Получение номера версии Cisco Secure ACS для Windows и сведений об отладке аутентификации, авторизации и учета

Содержание

Введение

В этом документе объясняется, как просмотреть Cisco Secure ACS для версии Windows, а также — как выполнить настройку и получить сведения об отладке AAA.

Перед началом работы

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Предварительные условия

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Сведения, содержащиеся в данном документе, относятся к серверам Cisco Secure ACS для Windows версии 2.6.

Получение безопасности Cisco для информации о версии Windows

Можно просмотреть сведения о версии при помощи линии команды DOC или при помощи GUI.

Использование командной строки DOS

Чтобы увидеть номер версии Cisco Secure ACS для Windows через командную строку DOS, используйте команду cstacacs или csradius с параметром -v для RADIUS и -x для TACACS+. Посмотрите примеры ниже:

```
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
```

Можно также видеть номер версии программы Cisco Secure ACS в Реестре Windows. Пример:

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

Использование графического интерфейса пользователя

Чтобы посмотреть версию с помощью Cisco Secure ACS GUI, перейдите на домашнюю страницу ACS. Это можно сделать в любое время, щелкнув значок Cisco Systems в левом верхнем углу экрана. На нижней половине домашней страницы будет отображена полная версия.

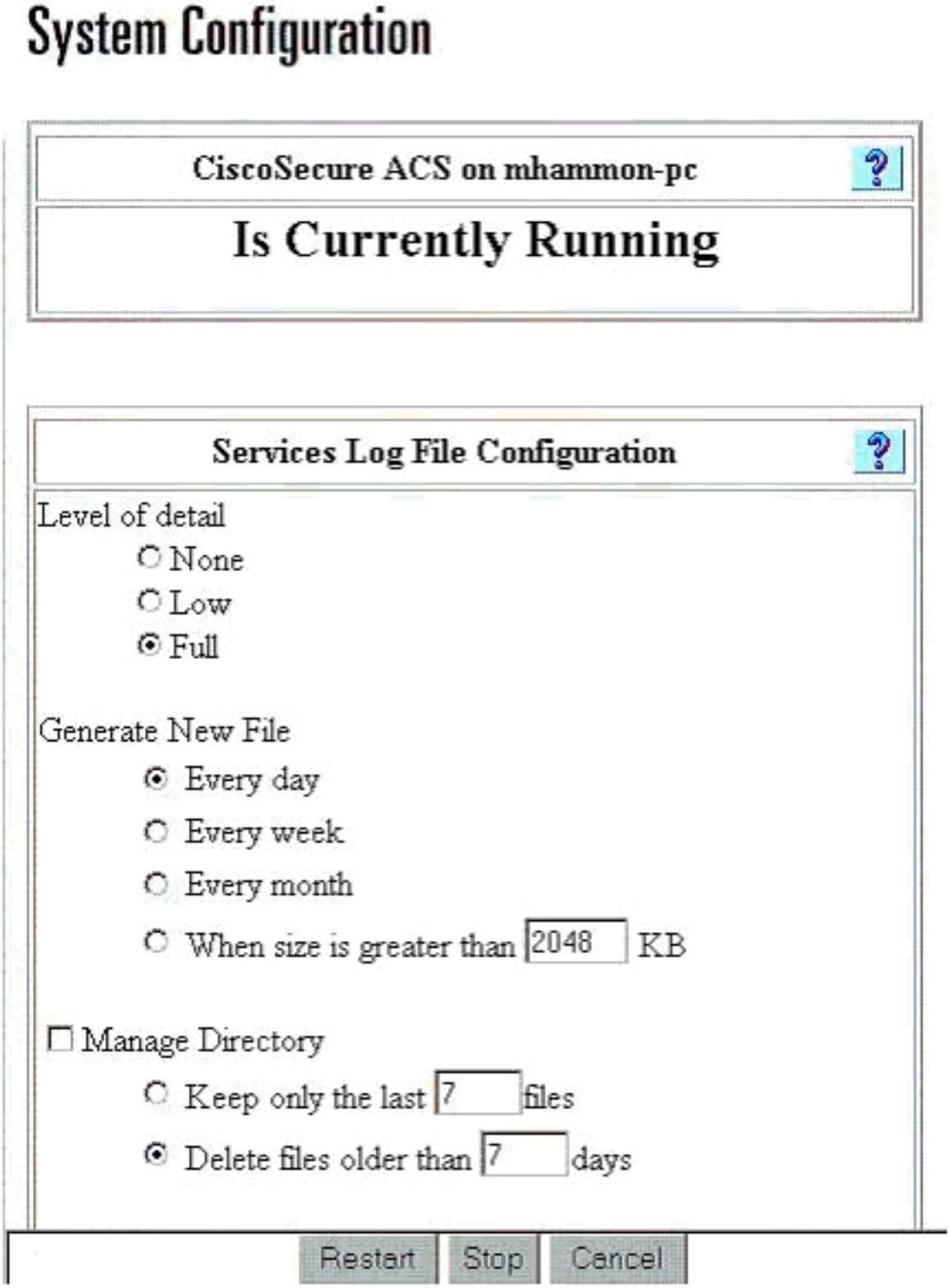
Настройка Cisco Secure ACS в соответствии с уровнями отладки Windows

