

Cisco Secure ACS UNIX FAQ

Document ID: 4186

Questions

Introduction

General

Licensing and Software

System Configuration and Setup

Databases

GUI and Web Administration

Token Servers

User Profiles and Passwords

Accounting

Errors and Debugging

Related Information

Introduction

This document provides answers to common questions about Cisco Secure Access Control Server (ACS) for UNIX (CSUnix).

General

Q. Can data be migrated between CSUnix and Cisco Secure ACS for Windows (ACS)?

A. There are currently no supported tools used to migrate users from one product to another product.

Q. Does CSUnix authenticate against an NT database, LDAP, or Novell s NDS?

A. No, but these features are present in Cisco Secure ACS for Windows (ACS). Cisco Access Registrar supports Lightweight Directory Access Protocol (LDAP).

Licensing and Software

Q. Is CSUnix version 2.3.6.2 supported on Oracle version 9.2.0?

A. The release notes for CSUnix version 2.6.3.2 state that Oracle Enterprise version 8.0.x, 8i, and 9i version 9.0.1 are supported versions. It is possible to upgrade to Oracle version 9.2.0. However, it is recommended that you backup your database before you upgrade.

Q. How do I update an expired license key?

A. For details on how to obtain a license key, refer to Licensing Issues for Cisco Secure UNIX.

Q. How do I find my version of Solaris and the IP address of my system?

A. In order to determine the version of Solaris that you use, issue the **uname a** command.

In order to determine the IP address in use by your system, issue the **ifconfig a** command.

Q. Where can I get software upgrades and patches for CSUnix?

A. Software upgrades can be obtained from the Cisco Secure Access Control Server Software (registered customers only) web site. Software patches can be obtained from the Cisco Secure Software Patches – UNIX (registered customers only) web site.

Note: You must enter **cspatchunix** in the Special Access Code field to reach the Cisco Secure Software Patches – UNIX (registered customers only) web site.

Users who do not have a valid Cisco ID can obtain software upgrades and patches from Cisco Technical Support via E-mail and telephone. Refer to the Cisco Worldwide Contacts web site.

Q. Can I upgrade from CSUnix to Cisco Secure for Windows or Cisco Access Registrar?

A. For information about the pricing and availability of "lateral upgrades," contact your local Cisco account team.

Q. How do I determine my version of CSUnix?

A. Issue this command:

```
$BASE/CSU/CiscoSecure -v
```

\$BASE represents the directory in which CSUnix is installed.

Q. How do I recycle (shut down and start) the CSUnix services?

A. There are two different ways to recycle the services.

- ◆ Issue the **/etc/rc0.d/K80CiscoSecure** command to shut down, then issue the **/etc/rc2.d/S80CiscoSecure** command to restart.

OR

- ◆ Issue the **\$BASE/utills/kcs** command to shut down, then issue the **\$BASE/utills/scs** command to restart.

\$BASE represents the directory in which CSUnix is installed.

After services are restarted, issue the **\$BASE/utills/psg** command. It displays an entry for every service.

Q. How can I find out where CSUnix is installed on my machine?

A. In order to determine the CSUnix installation location, issue the **pkginfo -l CSCEacs** command.

Q. How do I know what values were selected during installation?

A. The CSUnix installation log is stored in **\$BASE/logfiles/cs_install.log**, where **\$BASE** represents the directory in which CSUnix is installed. This file lists all values selected during the installation.

Q. What are the hardware and software requirements for my version of CSUnix?

A. Requirements information is in the installation instructions for your specific software version. Requirements information is also summarized in Cisco Secure ACS UNIX Compatibility.

Q. Are there any export restrictions on CSUnix?

A. No, CSUnix is bundled with the exportable version of the Netscape FastTrack Server.

System Configuration and Setup

Q. How do I change the IP address, hostname, or fully qualified domain name (FQDN) of the CSUnix server?

A. The IP address, hostname, and FQDN for the server are stored in several files, based on the version of CSUnix in use. For this reason, the supported method used to change an IP address, hostname, or FQDN is to uninstall the software and then reinstall it with the desired settings. This operation does *not* affect the database. Users and groups are retained.

