

Cisco Secure ACS for Windows FAQ

Document ID: 8539

Questions

Introduction

How do I correct the 'User Access Filtered' error?

Does the 64 bit Operating System (OS) work with ACS products?

I cannot connect the ACS Solution Engine (SE) with an external Windows database. Why?

Is the authorization command supported in ACS Express?

How can I enable IETF pair # 80 – framed–pool on a Cisco Secure ACS?

How do I determine what the Message type 'Authen failed' means?

The user is unable to authenticate against sub–domain using ACS Express. Why does this occur?

Does the VMWare ESX Server support Windows ACS 4.1 and 4.2?

When I set up authentication, I receive the `Chpass is currently disabled.` error when I try to authenticate. How do I fix this problem?

When I attempt to download the database with the `csutil.exe –d` command, it results in the error message "Failed to initialize crypto API". What does this mean?

When I attempt to upgrade from Cisco Secure ACS for Windows 3.0.3 to 3.2, I receive the "ACS FOLDER IS LOCKED BY ANOTHER APPLICATION" error message.

What do I need to do?

Are the logs transferred in native ACS format or do/can they get converted to syslog?

How do you generate a log file on a daily basis on Cisco Secure ACS SE?

Are there any tools available that can be used to access and/or sort through the files?

When was Point–to–Point Tunneling Protocol (PPTP) with Microsoft Point–to–Point Encryption (MPPE) 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 to log in locally. Now everyone is locked out. How do I fix this?

The ACS documentation chapter on Cisco Secure ACS Command–Line Database utility explains how to bulk import a large number of users into ACS with the `csutil –i` command. How do I bulk import network access servers (NASes)?

I do not want the administrative overhead of having to list all the network access servers (NASes) in my network, and they all have the same tacacs–server keys. How do I set up a default key to use with my NASes?

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)? Why is CHAP unable to be used with the NT database?

Does 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 is successful, and the services run. What is the problem?

What do I need to check when users are unable to authenticate against the NT database?

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

What do I need to 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 does not work for multilink services. What do I need to do?

Does ACS have any RADIUS support?

Is there a limit on the number of network access servers (NASes) that are supported by ACS?

With Cisco Secure you can force the users to change their passwords after a given time period. Are you able to do this when you use the Windows NT database for authentication?

How do users change their own passwords?

If replication fails, what things do I need to 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 version 3.0 and later?

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?

Is ACS able to do translation proxy between RADIUS and TACACS+ and the reverse?

How do I assign Domain Naming System (DNS) and Windows Internet Naming Service (WINS) server IP addresses for PPP connections from ACS using TACACS+?

How do I assign Domain Naming System (DNS) and Windows Internet Naming Service (WINS) server IP addresses for PPP connections from ACS using RADIUS?

How do you change the port in which the 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 do I fix this kind of corruption?

I cannot start services for RADIUS after I re-install the software several times. The event error says that service was terminated with `service specific error 11`. The ACS installation fails and I see an error about `NSLDAPSSL32V30.dll` that says it cannot overwrite the file. What causes this and how do 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 use ACS with servers in geographically dispersed areas, and services are disrupted when I replicate. How do I deal with this?

How do I obtain ACS 3.2 in order to upgrade to an earlier 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 receive the `Error in authentication` error message on the router. What do I need to do?

Default settings allow users to change their own passwords by connecting to the router via Telnet. How do I disable this option?

Sometimes the timeout occurs during the attempt of communication to the remote agent. Why?

How do I recover the password for the Cisco Secure ACS Server?

How do I remove or delete the remote agents in the ACS?

Is DHCP relay supported on the ACS?

When remote agents are added to the ACS, this error occurs: Failed to commit all Fields. How can I resolve this error?

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

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

Q. How do I correct the 'User Access Filtered' error?

A. Either disable Network Access Restrictions (NAR) or completely configure it for use.

Q. Does the 64 bit Operating System (OS) work with ACS products?

A. No.

Q. I cannot connect the ACS Solution Engine (SE) with an external Windows database. Why?

A. The reason for this issue is the external Windows database is a 64 bit OS. ACS products do not work with the 64 bit OS.