Ниже приводится объяснение различных параметров отладки, которые необходимы для получения максимального объема сведений об отладке.

Как задать полный уровень записи в ГИП ACS

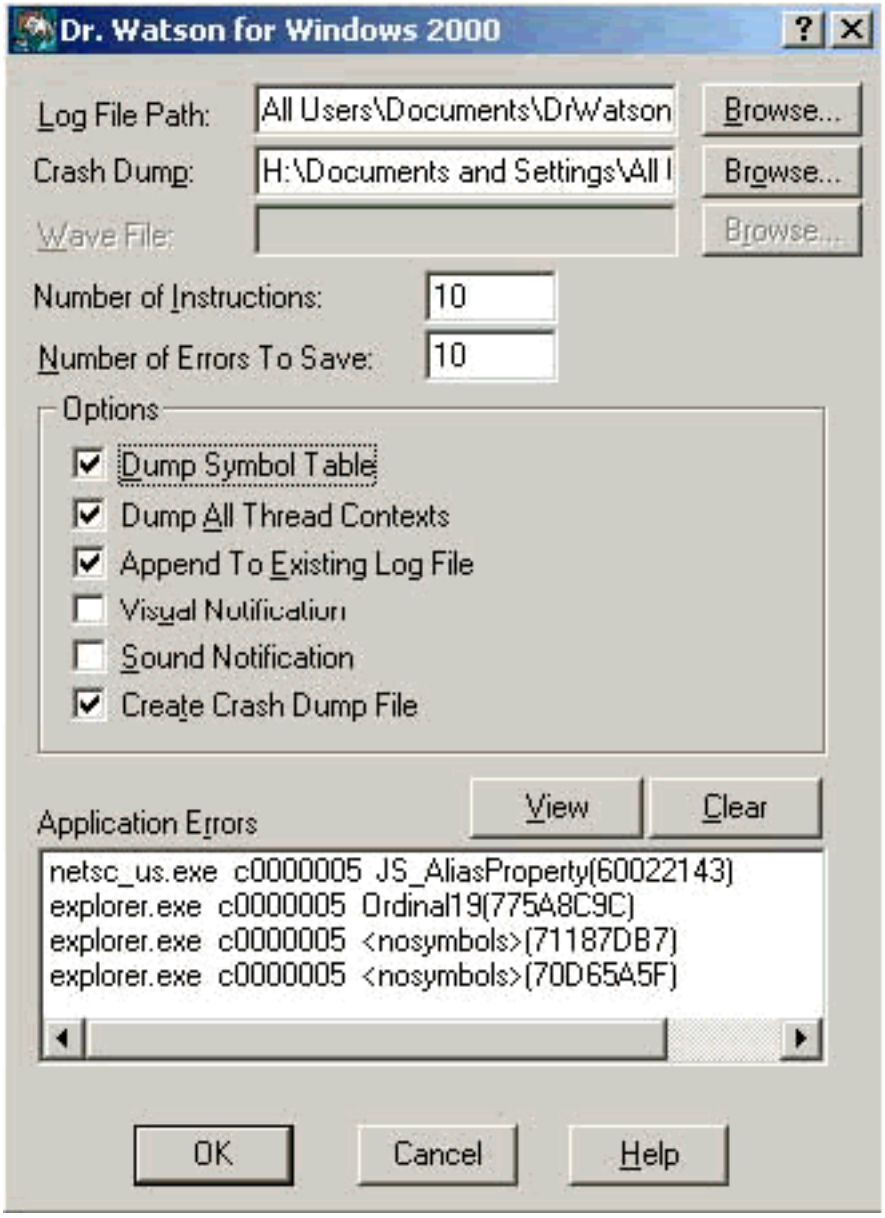
Необходимо настроить ACS на запись всех сообщений в журнал. Чтобы сделать это, выполните перечисленные ниже шаги:

1. **Из домашней страницы ACS перейдите к Systems Configuration > Service Control.**
2. **Под заголовком Service Log File Configuration установите значение Full для степени детализации.**При необходимости можно вносить изменения в разделы Generate New File (Создание нового файла) и Manage Directory (Управление каталогами).