Complete these steps to make changes to the settings on your CSUnix server:

1. Shut down the software.
2. Back up the database. Oracle or Sybase can be backed up by the database administrator. Copy the **csecure.db** and **csecure.log** files to a safe place in order to back up SQLAnywhere. This is a precaution only, as the tables are not dropped during the uninstallation and reinstallation process. In addition, keep a copy of the **\$BASE/config/CSU.cfg** file. This file contains device information. **\$BASE** represents the directory in which CSUnix is installed.
3. Issue the **pkgm CSCEacs** command to uninstall the program. This command leaves the **csecure.db** and **csecure.log** files in place.
4. Ensure that name resolution works. In order to do this, issue the **hostname**, **nslookup**, and **ifconfig** commands as shown in this output.

```
# hostname

rtp-evergreen

# nslookup rtp-evergreen

Server: redclay2.cisco.com
Address: 172.18.125.3
Non-authoritative answer:
Name: rtp-evergreen.cisco.com
Address: 172.18.124.114

# nslookup rtp-evergreen.cisco.com
```

```
Server: redclay2.cisco.com
Address: 172.18.125.3
Non-authoritative answer:
Name: rtp-evergreen.cisco.com
Address: 172.18.124.114
```

```
# nslookup 172.18.124.114
```

```
Server: redclay2.cisco.com
Address: 172.18.125.3
Name: rtp-evergreen.cisco.com
Address: 172.18.124.114
```

```
# ifconfig -a
```

```
lo0: flags=849<UP,LOOPBACK,RUNNING,MULTICAST> mtu 8232
inet 127.0.0.1 netmask ff000000
le0: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500
inet 172.18.124.114 netmask ffff0000 broadcast 172.18.255.255
ether 8:0:20:76:79:f9
```

5. Install the software. Issue the **pkgadd -d path_to_software** command and indicate that this is an upgrade install as shown in this output.

```
New CiscoSecure install          no
.
.
.
SQLAnywhere DB directory         original_path
```

```
!--- Use the path in which the csecure.* files are located.
```

```
Drop existing database tables    no
```

6. After the installation is complete, start the software and ensure that the services run.

Q. I am having problems with the Domain Name System (DNS) on my network. How do I disable DNS IP-to-Hostname resolution on the CSUnix system so that it does not try to resolve names?

A. By default, CSUnix tries to resolve the incoming IP of the client device to a fully qualified domain name (FQDN) and then compares the FQDN to entries in the **CSU.cfg** file. If DNS in the network does not work properly, this can cause slow authentication and odd problems. In order to prevent CSUnix from attempting resolution, back up the **\$BASE/config/CSU.cfg** file (where **\$BASE** represents the directory in which CSUnix is installed). Next, modify it by adding this line to the beginning section with the other **NUMBER** entries:

```
NUMBER config_get_names_from_dns = 0;
```

Save the modified file, then recycle the server.

Q. How do I set the number of acceptable failed login attempts?

A. Complete these steps in order to set this value on a global basis for all users.

1. Open the **\$BASE/config/CSU.cfg** file (**\$BASE** represents the directory in which CSUnix is installed).
2. Add this line to the beginning section with the other **NUMBER** entries:

```
NUMBER config_max_failed_authentication = n;
```

Replace *n* with the number of permissible failed attempts.
Complete these steps in order to set this value on a per-user or per-group basis in CSUnix version 2.3.5.1 or later:

1. Open the **\$BASE/config/CSU.cfg** file.
2. Add this line to the beginning section with the other **NUMBER** entries:

```
NUMBER config_allow_global_max_failed_login_session_enable = 0;
```

Because the system uses the global settings by default, this line is used to turn off the global maximum bad authentications and allow per-user or per-group maximums to be set.

