

Cisco – Cisco Secure ACS for Windows Frequently Asked Ques

Table of Contents

<u>Cisco Secure ACS for Windows Frequently Asked Questions</u>	1
<u>Questions</u>	1
<u>Related Information</u>	12

Cisco Secure ACS for Windows Frequently Asked Questions

This document provides answers to some common questions about Cisco Secure ACS for Windows (ACS).

Questions

- When was PPTP (Point-to-Point Tunneling Protocol) with MPPE (Microsoft Point to Point Encryption) keying support added to Cisco Secure ACS for Windows?
- Does ACS support Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)?
- The ACS has been reconfigured to require a user name and password for logging in locally, and now everyone is locked out. How can I fix this?
- The ACS documentation chapter on Cisco Secure ACS Command-Line Database utility explains how to bulk import a large numbers of users into ACS using the **csutil -i** command, but how do I bulk import network access servers (NASs)?
- I don't want the administrative overhead of having to list all the network access servers (NASs) in my network, and they all have the same "tacacs-server keys." How can I set up a default key to use with my NASs?
- I want to have a device "speak" both TACACS+ and RADIUS with ACS for authentication. I want one for dial and the other for router management. How can I do this?
- What are the differences between Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP), and why can't CHAP be used with the NT database?
- Will ACS act like a proxy server to other servers?
- Where is the user information in ACS stored?
- How do I back up ACS?
- Can I use the backup utility on one ACS and then restore the information on another server?
- How can I find out the exact release of my ACS software?
- Can Security Dynamics International (SDI) and ACS be installed on the same system?
- Can I send accounting information to another system and also have a copy on the local system?
- Is domain stripping supported with ACS?
- What is relational database management system (RDBMS) synchronization?
- When I try to bring up the GUI, I get an "Invalid administration control" error. The installation went fine, and the services are running. What is the problem?
- What should I check when users are unable to authenticate against the NT database?
- How do I configure the Novell Directory Server (NDS) database?
- What should I check when users are unable to authenticate against the Novell Directory Server (NDS) database?
- How can I troubleshoot a Security Dynamics International (SDI) authentication problem?
- My ACS authentication isn't working for multilink services. What should I do?
- Does ACS have any RADIUS support?
- Is there a limit on the number of network access servers (NASs) that can be supported by ACS?
- With Cisco Secure you can force the users to change their passwords after a given time period. Can you do this when you are using the Windows NT database for authentication?
- How can users change their own passwords?
- If replication fails, what things should I look for?
- My ACS "Logged in Users" report works with some devices, but not with others. What is the problem?
- How is the the CRYPTOCard software handled in ACS 3.0?
- What is the CRYPTOAdmin Authentication Server license policy for Cisco customers?
- ACS accounting displays the message "NAS reset". What can cause this message to appear?

- What encryption algorithm is used to store ACS passwords?
- Does Cisco recommend a software application that can be used to do reporting on accounting logs available in ACS?
- Can ACS do translation proxy between RADIUS and TACACS+ and vice versa?
- How can I assign DNS and WINS server IP addresses for PPP connections from ACS using TACACS+?
- How can I assign DNS and WINS server IP addresses for PPP connections from ACS using RADIUS?
- How can you change the port in which RADIUS server listens in the registry settings?
- Can I change the default port for TACACS+ to a value other than TCP 49?
- I see odd things in the ACS GUI. For example, the same users appear in multiple groups and I cannot delete users from the database. How can I fix this kind of corruption?
- I can't start services for RADIUS after re-installing the software several times. The event error says that service was terminated with "service specific error 11".
- ACS installation fails, returning an error about "NSLDAPSSL32V30.dll" and saying that it cannot over write the file. What causes this and how can I resolve the error?
- When I access the ACS GUI through a firewall, the address for the server in the URL field changes from a global IP address to a local address. Why does this happen?
- I'm using ACS with servers in geographically dispersed areas, and services can be somewhat disrupted when I do replication. How can I deal with this?
- How can I obtain ACS 3.0 to upgrade a previous version?
- Can a user be in more than one group at a time?
- When I turn on "enable authentication" in the switch or router with commands such as **aaa authentication enable default tacacs+** or **set authentication login tacacs enable telnet primary**, I am locked out of enable mode and the router says "Error in authentication". What should I do??
- Default settings allow users to change their own passwords by Telnetting to the router. How can I disable this option?