[Как настроить регистрацию Dr. Watson]

В командной строке введите drwtsn32, и отобразится окно Dr. Watson. Убедитесь, что отмечены пункты Dump All Thread Contexts и Dump Symbol Table.



Создается файл package.cab

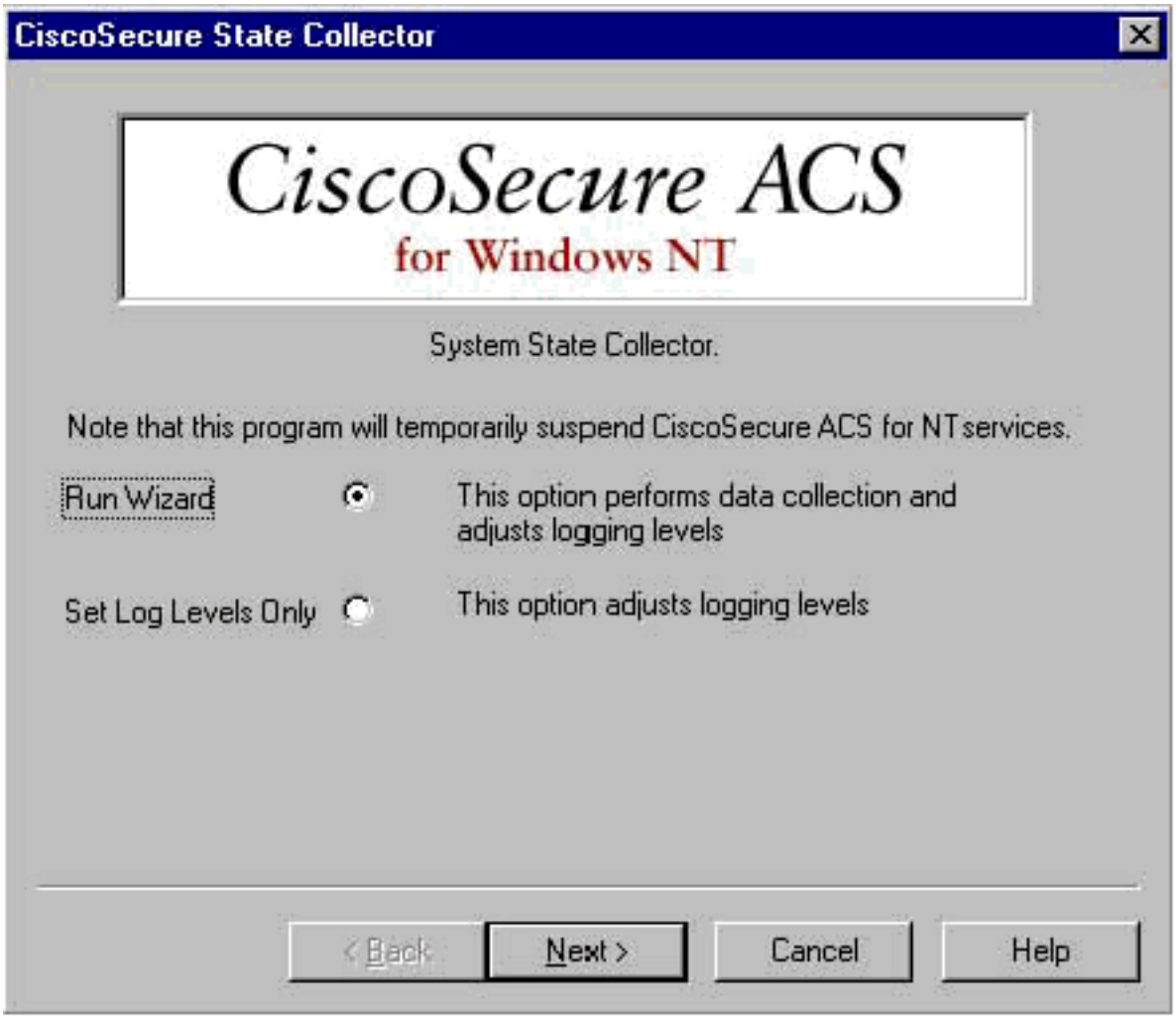
Что такое package.cab?

Package cab – это zip-файл, содержащий все необходимые файлы для эффективного устранения неисправностей ACS. Можно использовать утилиту CSSupport.exe, чтобы создать package.cab, или можно объединить данные файлы вручную.