Q. Is the authorization command supported in ACS Express?

A. No, this is available only with ACS and not with ACS Express.

Q. How can I enable IETF pair # 80 – framed–pool on a Cisco Secure ACS?

A. You cannot directly edit this attribute because the ACS GUI already has an option on how to set this value.

Within the "IP address assignment" section of the group editing, you have three options: "no ip address assignment", "assigned by dialup client", and "Assigned from AAA client pool". There is a fourth option, "Assigned from AAA server pool", if you have the pools assigned.

You need to use the third option ("Assigned from AAA client pool"). Setting this and then setting the name of the pool will return this value in attribute 88. User–side settings have these options if you need this to be configured at a per–user level. Also, you need to set the AAA client to authenticate using RADIUS (IETF).

Q. How do I determine what the Message type 'Authen failed' means?

A. Note the date and time of the message, go to the CSAAuth log file, and search on the date and time. A more detailed explanation of the message is then presented.

Q. The user is unable to authenticate against sub-domain using ACS Express. Why does this occur?

A. This issue occurs when the user does not provide a domain name. If the domain name is not provided, the ACS Express will try to append the domain name of the domain that the ACS Express is joined. If a user resides in a sub-domain, and the ACS Express is joined to a parent domain, then the user needs to provide a fully qualified domain name in the user name authentication.

Q. Does the VMWare ESX Server support Windows ACS 4.1 and 4.2?

A. ACS 4.1 and 4.2 have been tested on the VMWare ESX server with this configuration:

- ◆ VMWare ESX Server 3.0.0
- ◆ 16 GB of RAM
- ◆ AMD Opteron Dual Core processor
- ◆ 300 GB hard drive
- ◆ Four virtual machines
- ◆ Windows 2003 Standard Edition
- ◆ 3 GB of RAM for the guest operating system

Q. When I set up authentication, I receive the Chpass is currently disabled. error when I try to authenticate. How do I fix this problem?

A. The user account password must be set to **change on login**. In order to change the password, select **System Configuration > Local Password Management > Disable TELNET Change Password against this ACS and return the following message to the users Telnet session "Chpass is currently disabled."** and uncheck the box. This allows you to change the password.

Q. When I attempt to download the database with the csutil.exe -d command, it results in the error message "Failed to initialize crypto API". What does this mean?

A. You receive this error message when you log into a Cisco Secure ACS Server with an account other than the local admin account. This causes the inability of the **csutils** command to run.

Another cause for this error is that the passwords and AAA keys in the ACS database are encrypted with the help of the Microsoft Crypto API. Only local administrators and the actual system are able to access the important information needed in order to decrypt these passwords and keys.

Q. When I attempt to upgrade from Cisco Secure ACS for Windows 3.0.3 to 3.2, I receive the "ACS FOLDER IS LOCKED BY ANOTHER APPLICATION" error message. What do I need to do?

A. Complete these steps.

1. Run the Filemon utility in order to check for any "sharing violations" while you try the installation.

Note: Do *not* use terminal services in order to upgrade and disable the service temporarily.

2. Change the **System Configuration > Service Control > Manage Directory** to only keep the last seven files.

Q. Are the logs transferred in native ACS format or do/can they get converted to syslog?

A. No, they are native syslog.

Q. How do you generate a log file on a daily basis on Cisco Secure ACS SE?

A. For each CSV log, Cisco Secure ACS writes a separate log file. When a log file reaches 10 MB in size, Cisco Secure ACS starts a new log file. Cisco Secure ACS retains the most recent 7 log files for each CSV log. For more information on generating a log, refer to Enabling or Disabling a CSV Log.

Q. Are there any tools available that can be used to access and/or sort through the files?

A. No tools are supplied with ACS. For additional information, see Does Cisco recommend a software application that can be used to report on accounting logs available in ACS?

Q. When was Point-to-Point Tunneling Protocol (PPTP) with Microsoft Point-to-Point Encryption (MPPE) 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. However, 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 versions 3.0 and later support MS-CHAP versions 1 and 2.

Q. The ACS has been reconfigured to require a user name and password to log in locally. Now everyone is locked out. How do I fix this?

A. The solution to this problem depends on the version of software in place. 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 is modified in the registry. Issue the **regedit** command and search for `allow AutoLocalLogin`. Change the registry value to **1** in order to allow local login, and then recycle the services.