3. In the user or group profile, add this line:

```
set server max-failed-login-count = n;
```

Replace *n* with the number of permissible failed attempts.

Q. How do I change the default port (9900) on which the database listens?



Caution: CSUnix has not been tested for interoperability with other software. Multiple applications that run on the same server is not supported. This can cause performance problems and port conflicts on ports other than the dataserver port.

If you wish to run multiple instances of the database, shut down the CSUnix processes and modify these files to use a port other than 9900:

- ◆ \$BASE/CSU/libdb.conf
- ◆ \$BASE/FastAdmin/turbo.conf
- ◆ \$BASE/config/CSConfig.ini

\$BASE represents the directory in which CSUnix is installed.

Q. How do I view group or user profiles at the command-line interface?

A. Issue these commands at the **\$BASE/CLI/** directory prompt, where **\$BASE** represents the directory in which CSUnix is installed.

- ◆ Enter **./ViewProfile -p 9900 -u *username*** in order to view a user profile.

Replace *username* with user name for the user profile that you want to view.

- ◆ Enter **./ViewProfile -p 9900 -g *groupname*** in order to view a group profile.

Replace *groupname* with the name for the group profile that you want to view.

Q. How do I set the CSUnix web page to run on a port other than Port 80?



Caution: CSUnix has not been tested for interoperability with other software. Multiple applications that run on the same server is not supported. This can cause performance problems and port conflicts on ports other than the dataserver port.

If you wish to run multiple web servers, shut down the CSUnix processes and modify these files to use a port other than Port 80:

- ◆ In the `$BASE/ns-home/httpd-servername/config` file (where `$BASE` represents the directory in which CSUnix is installed), change **Port 80** to **Port *n***, where *n* is the new port on which you want it to run.
- ◆ In the `$BASE/FastAdmin/turbo.conf` file, change `NS_PATH=server/cs/` to `NS_Path=server:n/cs`, where *n* is the port number entered in the file.

Q. I forgot my password. How can I reset the Administrator profile?

A. Issue these commands in order to reset the Administrator password:

```
$BASE/CLI/DeleteProfile -p 9900 -u superuser
$BASE/CLI/AddProfile -p 9900 -u superuser
-a 'member = administrator \n privilege = web "password" 15 '
```

Note: The second command must be on *one* line.

Replace *password* in the second command with your new password. `$BASE` represents the directory in which CSUnix is installed.

Q. How can I tell what versions of the Acme FastTrack, Netscape Administration, and Netscape Communications servers are in use with Cisco Secure?

A. Cisco Secure uses a modified version of Acme Server version 1.7, dated November 13, 1996.

In order to determine the Netscape server versions, issue these commands (where `$BASE` represents the directory in which CSUnix is installed):

```
$BASEDIR/ns-home/admserv/ns-admin -v
Netscape Communications Corporation Netscape-Administrator/2.14,sec=e

$BASEDIR/ns-home/bin/httpd/ns-httpd -v
Netscape Communications Corporation Netscape-FastTrack/2.01c
```

Databases

Q. How many users does the 500 MB disk space requirement support using an SQLAnywhere database?

A. The 500 MB disk space requirement supports a maximum of 5,000 users.

Q. When is the `csdblog_YY-MM-DD` file created?

A. The `csdblog_YY-MM-DD` file is created the first time DBServer starts up and is then re-generated every 24 hours (approximate time).

Q. What is the highest number of users that can reasonably be maintained on a CSUnix server with SQLAnywhere, Oracle Server, or Sybase Server?

A. SQLAnywhere is officially supported for up to 5,000 users. Oracle and Sybase have been tested with up to a million users, each with ten attribute–value (AV) pairs. With this many users, maintenance is faster with the command–line interface (CLI) utilities instead of the HTML interface or the Java–based advanced GUI. Note that browsing via the GUI can be very slow. It can sometimes be faster to use the **Find** option in the advanced GUI or the **Edit > View** option in the HTML interface.