Создание файла package.cab с помощью служебной программы CSSupport.exe

Если у вас есть проблема ACS, для которой необходимо собрать информацию, выполнить файл CSSupport.exe как можно скорее после наблюдения проблемы. Используйте линию Команды DOS или GUI Проводника Windows для выполнения CSSupport от C:\program files\Cisco Secure ACS v2.6\Utils> CSSupport.exe.

После исполнения файла CSSupport.exe отображается следующее окно.



На этом экране представлены две основные опции:

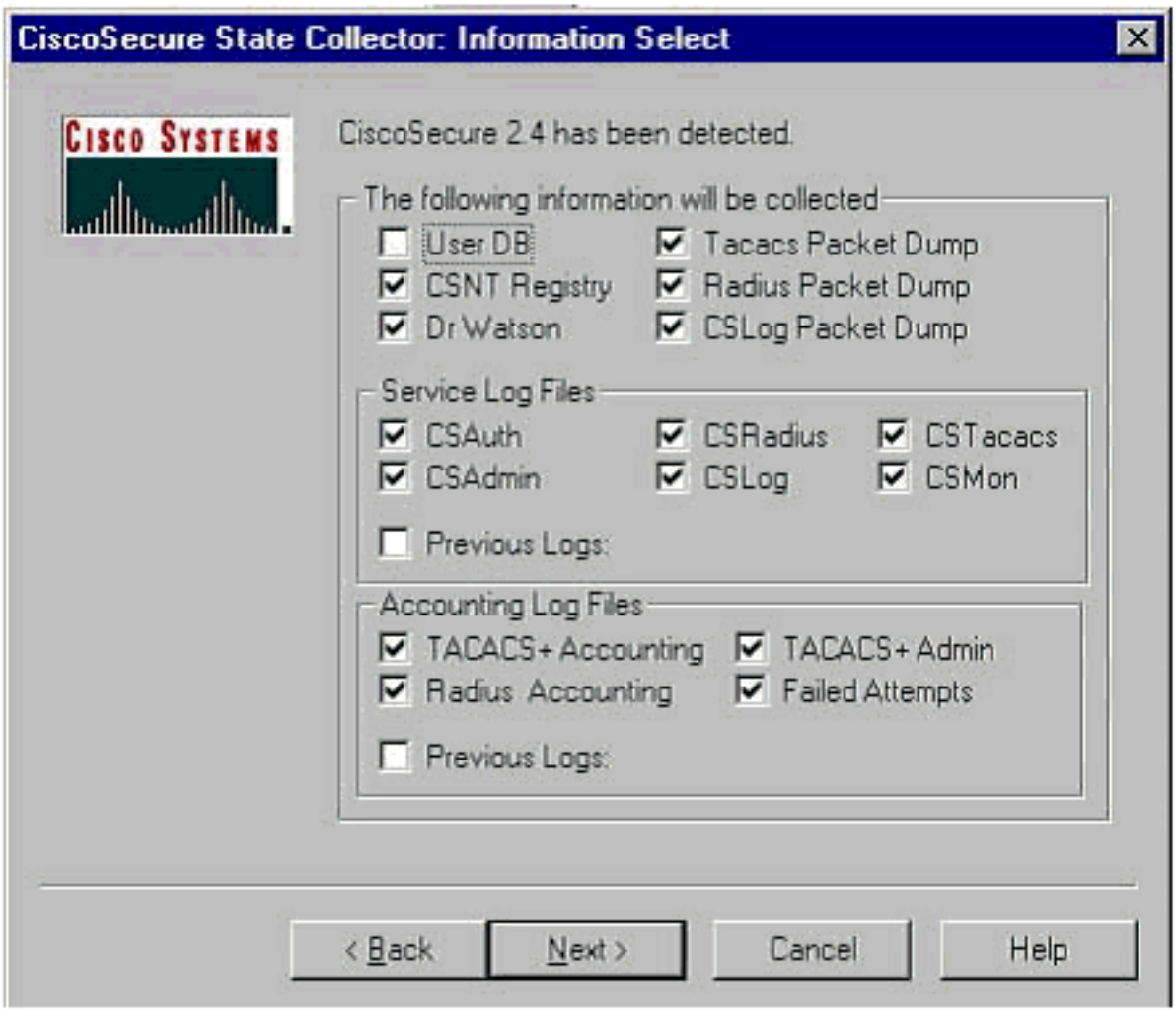
- Выполните Мастера, который ведет вас через серию четырех шагов:Центр сбора состояний безопасности Cisco: Выбор данныхЦентр сбора состояний безопасности Cisco: Выбор установкиЦентр сбора состояний безопасности Cisco: Детальность протоколированияЦентр сбора состояний безопасности Cisco (фактический сбор)или
- Уровень Журнала набора Только, который позволяет вам пропускать первые несколько шагов и идти непосредственно к Центру сбора данных о состоянии безопасности Cisco: Экран журнала подробных сообщений

Для новой настройки выберите **Run Wizard** для перехода посредством шагов, должен был установить журнал. **После начальной настройки для корректировки уровней регистрации можно использовать параметр Set Log Levels Only**. Сделайте свой выбор и нажмите **Next**.