In ACS versions 2.6 and later, issue the **regedit** command and remove the users in this location:

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

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

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

A. The procedure used to bulk import NASes is similar to the import of users. This 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 NASes can also be imported into a particular Network Device Group. This flat-file is an example:

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

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

A. Add a default NAS in the NAS configuration area by leaving the host name and IP address blank. Enter only the key. Click **Submit**. You then see NAS `others` and `*.*.*.*`.

Note: This procedure only works for TACACS+, and 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 network access server (NAS) as described in the previous question for TACACS+, and then enumerate the NAS for RADIUS. The NAS sends RADIUS dial requests to ACS on the RADIUS port if the **aaa authentication ppp default if-needed RADIUS** command is issued.

The NAS sends TACACS+ Router Management requests to ACS on the TACACS+ port if the **aaa authentication login default TACACS+** command is issued.

Q. What are the differences between Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP)? Why is CHAP unable to be used with the NT database?

A. PAP sends passwords in the clear between the user and the TACACS+ or RADIUS client or device. If the password is correct, the authentication is acknowledged. Otherwise, the connection is terminated.

CHAP sends a challenge message to the remote user. The remote user responds with a value that calculates with the use of a one-way hash function. The client or 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 CHAP RFC (1994) requirement. It states:

"CHAP requires that the secret be available in plaintext form. Irreversibly encrypted password databases commonly available cannot be used."

This generally precludes the use of the NT database for CHAP, with Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) as an option.

Microsoft offers a hotfix that can provide a workaround for Microsoft Windows NT user databases. It allows user passwords to be saved in plain text format. For additional information, refer to CHAP Update for IAS (NT4.0 RADIUS Server) Authentication to Windows NT4.0 Domain Controllers .

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

A. Yes, ACS receives authentication requests from the network access servers (NASes) and forwards them to other servers. You need to define the other servers. In order to do this, select **Network Configuration > AAA Servers** 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 in order 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 with the help of the System Configuration tab, or 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 these 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 that runs the same version of software. If there is a need to clone an ACS box, replication is available instead.

If you need to copy only users and groups from one server to another, issue the **csutil -d** command. The new dump text (.txt) file is then copied to the target box. After this, issue the **csutil -n -l** command in order 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 you can use in order to check the release.

- ◆ When you bring up the browser, look for this 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:

```
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, an ACS and the SDIs Access Control Entry (ACE) server can be run on the same machine. There is also a client-server arrangement with an 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, select **System Configuration > Logging** in order to configure this.

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 probably comes in as DOMAIN_A\user or as user, names can appear in ACS as "DOMAIN_A\user" or as "user." This results in both entries in the database. The duplicate entries can be avoided with the use of domain stripping. This is where the prefix domain with the delimiter \ can be erased in order to have a consistent database. In order to set this up, select **Network Configuration > Proxy Distribution Table**.

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

A. ACS supports RDBMS databases, such as Oracle, in order to synchronize the database between two systems that use any RDBMS.

Q. When I try to bring up the GUI, I get an Invalid administration control error. The installation is successful, and the services run. What is the problem?

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

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

A. Complete these steps in order to troubleshoot the problem.

1. Check to see if you can authenticate the user on the local domain. In order to ensure this, select **Start > Shutdown > Close all programs and log on as a different user**. If you cannot authenticate the user on the local domain, ACS does 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 Password Authentication Protocol (PAP) or Microsoft Challenge Handshake Authentication Protocol (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**, complete these steps:

1. See your Novell NetWare administrator in order 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 (.). Separate multiple context lists 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), enter this information:

```
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 are deleted.

Q. What do I need to 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. You can add more containers later.

If you are successful, check the NAS in order to see if you are able to authenticate the shell user (Telnet user). Also ensure that for PPP you have Password Authentication Protocol (PAP) authentication configured on the asynchronous interface.

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

A. Complete these steps in order to troubleshoot an SDI authentication problem.

1. Authenticate the user with the Access Control Entry (ACE) test agent.
2. If this works, confirm that the card is synchronized with the database. Ensure you use Data Encryption Standard (DES) encryption on the SDI server when the card is initialized. A choice of SDI does not work.
3. Bring up the activity monitor on the ACE server while you attempt Telnet authentication to a device.
4. 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, check the settings on the network access servers (NAS) in order to ensure that Password Authentication Protocol (PAP) is configured. Then try to connect as a non-SDI user.
6. If this works, connection as an SDI user is expected to work. Enter 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 dial is configured to bring up the post terminal screen after you dial, ensure you issue this authentication, authorization, and accounting (AAA) command on the NAS:

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

The key is to use **if-needed**. This means that the user is already authenticated by issuing this AAA command:

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

Then you do not have to authenticate the user again when you do PPP. This also applies when you use the normal PAP password.