Q. How do I manually start the SQLAnywhere database?

A. Complete these steps in order to manually start the SQLAnywhere engine:

1. Set the necessary environment variables for the root user. In this example, c–shell is used. Also, issue these commands:

```
setenv SQLANY $BASE/SYBSSa50
setenv LD_LIBRARY_PATH $SQLANY/lib
set PATH=($path $SQLANY/bin)
```

2. Issue this command in order to start the database:

```
dbeng50 -n csecure $BASE/SQLANY/csecure.db
```

Replace *\$BASE/SQLANY* with the location of the SQLAnywhere database file.

Q. What value do I need to set for the database server connections?

A. In CSUnix version 2.3, the default value is 10. The database connections are shared with other applications like command–line interface (CLI) utilities and the GUI when they run and access the database. As a general rule, the number of database connections needs to equal the peak authentications per second, plus at least 3 for other ACS tasks, and approximately 25 percent for growth.

There are other factors that need to be considered. If you use the CLI online, then you need to add the number of parallel CLI connections that are used. For each parallel CLI connection, add an additional database connection. With CSUnix 2.3, accounting buffering uses up to eight database connections when enabled.

Note: The number of database connections is based on how CSUnix is used. Use this information only as a guideline.

Q. Is there a way I can view the database using SQL?

A. Yes, you can use the SQLAnywhere graphical user interface (ISQL) or the **ExecSql** command at the command line. Refer to Using ISQL to View the Cisco Secure Database for additional details. This document explains the database structure, gives an example of records, illustrates typical queries, and shows how to execute the queries using ISQL or using the **ExecSql** command through the command–line interface (CLI). It also discusses the **ViewProfile** and **DBClient** commands.

Q. How do I replicate the database using the default database software (SQLAnywhere) that comes with CSUnix?

A. Database replication with SQLAnywhere is not supported. Cisco only supports replication with Sybase Adaptive Server and Oracle 7.3.4 and later.

Two methods used to make a copy of an SQLAnywhere database are shown here.

- ◆ The SQLAnywhere database files (**csecure.db** and **csecure.log**) can be copied from one server to another after the services are shut down on the source server and the target server. Permissions and ownership of the files must be the same on the source server and the target server.
- ◆ The **dbbackup** command can be issued while the source server is up to create backup database files (**csecure.db** and **csecure.log**). These files can then be copied to the target server after services on the target server are shut down. Permissions and ownership of the files must be the same on the source server and the target server.

Q. How do I back up the SQLAnywhere database using the dbbackup command while CSUnix runs?

A. Complete these steps in order to issue the **dbbackup** command to back up the SQLAnywhere database while CSUnix still runs.

Note: This procedure assumes that you use c-shell. If you use a different shell, the **env** command allows you to check that the environment variables are set as shown here.

1. Issue these commands in order to set the environment variables:

```
setenv SQLANY $BASE/SYBSSa50
setenv LD_LIBRARY_PATH $SQLANY/lib
set path=($path $SQLANY/bin)
setenv SATMP $SQLANY/tmp
```

2. Issue this command in order to run the dbbackup utility:

```
dbbackup -c "ENG=csecure; UID=DBA; PWD=SQL" -x target_directory
```

Replace *target_directory* with the location where you want the csecure.db and csecure.log backups to be saved.

Q. Can I have CSUnix primary and backup servers so that devices can connect to the backup server if the primary server is down?

A. Yes, this failover connection to a backup server is determined at the device level. Most Cisco devices allow for failover when the primary CSUnix server is unavailable. For routers, the **tacacs-server host** or **radius-server host** entries are configured with the name or IP addresses of the various servers. User information must be available to the various servers in the event of a failover.