Мастер запуска

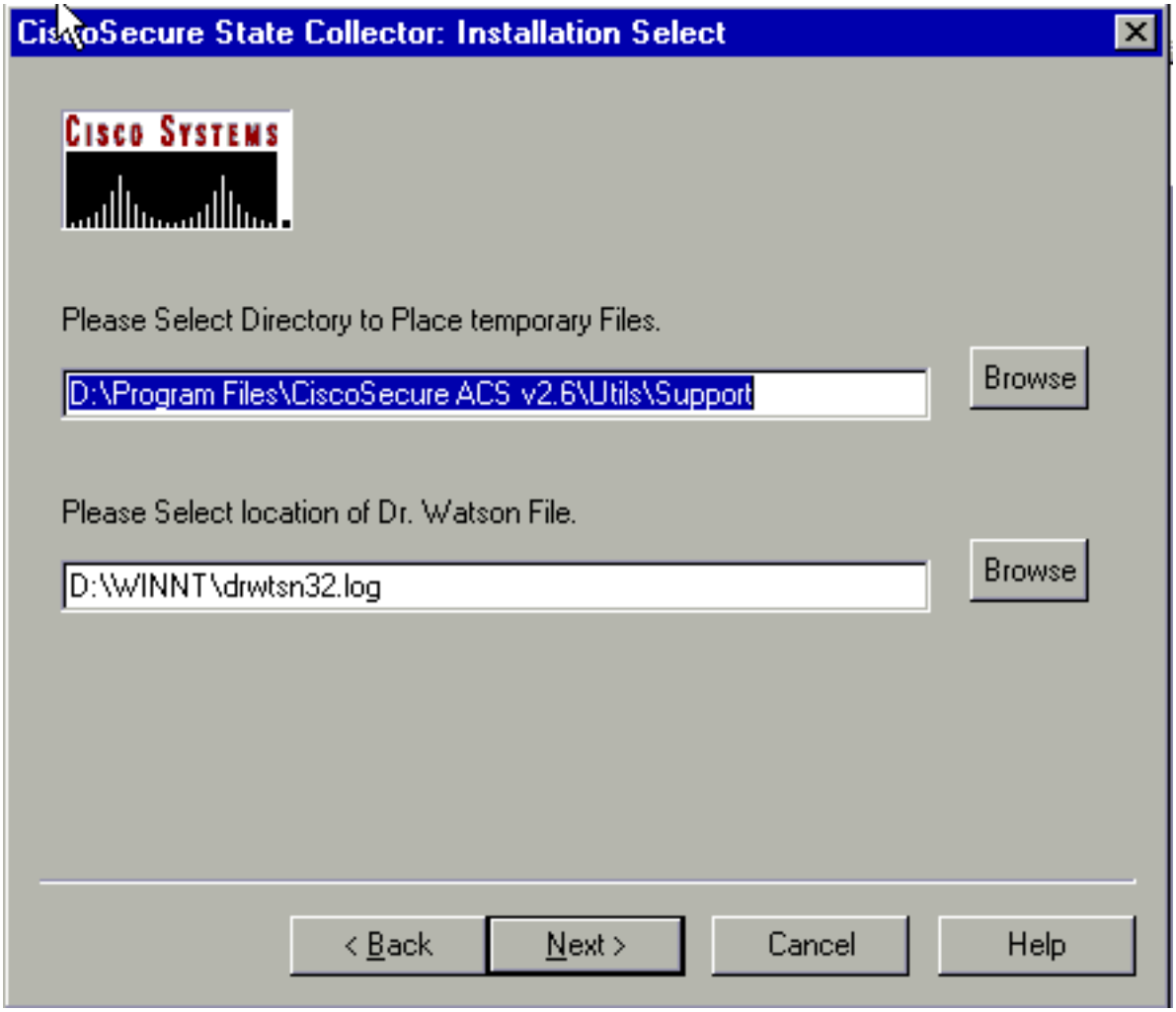
Ниже объясняется, как выбирать информацию при помощи параметра Run Wizard.