Related Information

Q. When was PPTP (Point-to-Point Tunneling Protocol) with MPPE (Microsoft Point to Point Encryption) keying support added to Cisco Secure ACS for Windows?

A. PPTP version 2.6 requires Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) authentication if MPPE keying (encryption) is to be done. In earlier versions, PPTP authentication is possible, but support for MPPE keying was not added until ACS version 2.6.

Q. Does ACS support Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)?

A. ACS presently supports MS-CHAP version 1. ACS version 3.0 supports MS-CHAP versions 1 and 2.

Q. The ACS has been reconfigured to require a user name and password for logging in locally, and now everyone is locked out. How can I fix this?

A. The solution to this problem depends on the version of software in place, but no matter what software version you have, be sure to back up the NT registry first. In early versions of ACS, the user name and password requirement for local login can be modified in the registry. Use the **regedit** command and search for "allowAutoLocalLogin." Change the registry value to 1 to allow local login, and then recycle the services.

In later ACS versions (2.6 and 3.0), you should use the **regedit** command and remove the users in the following:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAA##\CSAdmin\Administrators
```

Under the Administrators key you will see all the administrators that you have created. Delete the users and exit the registry. Upon accessing ACS, you will not be prompted for a user name and password. Once you are in the GUI, you can add administrators.

Q. The ACS documentation chapter on Cisco Secure ACS Command-Line Database utility explains how to bulk import a large numbers of users into ACS using the `csutil -i` command, but how do I bulk import network access servers (NASs)?

A. The procedure to bulk import NASs is similar to the import of users. The following flat-file is an example:

```
ONLINE
ADD_NAS:sam_i_am:IP:10.31.1.51:KEY:cisco:VENDOR:CISCO_T+
ADD_NAS:son_of_sam:IP:10.31.1.52:KEY:cisco:VENDOR:CISCO_R
```

The NASs may also be imported into a particular Network Device Group. The following flat-file is an example:

```
ADD_NAS:koala:IP:10.31.1.53:KEY:cisco:VENDOR:CISCO_R:NDG:my_ndg
```

Q. I don't want the administrative overhead of having to list all the network access servers (NASs) in my network, and they all have the same "tacacs-server keys." How can I set up a default key to use with my NASs?

A. You can add a default NAS in the NAS configuration area by leaving the host name and IP address blank. Put in only the key. Click **Submit**, and you will see NAS "others" and " *.*.*.*."

Note: This procedure only works for TACACS+, not RADIUS.

Q. I want to have a device "speak" both TACACS+ and RADIUS with ACS for authentication. I want one for dial and the other for router management. How can I do this?

A. Configure a default NAS as described in the previous question for TACACS+, and then enumerate the NAS for RADIUS. The NAS will send RADIUS dial requests to ACS on the RADIUS port if configured for **aaa authentication ppp default if-needed RADIUS**.

The NAS will send TACACS+ router management requests to ACS on the TACACS+ port if configured for **aaa authentication login default TACACS+**.

Q. What are the differences between Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP), and why can't CHAP be used with the NT database?

A. Password Authentication Protocol (PAP) sends passwords in the clear between the user and the TACACS+/RADIUS client/device. If the password is correct, the authentication is acknowledged; otherwise the connection is terminated.

Challenge Handshake Authentication Protocol (CHAP) sends a challenge message to the remote user. The remote user responds with a value calculated using a one-way hash function. The client/device checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise, the connection is terminated. Passwords are not sent in the clear.

CHAP cannot be used with the NT database because of the requirement of the CHAP RFC (1994). It states: "CHAP requires that the secret be available in plaintext form. Irreversibly encrypted password databases commonly available cannot be used." This precludes use of the NT database for CHAP. MS-CHAP is still an option.

Q. Will ACS act like a proxy server to other servers?

A. Yes, ACS can receive authentication requests from the network access servers (NASs) and forward them to other servers. You need to define the other servers by going to the **Network Configuration > AAA Servers** section on the source. The source server is defined as a TACACS+ or RADIUS NAS on the target. Once those are defined, configure the Distributed System Settings in the source Network Configuration to define the proxy parameters.

Q. Where is the user information in ACS stored?

A. ACS has its own proprietary database. It is stored in multiple files.

Q. How do I back up ACS?

A. You can back up ACS through the GUI using the System Configuration tab, or you can use the command-line interface (CLI). If you use the GUI, there is a backup of the users, groups, and registry settings. If you use the CLI, issue the following commands:

For a dump of users and groups:

```
$BASE\utils\csutil -d
```

For a backup of users, groups, and registry settings:

```
$BASE\utils\csutil -b
```

Q. Can I use the backup utility on one ACS and then restore the information on another server?

A. No, the backup utility is intended to save the user, group, and registry information from one ACS box and restore it to the same ACS box running the same version of software. If there is a need to clone a ACS box, replication is available instead.

If you need to copy only users and groups from one server to another, use the **csutil -d** command. The resulting dump text (.txt) file is then copied to the target box, and you can use the **csutil -n -l** command to initialize the database and import the users and groups.

Q. How can I find out the exact release of my ACS software?

A. There are two ways of checking the release.

- ◆ When you bring up the browser, look for the following at the bottom of the page:

```
Cisco Secure ACS v2.3 for Windows NT
```

```
Release 2.3(2)
```

- ◆ Bring up the DOS prompt on the Cisco Secure machine and run the following:

```
D:\Program Files\Cisco Secure ACS v2.3\Utils>csutil
```

```
CSUtil v2.3(2.4), Copyright 1997, Cisco Systems Inc
```

Q. Can Security Dynamics International (SDI) and ACS be installed on the same system?

A. Yes, ACS and SDI's ACE server may be run on the same machine. There can also be a client-server arrangement with ACS and ACE Client on one machine and the ACE server on another.

Q. Can I send accounting information to another system and also have a copy on the local system?

A. Yes, you can configure this by going to **System Configuration > Logging**.

Q. Is domain stripping supported with ACS?

A. Yes, ACS does support domain stripping. This is useful when there is a combination of Virtual Private Dialup Network (VPDN) and non-VPDN users. Another use for domain stripping is when the external NT database is used for authentication. The first time the users log in, the user name is autopopulated in ACS. Since a user may come in as "DOMAIN_A\user" or as "user," names may appear in ACS as "DOMAIN_A\user" or as "user," resulting in both entries in the database. The duplicate entries can be avoided by using domain stripping, wherein the prefix domain with the delimiter "\" can be erased to have a consistent database. You can set this up by going to **Network Configuration > Proxy Distribution Table**.

Q. What is relational database management system (RDBMS) synchronization?

A. ACS can support RDBMS databases, such as Oracle, to synchronize the database between two systems using any RDBMS.

Q. When I try to bring up the GUI, I get an "Invalid administration control" error. The installation went fine, and the services are running. What is the problem?

A. This problem is usually seen when the browser has a proxy server configured. To fix it, disable proxy server completely and then bring up the ACS administration screen.

Q. What should I check when users are unable to authenticate against the NT database?

A.

1. First check and see if you can authenticate the user on the local domain. To be sure you can go to **Start > Shutdown > Close all programs and log on as a different user**. If you cannot authenticate the user on the local domain, ACS will not work.
2. If you have checked **verify grant dialin permission for the users** in the Cisco Secure database configuration, check to see if dialin permission is granted for this user in the NT database.
3. If this is a dial connection, make sure that PAP or MS-CHAP (not CHAP) is configured on the router and PC.

Q. How do I configure the Novell Directory Server (NDS) database?

A.

If you select **NDS Server Support**, follow these steps:

1. See your Novell NetWare administrator to get the names and other information for the tree, container, and context.

2. Click **NDS Server Support**.
3. Enter a name for the configuration. This is for informational purposes only.
4. Enter the tree name.
5. Enter the full context list, separated by dots (.). You can enter more than one context list. If you do, separate them with a comma and space. For example, if your organization is Corporation, your organization name is Chicago, and you want to enter two context names, Marketing and Engineering, you would enter:

`Engineering.Chicago.Corporation, Marketing.Chicago.Corporation`

You do not need to add users in the context list.

6. Click **Submit**. Changes take effect immediately; you do not need to restart the ACS.

Caution: If you click **Delete**, your NDS database settings will be deleted.

Q. What should I check when users are unable to authenticate against the Novell Directory Server (NDS) database?

A. Check to see if the tree name, context name, and container name are all specified correctly. Start with one container where users are present, then you can add more containers later, if needed. If you are successful, then check on the NAS to see if you are able to authenticate the shell user (Telnet user). Also make sure that for PPP you have PAP authentication configured on the asynchronous interface.

Q. How can I troubleshoot a Security Dynamics International (SDI) authentication problem?

A.

1. The first thing you should do is authenticate the user with the ACE test agent.
2. If this works, then you can confirm that the card is synchronized with the database. Make sure to use DES encryption on the SDI server when the card is initialized. Choosing SDI will not work.
3. The next thing you should do is bring up the activity monitor on the ACE server while attempting Telnet authentication to a device.
4. Then check to see if there are any errors on the activity monitor on the ACE server.
5. If the ACE server works, but there is a problem with the dial users, then check the settings on the network access servers (NAS) to be sure that PAP is configured. Then try connecting as a non-SDI user.
6. If that works, then connecting as an SDI user should work. Put the user name in the user name tab and the passcode in the password tab on Dial-up Networking.
7. If the client from where you are dialing is configured to bring up the post terminal screen after dialing, then make sure you have the following AAA statement on the NAS:

```
aaa authentication ppp default if-needed tacacs+/Radius
```

The key is to use >if-needed> because this means that if the user is already authenticated by the following AAA statement:

```
aaa authentication login default tacacs+/radius
```

Then you don't have to authenticate the user again when doing PPP. This also applies when using the normal PAP password.

My ACS authentication isn't working for multilink services. What should I do?

A. You should go to **Interface Configuration > Tacacs+ (Cisco) > Add New Service**. Assign >ppp> as the service and >multilink> as the protocol.

Note: PPP and multilink are all lower case.

Q. Does ACS have any RADIUS support?

A. The degree of RADIUS support depends on the version of ACS. RFCs 2138 and 2139 are always supported, as are IOS vendor-specific attributes (VSAs). For a list of RADIUS support in a particular version, go to **Network Configuration > Network Device Groups > AAA Clients Area**.

Q. Is there a limit on the number of network access servers (NASs) that can be supported by ACS?

A. There is no limit because it is a function of how much the Windows NT registry can support, which is estimated to be thousands of servers. NAS information is not stored in the database. It is stored in the registry, which is why when you use the **csutil -d** command, you do not back up any NAS information.

Q. With Cisco Secure you can force the users to change their passwords after a given time period. Can you do this when you are using the Windows NT database for authentication?

A. Currently this feature only works when you are using the Cisco Secure database for authentication. This feature is being added in ACS 3.0, but it also requires device/client support. Device/client support will gradually be added to various hardware by Cisco Systems.

Q. How can users change their own passwords?

A. Users can be notified of expiring Cisco Secure database passwords on dial connections if the Cisco Secure Authentication Agent is on the PC. They can also use User Changeable Password software, which runs with Microsoft IIS, once the users are in the network. When the users are on the network, they can aim their browsers to the system where User Control Point (UCP) is installed and change their passwords.

Q. If replication fails, what things should I look for?

A. From the command line, issue the **net stop csauth** command to stop the service on each server. Then use the **csauth -z -p** command to run both the source and the target in debug, and look for messages in the window. The output also goes into the \$BASE\CSAuth\Logs\auth.log. Often one or more of the AAA servers is misconfigured, so look for messages on the target reporting requests from illegal or unknown hosts. If the source has several network adapters, then it can cause the target to see the wrong IP address and reject the source as unknown.

Q. My ACS "Logged in Users" report works with some devices, but not with others. What is the problem?

A. For the "Logged in Users" report to work (and this also applies to most other features involving sessions), packets should include at least the following fields:

Authentication Request packet

nas-ip-address
nas-port

Accounting Start packet

nas-ip-address
nas-port
session-id
framed-ip-address

Accounting Stop packet

nas-ip-address
nas-port
session-id
framed-ip-address

Attributes (such as nas-port and nas-ip-address) that appear in multiple packets should contain the same value in all packets.

If a connection is so brief that there is little time between the start and stop packets (for example, HTTP through the PIX), then logged-in users will not work either.

ACS version 3.0 allows the device to send either nas-port or nas-port-id.

Q. How is the the CRYPTOCARD software handled in ACS 3.0?

A. In ACS 3.0, the CRYPTOAdmin server component is removed from ACS; any future licenses, free or otherwise, must be obtained directly from CRYPTOCARD.

Q. What is the CRYPTOAdmin Authentication Server license policy for Cisco customers?

A. A full description of licensing terms and conditions and future upgrades can be obtained by sending an e-mail to sales@cryptocard.com, referencing product code CA5.1SC. A CRYPTOAdmin Server software evaluation package, including a time-limited license and software tokens, can be obtained from CRYPTOCARD's Download page.

Q. ACS accounting displays the message "NAS reset". What can cause this message to appear?

A. The "NAS reset" messages can be caused by reboot of the device or by having configured "tacacs-server host #.#.# single-connection" on IOS. If the device did not reboot, changing the configuration to "tacacs-server host #.#.#" should eliminate the messages.

Q. What encryption algorithm is used to store ACS passwords?

A. Passwords are encrypted using the Crypto API Microsoft Base Cryptographic Provider v1.0. This

offers either 56-bit or 128-bit encryption, depending on how the server is set up. The default cipher will be RC4.

Q. Does Cisco recommend a software application that can be used to do reporting on accounting logs available in ACS?

A. The ACS accounting logs can be recorded in one of two formats:

- ◆ **CSV files** The comma-separated value (CSV) format records data in columns separated by commas. This format is easily imported into a variety of third-party applications, such as Microsoft Excel or Microsoft Access. After data from a CSV file is imported into such applications, you can prepare charts or perform queries, such as determining how many hours a user was logged in to the network during a given period.
- ◆ **ODBC-compliant database tables** Open database connectivity (ODBC) logging lets you configure ACS to log directly into an ODBC-compliant relational database, where information is stored in tables, one table per log. After the data is exported to the relational database, you can use the data in any way you need.

With either method, software to parse logs is widely available, but Cisco does not recommend a particular vendor.

Q. Can ACS do translation proxy between RADIUS and TACACS+ and vice versa?

A. ACS can proxy from RADIUS to RADIUS or from TACACS+ to TACACS+, but it cannot do proxy between dissimilar protocols.

Q. How can I assign DNS and WINS server IP addresses for PPP connections from ACS using TACACS+?

A. You can specify DNS and WINS server IP addresses from the ACS on a per-user user basis or for a group of users by adding the following lines as custom attributes of PPP IP in the group setup.