Q. Can I set up CSUnix in a distributed environment, with all administration done at a central site and the database distributed to local CSUnix servers?

A. Yes, you can set up a distributed environment with CSUnix using Oracle or Sybase databases.

Q. How does CSUnix interface with the database? Does it allow dynamic creation of accounts that can then be added to the CSUnix database?

A. CSUnix provides a command-line interface (CLI) and a GUI used to manage users and groups. Use either the CLI or the GUI to access the database to manage profiles, rather than any direct access to the database through SQL.

Q. I currently have one database type in Cisco Secure, and I want to migrate user or group data to a different database type (for example, Oracle to Sybase, SQLAnywhere to Oracle). How do I do this?

A. Complete these steps to export the users to a flat file and import them into CSUnix from that file.

Note: Prior to version 2.3.6.1, this procedure only imports TACACS+ profiles. As of version 2.3.6.1, this procedure also works for RADIUS profiles.

1. Issue this command in order to export the users into a flat file:

```
$BASEDIR/utils/CSexport -p file_path -d export_file_name
```

\$BASE represents the directory in which CSUnix is installed.

2. Issue these commands in order to import the users from this flat file:

```
$BASEDIR/utils/CSimport -t -p file_path -s import_file_name
```

```
!--- Run CSimport in test mode.
```

```
$BASEDIR/utils/CSimport -c -p file_path -s import_file_name
```

```
!--- Commit the changes to the database.
```

In these commands, *export_file_name* is the exported file name, *import_file_name* is the imported file name, and *file_path* is the directory in which the file is located.

Q. How do I determine the number of users that exist in the database for each CSUnix server? What SQL command syntax do I need to use?

A. Issue this command from the **\$BASE/utils/bin** directory (where **\$BASE** represents the directory in which CSUnix is installed):

```
$BASE/utils/bin/ ./ExecSql "select count(distinct profile_id) from cs_profile"
```

This command counts all user and group profiles. If you want to count only user profiles, replace **cs_profile** with **cs_user_profile**.

Q. What databases or database clients are compatible with my version of CSUnix?

A. For information on compatibility, refer to the install instructions for your specific version or to the summary in Cisco Secure ACS UNIX Compatibility.

Q. I have an existing database (or any relational database management system [RDBMS]) unrelated to Cisco Secure that contains my user information. Does CSUnix provide an import tool that can allow me to import this user information?

A. CSUnix does not provide a tool you can use to import users from an existing non-Cisco-Secure database. Because all databases have some mechanism to view and modify data, the "user info" can be extracted using SQL. Queried information from the existing database can be collected into a flat file and converted to a CSUnix syntax format that can then be imported into CSUnix with the **CSimport** command (for TACACS+) or the **CSmigrate** command (for RADIUS).

GUI and Web Administration

Q. I am unable to view all options in the ACS GUI. How do I correct this problem?

A. Turn on remote agent logging under **Interface Configuration > Advanced Options**. Check all of the options that you need.

Q. How do I access the Netscape FastTrack administrative server?

A. The FastTrack administrative server is usually accessed through a web browser. Use this procedure:

1. Go to this URL:

```
http://server_name:64000
```

Replace *server_name* with the name or IP address of the FastTrack administrative server.

2. Enter your username and password as shown here.

```
Username: admin  
Password: password
```

3. If the password does not work, complete these steps in order to reset it.
 - a. Edit the **\$BASE/ns-home/amdpw** file (where **\$BASE** represents the directory in which CSUnix is installed).
 - b. Find this line in the file:

```
admin:GuBqifMleNxmY
```

- c. Remove the encrypted password text after the colon and save the file. You can now log in as **admin** using a blank password.
4. If you get an `Unauthorized host` error message, complete these steps.
 - a. Edit the **ns-admin.conf** file in the **\$BASE/ns-home/admserv/** or **\$BASE/ns-home/admin-serv/** directory (where **\$BASE** represents the

directory in which CSUnix is installed).