1. **Центр сбора состояний безопасности Cisco: Выбор данных**Все параметры должны выбираться по умолчанию, кроме User DB (БД пользователя) и Previous Logs (Предыдущие журналы). **Если предполагается, что проблема в базе данных пользователя или группы, выберите User DB. Если требуется, чтобы старые журналы были включены, то выберите параметр "Previous Logs". По окончании нажмите кнопку**

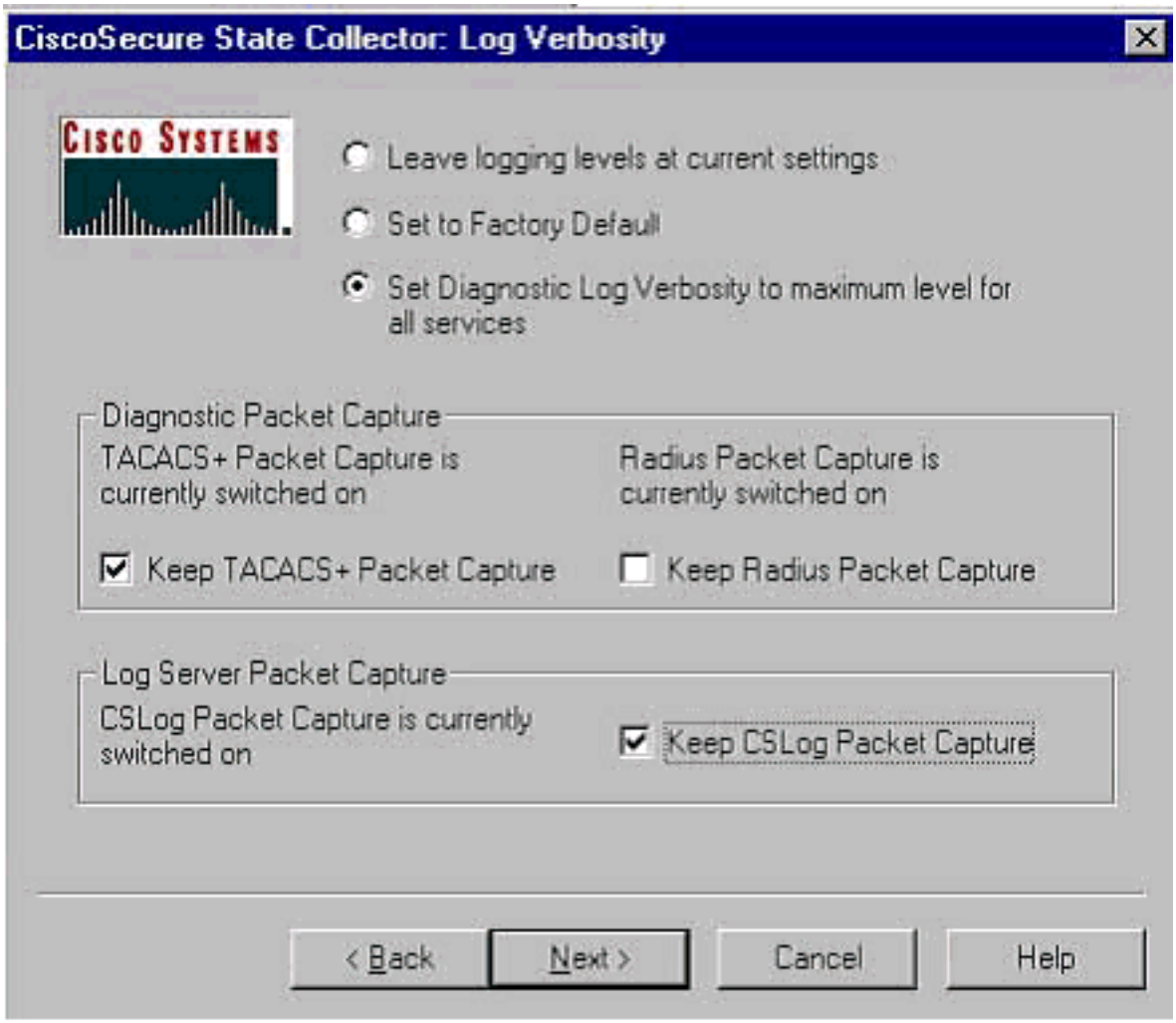


"Далее".

