DOS y ajuste la propiedad Windows Screen Buffer height a 300.

Utilice los siguientes comandos para 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 los siguientes comandos para CSTacacs:

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

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

Obtención de información de depuración de reiteración de AAA de Cisco Secure para Windows NT

Los servicios CSAuth de Windows NT se pueden ejecutar en el modo de línea de comando al diagnosticar un problema de réplica.

Nota: El acceso a la GUI es limitado si algún servicio Cisco Secure para Windows NT se está ejecutando en el modo de línea de comandos.

Para obtener información de depuración de reiteración de CSAuth, abra una ventana DOS y modifique la altura de la memoria intermedia de la pantalla de propiedades de Windows a 300.

Utilice los siguientes comandos para CSAuth en los servidores de origen y destino:

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

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

La depuración se escribe en la ventana del símbolo del sistema y también se incluye en el archivo \$BASE\csauth\logs\auth.log.

Prueba de autenticación del usuario sin conexión

Puede probarse la autenticación del usuario a través de la Interfaz de la línea de comandos (CLI) RADIUS se puede probar con "radtest" y TACACS+ con "tactest". Estas pruebas pueden ser útiles si el dispositivo de comunicación no está produciendo información de depuración útil y si hay alguna pregunta sobre si hay un problema con Cisco Secure ACS Windows o un problema con el dispositivo. Tanto radtest como tactest se encuentran en el directorio \$BASE\utils. A continuación se presentan ejemplos de cada prueba.

Prueba de Autenticación de Usuario RADIUS sin Conexión con 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.

```

Prueba de la Autenticación de usuario TACACS+ fuera de línea con 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>

```

Determinación de las razones de las fallas de la base de datos de Windows 2000/NT

Si la autenticación se pasa a Windows 2000/NT pero falla, puede activar la función de auditoría de Windows yendo a **Programas > Herramientas administrativas > Administrador de usuarios para dominios, Políticas > Auditoría**. Ir a **Programas > Herramientas administrativas > Visor de eventos** muestra fallas de autenticación. Las fallas halladas en el registro de intentos fallidos se muestran en un formato como el que se ejemplifica a continuación.

NT/2000 authentication FAILED (error 1300L)

Estos mensajes se pueden investigar en el sitio web de Microsoft en [Windows 2000 Event & Error Messages](#) y [códigos de error en Windows NT](#) .

El mensaje de error 1300L se describe como se muestra a continuación.

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

Autenticación de RADIUS correcta

```
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/recv errors : 0

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

Autenticación incorrecta de RADIUS

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>
```

[Buena autenticación de TACACS+](#)

```
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>
```

[Autenticación TACACS+ que resultó mal \(condensada\)](#)

```
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>
```

[Información Relacionada](#)

- [Soporte Técnico - Cisco Systems](#)