Note: It can be possible that one of these files is not present.

b. Delete the **Hosts** and **Addresses** lines in the file.



Caution: Be sure to only delete the **Addresses** (ending in **es**) lines. *Do*

not delete the **Address** (no **es** ending) line.

c. Save the file.

d. Restart the administration server by issuing the **stop-admin** command and then the **start-admin** command at the **\$BASE/ns-home/** directory.

Q. What browsers are compatible with my version of CSUnix?

A. For information on compatibility, refer to the install instructions for your specific version or to the summary in Cisco Secure ACS UNIX Compatibility.

Token Servers

Q. Can I add the Security Dynamics Incorporated (SDI) ACE server after I install CSUnix?

A. Yes, you can enable the SDI ACE server with this procedure.

Note: Before you attempt an integration with CSUnix, it is a good idea to do an SDI client test authentication in order to ensure that SDI works by itself.

1. Shut down CSUnix.
2. Add these lines to the **\$BASE/config/CSU.cfg** file (where **\$BASE** represents the directory in which CSUnix is installed).

```
AUTHEN config_external_authen_symbols = {  
  {  
    "./libsdi.so",  
    "sdi"  
  }  
}
```

3. Restart CSUnix.

You can also enable the SDI ACE server using the CSUnix GUI, as shown here.

Note: Before you attempt an integration with CSUnix, perform an SDI client test authentication to ensure that SDI works by itself.

1. On the GUI menu, choose **AAA > General**.
2. In the **Authentication Methods** area of the General tab, click the **Secure Dynamic (ACE Server)** radio button.

For more information, refer to Configuring Cisco Secure UNIX and Secure ID (SDI Client).

Q. Can I install a Security Dynamics Incorporated (SDI) ACE server and CSUnix on the same machine?

A. Yes, if TACACS+ and RADIUS are disabled on the SDI ACE server. Errors can occur if both SDI ACE server and TACACS+ or RADIUS run at the same time. This is because SDI ACE server can use the same authentication protocols on the same ports.

Q. Can I use Challenge Handshake Authentication Protocol (CHAP) authentication with a Security Dynamics Incorporated (SDI) ACE server?

A. Yes, but the passcode is entered in a different way. For more information, refer to *Configuring Cisco Secure UNIX and Secure ID (SDI Client)*.

Q. What is token-caching and how do I enable it?

A. With token-based authentication, tokens are often good for only a limited period of time and cannot be reused within that period of time. These restrictions can cause problems for ISDN or multilink users. The initial token authentication is successful, but subsequent re-authentications can fail because the user interface does not allow users to input additional tokens.

When token-caching is used, the re-authentication requests are still sent to CSUnix. Then CSUnix sends back a `PASS` if the session or timeout conditions are met.

Complete these steps in order to use token-caching.

1. Token caching must be enabled in the user or group profile by adding this line:

```
set server token-caching=enable
```

2. Issue this command in order to set the condition or conditions under which the password expires and therefore how long the password remains valid.

```
set server token-caching-expire-method= [session | timeout | both]
```

◇ **session** keeps the cached password valid for the duration of the original session.

◇ **timeout** keeps the cached password valid for the specified amount of time.

◇ **both** keeps the cached password valid for the session and for a specified amount of time.

3. If either **timeout** or **both** was chosen in step 2, use this command to set the amount of time during which the password remains valid.

```
set server token-caching-timeout=120
```

Q. Does the functionality offered by CRYPTOAdmin supersede the support for CRYPTOCards that are incorporated into our CSUnix products? How do they differ?

A. The CRYPTOCard server bundled with CSUnix only provides token card support, whereas CRYPTOAdmin is a user-friendly management tool used to set up tokens and users. CRYPTOAdmin works with CSUnix and provides a client GUI which does not come bundled with CSUnix. CSUnix contains the CRYPTOCard toolkit. Therefore, CRYPTOAdmin effectively complements CSUnix. Refer to the CRYPTOCard web site for more information about CRYPTOAdmin.