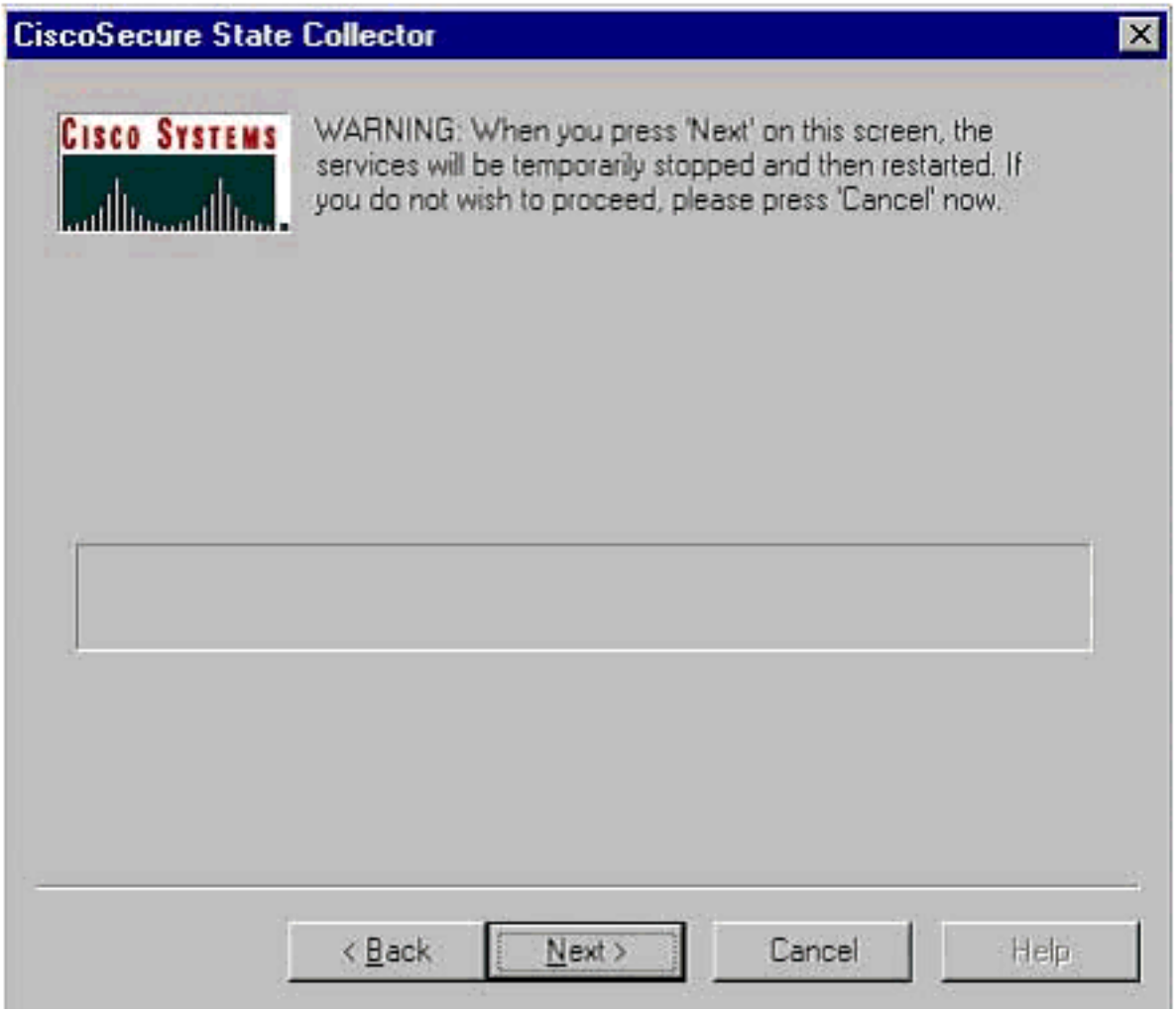
2. **Центр сбора состояний безопасности Cisco: Выбор установки**Выберите каталог, в который вы хотите разместить package.cab. По умолчанию является C:\Program Files\Cisco Secure ACS v.26\Utils\Support. Это расположение при желании можно изменить. Убедитесь, что указано правильное расположение Dr. Watson. Рабочий CSSupport требует, чтобы вы запустили и остановили сервисы. **Если требуется остановить и запустить службы безопасности Cisco, нажмите кнопку "Next" (Далее) для продолжения.**



3. **Центр сбора состояний безопасности Cisco: Детальность протоколирования**Выберите опцию для **Многословия Журнала диагностики Набора к максимальному уровню для всех сервисов**. Под заголовком Diagnostic Packet Capture выберите TACACS+ или RADIUS, в зависимости от того, что используется. **Выберите параметр Keep CSLog Packet Capture**. **Закончив, нажмите кнопку Next (Далее).Примечание:** Если вы хотите иметь журналы с предыдущих дней, необходимо выбрать **параметр для команды Предыдущие журналы** в шаге 1 и затем установить число дней, вы хотите возвратиться.