```
dns-servers = 10.1.1.1 10.1.1.3  
wins-servers = 10.1.1.5 10.1.1.16
```

Q. How can I assign DNS and WINS server IP addresses for PPP connections from ACS using RADIUS?

A. You can specify DNS and WINS server IP addresses from the ACS on a per-user user basis or for a group of users by adding the following lines under Cisco RADIUS Attributes and AV-pair in group setup.

```
ip:wins-server=123.1.1.1 123.1.1.2  
ip:dns-servers=212.1.1.1 212.1.1.2
```

Q. How can you change the port in which RADIUS server listens in the registry settings?

A. Since version 2.5, ACS listens on RADIUS ports UDP 1645 and UDP 1812 for authentication and on ports 1646 and 1813 for accounting.

If you are using an older version, the listening ports can be changed by "regeditting" attribute values of the proper key in the Windows Registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAAv2.3\CSRradius  
"AuthenticationPort"=dword:1812
```

```
"AccountingPort"=dword:1813
This can also be changed in the newer version:
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAAv3.0\CSRADIUS
AccountingPort = 1646
AccountingPortNew = 1813
AuthenticationPort = 1645
AuthenticationPortNew = 1812
```

Q. Can I change the default port for TACACS+ to a value other than TCP 49?

A. You can change the default value of the port for TACACS+ services by editing attribute values of the proper key in the Windows Registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAAv3.0\CSTacacs
"Port"=dword:59
```

Q. I see odd things in the ACS GUI. For example, the same users appear in multiple groups and I cannot delete users from the database. How can I fix this kind of corruption?

A. Adding a user is a two-step process:

1. Add a new record to the end of the file.
2. Create an index path to the new record.

If there is an interruption of the CSAuth services during this process, it is possible that the record is in the database but cannot be edited because it uses a lookup through the indexing code.

To clean up the database, go into the command line and type the following command:

```
$BASE\utils\csutil -q -d -n -l dump.txt
```

"\$BASE" is the directory where the software was installed; issuing this command causes the database to be unloaded and reloaded to clear up the counters.

Q. I can't start services for RADIUS after re-installing the software several times. The event error says that service was terminated with "service specific error 11".

A. There are several different reasons why you might not be able to start the CSRADIUS service. The most common problem is running Windows with an unsupported service pack or there is software contention with another application. Supported platforms and service packs are specified in the installation documentation.

To check for port conflicts, you can go to the command line of the server and type **netstat -an | findstr 1645** and **netstat -an | findstr 1644** to see if any other service is using these User Data Protocol (UDP) ports. If another service is using these ports, you will see something similar to the following:

```
UDP 0.0.0.0:1645 *:*
UDP 0.0.0.0:1646 *:*
```

Another possible cause of the error message is that Microsoft Server services may not have been started. To check this, go to **Control Panel > Services** and ensure that the Server service options for **Started** and **Automatic** are selected.

Q. ACS installation fails, returning an error about "NSLDAPSSL32V30.dll" and saying that it cannot overwrite the file. What causes this and how can I resolve the error?

A. This error can be caused by contention with an installation of Cisco Secure VPN Client version 1.1. You can resolve the conflict by removing the VPN Client from the system.

Q. When I access the ACS GUI through a firewall, the address for the server in the URL field changes from a global IP address to a local address. Why does this happen?

A. In the current version of ACS 3.0, this problem has been addressed. The global IP address will not change when you change to subsequent pages after the initial login.

Q. I'm using ACS with servers in geographically dispersed areas, and services can be somewhat disrupted when I do replication. How can I deal with this?

A. First, make sure that the authenticating devices are configured for failover; in other words, make sure there are at least two servers defined to provide backup if one server is unreachable. (This is a good idea whether replication is involved or not.) For example, if the arrangement has one ACS in the U.S. replicating to a second ACS in Australia, configuring the authenticating devices to try the U.S. then Australia may not be the best plan. You might consider installing a second local server (in the U.S.) and replicating from the U.S. master to the U.S. slave. The U.S. slave could then replicate to the Australia slave.

Q. How can I obtain ACS 3.0 to upgrade a previous version?

A. Please refer to the Q & A for Cisco Secure ACS Version 3.0 for Windows 2000 and NT.

Q. Can a user be in more than one group at a time?

A. No, a user cannot be in more than one group at a time.

Q. When I turn on "enable authentication" in the switch or router with commands such as `aaa authentication enable default tacacs+` or `set authentication login tacacs enable telnet primary`, I am locked out of enable mode and the router says "Error in authentication". What should I do?

A. Check the failed attempts log in the ACS. If the log says "CS password invalid", it may be that there has not been a special enable password set up for the user. This is required when configuring "enable authentication". If you do not see **Advanced TACACS+ Settings** in the user options, go into **Interface Configuration > Advanced Configuration Options > Advanced TACACS+ Features** and select that option to get the TACACS+ settings to appear in the user settings. Then select **Max privilege for any AAA Client** (this will usually be 15) and enter the **TACACS+ Enable Password** that you want the user to have for enable.

Q. Default settings allow users to change their own passwords by Telnetting to the router. How can I disable this option?

A. To prevent users from changing their passwords via Telnet, follow the steps below.

1. Back up the local registry.
2. Go to registry key
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAAv<your_version>\CSTacacs.

3. Add a registry value by highlighting CSTacacs, right-clicking and selecting **NEW-DWORD**.
4. When the new key appears on the right-hand side of the window, type **disablechangepassword** into the new key window.
5. The default value for the new key is 0, which allows users to change the password. Right-click on the new key, select **Modify**, then change the key value to 1 to disable the ability to change the password.
6. After adding this new key, restart the cstacacs and csauth services.

Related Information

- [Cisco Secure ACS for Windows Documentation](#)
- [Cisco Secure ACS for Windows Support Page](#)
- [Field Notices for Cisco Secure ACS for Windows](#)

All contents are Copyright © 1992--2002 Cisco Systems Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Dec 13, 2002

Document ID: 8539