Q. My ACS authentication does not work for multilink services. What do I need to do?

A. Select **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. Request For Comments (RFCs) 2138 and 2139 are always supported, as are Cisco IOS® Software vendor-specific attributes (VSAs). For a list of RADIUS support in a particular version, select **Network Configuration > Network Device Groups > AAA Clients Area**.

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

A. There is no limit because it is a function of how much the Windows NT registry supports. This is estimated to be thousands of servers. NAS information is not stored in the database. It is stored in the registry. This is why when you issue 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. Are you able to do this when you use the Windows NT database for authentication?

A. This feature is available in all versions, when you use the Cisco Secure database for authentication. Versions 3.0 and later offer support of Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) Version 2 and MS-CHAP Password Aging. This works with the Microsoft Dial-Up Networking client, the Cisco VPN Client (versions 3.0 and later), and any desktop client that supports MS-CHAP. This feature prompts you to change your password after a login where the password has expired. The MS-CHAP-based password-aging feature supports users who authenticate with a Windows user database and is offered in addition to password aging supported by the Cisco Secure user database. This feature is added in ACS 3.0, but it also requires device or client support. Cisco Systems is gradually adding such device or client support to various hardware.

Q. How do users change their own passwords?

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

Q. If replication fails, what things do I need to look for?

A. From the command line, issue the **net stopcsauth** command in order to stop the service on each server. Then issue the **csauth -z -p** command in order 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 file. Often one or more of the authentication, authorization, and accounting (AAA) servers is misconfigured. Therefore, look for messages on the target that report requests from illegal or unknown hosts. If the source has several network adapters, then it causes 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. In order for the Logged In Users report to work (this also applies to most other features that involve sessions), packets need to include at least these 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 need to 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 do not work.

ACS versions 3.0 and later allow the device to send either `nas-port` or `nas-port-id`.

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

A. In ACS versions 3.0 and later, 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 the license terms and conditions and future upgrades are obtained by sending an E-mail to sales@cryptocard.com, the product code to use as a reference is CA5.1SC. A CRYPTOAdmin Server software evaluation package, that includes a time-limited license and software tokens, are 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 a reboot of the device or by issuing the **`tacacs-server host #.#.#.# single-connection`** command on the Cisco IOS Software. If the device does not reboot, issue the **`tacacs-server host #.#.#.#`** command in order to change the configuration to eliminate the messages.

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

A. Passwords are encrypted with the help of the Crypto API Microsoft Base Cryptographic Provider version 1.0, using the RC2 algorithm and a 40-bit key. For further information, refer to User Databases – About the Cisco Secure User Database.

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 are 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, prepare charts or perform queries, such as to determine how many hours a user is logged in to the network during a given period.
- ◆ **ODBC-compliant database tables** Open database connectivity (ODBC) logging allows you to 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, use the data in any way you need.

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

Q. Is ACS able to do translation proxy between RADIUS and TACACS+ and the reverse?

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

Q. How do I assign Domain Naming System (DNS) and Windows Internet Naming Service (WINS) server IP addresses for PPP connections from ACS using TACACS+?

A. You are able to specify DNS and WINS server IP addresses from the ACS on a per-user basis or for a group of users with the addition of these 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 do I assign Domain Naming System (DNS) and Windows Internet Naming Service (WINS) server IP addresses for PPP connections from ACS using RADIUS?

A. You are able to specify DNS and WINS server IP addresses from the ACS on a per-user basis or for a group of users with the addition of these 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 do you change the port in which the RADIUS server listens in the registry settings?

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

If you use an older version, change the listening ports. In order to do this, re-edit the 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\CSRradius
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. Change the default value of the port for TACACS+ services. In order to do this, edit the 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 do I fix this kind of corruption?