4. **Центр сбора состояний безопасности Cisco**Вы увидите предупреждение, указывающее на то, что в случае продолжения ваши службы будут остановлены, а затем перезапущены. Это прерывание необходимо для CSSupport для захвата всех необходимых файлов. Время простоя должно быть минимальным. Вы сможете наблюдать, как службы останавливаются и перезапускаются на этом окне. **Для продолжения нажмите кнопку**



"Next". Когда сервисы перезапускают, package.cab может быть найден в заданном местоположении. **После нажатия кнопки "Готово" файл package.cab будет готов.**Перейдите к местоположению, которое вы задали для package.cab, и переместите его к каталогу, где это может быть сохранено. Специалист технической поддержки может запросить ее в любой момент процесса устранения неполадок.

Уровни журнала набора только

Если Центр сбора состояний (State Collector) ранее запускался и сейчас требуется просто изменить уровни записи, можно использовать функцию Set Log Levels Only (Задать только уровни записи), чтобы перейти к Центру сбора состояний безопасности Cisco: Экран журнала подробных сообщений, где устанавливается диагностический захват пакета. **После нажатия кнопки Next будет открыта страница предупреждения Warning. Затем опять нажмите Next для остановки устройства, сбора файла или перезапуска служб.**

Сбор файла package.cab вручную

Ниже приводится список файлов, которые скомпилированы в package.cab. Если CSSupport не функционирует должным образом, можно собрать эти файлы с помощью Проводника 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
```

Получение сведений отладки AAA Cisco Secure для Windows NT

Сервисы Windows NT CSRadius, CSTacacs и CSAuth могут запускаться в режиме командной строки во время поиска и устранения ошибок.

Примечание: Если какой-либо Cisco Secure для сервисов Windows NT работает в режиме командной строки, доступ к ГИП ограничен.

Для получения CSRadius CSTacacs или отладочная информация CSAuth, открывает Окно DOS и отрегулировал высоту для свойства Screen Buffer Windows к 300.

Используйте следующие команды для CSRadius:

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

Используйте следующие команды для CSTacacs:

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

Получение сведений отладки средств копирования AAA Cisco Secure для Windows NT

При устранении проблем репликации службы CSAuth в Windows NT можно запускать в режиме командной строки.

Примечание: Если какой-либо Cisco Secure для сервисов Windows NT работает в режиме командной строки, доступ к ГИП ограничен.

Для получения информации об отладке репликации CSAuth откройте окно DOS и выставьте в Windows значение высоты (height) экрана буфера (Screen Buffer) на 300.

Используйте следующие команды для CSAuth и на источнике и на конечных серверах:

```
c:\program files\ciscosecure acs v2.6\csauth>net stop csauth c:\program files\ciscosecure acs v2.1\csauth>csauth -p -z
```

Отладка записана в окно командной строки, и это также входит в файл $BASE\csauth\logs\auth.log.

Тестирование аутентификации пользователей в автономном режиме

Аутентификацию пользователей можно тестировать в интерфейсе командной строки (CLI). RADIUS может быть протестирован при помощи "radtest", а TACACS+ – при помощи "tactest"." Это тестирует, может быть полезным, если подключающееся устройство не производит полезную отладочную информацию, и если существует некоторый вопрос относительно того, существует ли Проблема Windows Cisco Secure ACS или проблема устройства. И radtest и tactest расположены в каталоге $BASE\utils. Ниже приведены примеры каждого теста.

Тестирование аутентификации ПОЛЬЗОВАТЕЛЯ RADIUS оффлайн с 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.
```

Тестирование аутентификации пользователей TACACS+ в автономном режиме с помощью 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>
```

Определение причин сбоев базы данных Windows 2000/NT

Если аутентификацию передают к Windows 2000/коротким тоннам, но отказывает, можно включить средство аудита Windows, перейдя **к Программам> Средства администрирования> Менеджер пользователей для Доменов, Политика> Аудит**. Переходящие **Программы> Средства администрирования> Просмотр событий** показывают ошибки проверки подлинности. Ошибки, найденные в журнале неудачных попыток, отображаются в формате, который показан в примере ниже.

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

Эти сообщения могут быть исследованы на веб-сайте Microsoft в Windows 2000 Event & Error Messages и Кодах ошибки в Windows NT.

1300L сообщение об ошибках описано как показано ниже.

```
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.
```

Примеры

Правильная аутентификация RADIUS

```
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>
```

Недействительная проверка подлинности 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 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>

Успешная аутентификация с помощью 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>

Ошибка проверки подлинности TACACS+ (суммированная)

```
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>

Дополнительные сведения

- Техническая поддержка - Cisco Systems