A. Complete these steps in order to add a user:

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

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

In order to clean up the database, go into the command line and issue the **\$BASE\utils\csutil -q -d -n -l dump.txt** command.

\$BASE is the directory where the software is installed. This command causes the database to be unloaded and reloaded in order to clear up the counters.

Q. I cannot start services for RADIUS after I re-install 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 are not 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.

In order to check for port conflicts, go to the command line of the server and issue the **netstat -an | findstr 1645** and **netstat -an | findstr 1644** commands to see if any other service uses these User Data Protocol (UDP) ports. If another service uses these ports, you see something similar to this output:

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

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

Another possible cause of the error message is that Microsoft Server services probably has not started. In order to check this, select **Control Panel > Services** and ensure that the Server service options for **Started** and **Automatic** are selected.

Q. The ACS installation fails and I see an error about NSLDAPSSL32V30.dll that says it cannot overwrite the file. What causes this and how do I resolve the error?

A. This error can be caused by contention with an installation of Cisco Secure VPN Client version 1.1. Resolve the conflict with the removal of 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 does not change when you change to subsequent pages after the initial login.

Q. I use ACS with servers in geographically dispersed areas, and services are disrupted when I replicate. How do I deal with this?

A. Ensure that the authenticating devices are configured for failover. In other words, ensure there are at least two servers defined in order 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. that replicates to a second ACS in Australia, configuring the authenticating devices to try the U.S. then Australia is probably not the best plan. Install a second local server (in the U.S.) and replicate it from the U.S. master to the U.S. slave. The U.S. slave then replicates to the Australia slave.

Q. How do I obtain ACS 3.2 in order to upgrade to an earlier version?

A. For more information, refer to Q & A for Cisco Secure ACS Version 3.2 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 receive the `Error in authentication error` message on the router. What do I need to do?

A. Check the failed attempts log in the ACS. If the log says `CS password invalid`, it can be that there has not been a special enable password set up for the user. This is required when you configure enable authentication. If you do not see **Advanced TACACS+ Settings** in the user options, select **Interface Configuration > Advanced Configuration Options > Advanced TACACS+ Features** and select that option in order to get the TACACS+ settings to appear in the user settings. Then select **Max privilege for any AAA Client** (this is usually 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 connecting to the router via Telnet. How do I disable this option?

A. In order to prevent users from changing their passwords through Telnet, complete these steps.

1. Back up the local registry.
2. Go to registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAAv<your_version>\CSTacacs`
3. Highlight **CSTacacs**. Then right-click and select **NEW-DWORD** in order to add a registry value.
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. This allows users to change the password. Right-click on the new key and select **Modify**. Then change the key value to **1** in order to disable the ability to change the password.
6. After you add this new key, restart the CSTacacs and CSAuth services.

Q. Sometimes the timeout occurs during the attempt of communication to the remote agent. Why?

A. Make sure that the software version on the ACS server and the remote agent must be the same. For example, if your ACS SE runs software version 4.1, then you must use the remote agent version 4.1 in the AD. If the software versions are not the same, the configuration will not work and you might receive this error message: `External DB user invalid or bad password`.

Q. How do I recover the password for the Cisco Secure ACS Server?

A. For the step-by-step procedure to recover the password for the Cisco Secure ACS Server, refer to Password Recovery Procedure for the Cisco Secure ACS Solution Engine which explains the recovery process in detail.

Q. How do I remove or delete the remote agents in the ACS?

A. Complete these steps in order to remove or delete the remote agents in the ACS:

1. Go to **Services** in the Windows server and stop the service of the ACS Agent.
2. Go to the ACS and stop the login services. Choose **System Configuration > login > Remote Login setup** and select **Do not log Remotely**.
3. Try to remove the remote agent. Refer to [Deleting a Remote Agent Configuration](#) for more information on deleting a remote agent.

Q. Is DHCP relay supported on the ACS?

A. No, DHCP relay is not supported on the ACS.

Q. When remote agents are added to the ACS, this error occurs: `Failed to commit all Fields`. How can I resolve this error?

A. The `Failed to commit all Fields` error message often occurs when a patch is not installed correctly or is corrupted. Re-imaging the ACS and restoring the configuration resolves the error.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [Cisco Secure ACS for Windows Documentation](#)
- [Cisco Secure ACS for Windows Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Aug 10, 2006

Document ID: 8539