User Profiles and Passwords

Q. How do I add User Profiles for TACACS+ in ACS (UNIX)?

A. In order to add this type of profile through the **AddProfile** command, the customer can use the **AddProfile -s** option [-s [Filename]]. The attributes can be put in a file and they can add the user as seen here.

```
*$BASEDIR/CLI* ./AddProfile -p 9900 -u userA -s script
```

These attributes are put in the script file.

```
*$BASEDIR/CL>* *vi script*

password = clear "userA"
default service=permit
service=Sandvine {
set Sandvine-HomeDir = "/tmp"
set Sandvine-Group = "sv_operator,sv_admin"
set Sandvine-Shell = "/bin/sh"
}
```

\$BASEDIR is the directory where Cisco Secure is installed.

Q. What are the minimum and maximum number of characters allowed in a password in CSUnix?

A. The database stores passwords up to 255 characters. The GUI interface enforces the minimum and the maximum. For more information, refer to the **Help** option in the CSUnix GUI. This describes the password rules.

Q. Does CSUnix allow me to change my password?

A. Yes, you can change your password through the Terminal (shell) login or through the CSUnix GUI. In order to change your password through the terminal (shell) login, complete these steps.

Note: This procedure only changes your clear-text password.

1. Use the **telnet** command to access the router.
2. When prompted, enter your assigned user name.
3. When asked for your password, leave it blank and press **Enter**. The message `Change password` sequence appears.
4. Enter your old password, then follow the prompts to enter and confirm your new password.

In order to change your password using the CSUnix GUI (HTML interface), complete these steps.

Note: This procedure automatically changes *all* of your assigned passwords. There is no way to change only some of your passwords.

1. Add this line to your user profile:

```
privilege = web "new_password" 1
```

Replace *new_password* with the new password that you would like to use.

2. In a web browser, go to this location:

```
http://host_name/cs
```

- Replace *host_name* with the name or IP address of the CSUnix server.
3. Log in with your assigned user name and the password used in step 1.

Q. Does CSUnix support password aging?

A. Yes, but only through the Telnet interface. Check these items:

- ◆ The user profile has an **until** date set for the password.
- ◆ The **CLI.cfg** file has lines that define these values:

```
config_warning_period x
config_expiry_period y
```

If all of these items are true, then the user receives an expiration message through Telnet *x* days prior to the **until** date. When the user starts the password change sequence by leaving their password blank and pressing **Enter**, the **until** date is incremented by *y* days. A sample user profile is shown in this output, with a brief explanation.

```
> ./ViewProfile -p 9900 -u abcde123

!--- In this example, abcde123 is used in place of an actual user name.

User Profile Information
user = abcde123{
profile_id = 21
profile_cycle = 1
password = clear "*****" until "8 Aug 2001"
}
```

In this example, if the **CSU.cfg** file has the lines **config_warning_period 5** and **config_expiry_period 30**, then the user named "abcde123" starts to receive Telnet warnings of password expiration on August 3 (five days prior to August 8). If the user changes the password in the Telnet interface on August 6, the **until** date in the profile is re-set for 30 days later. This results in a new expiration date of September 5.

Q. Is there an attribute that expires a user after a specified number of days of inactivity on an account?

A. Password aging is the closest option. See the password aging question in this document for more details. If a user does not log in by the date on which the password expires, then the account expires.

Note: Because password changing is not supported using PPP, this means that the expiration of users only works for terminal mode login.

Q. Does CSUnix enforce any restrictions on the password choices? In other words, does it disallow "easy" or "crackable" passwords?

A. No. CSUnix does not enforce any password restriction policies, including checking a dictionary or remembering older passwords. The principal restriction is that passwords must be a minimum length of six alphanumeric characters in order to be accepted. The only valid characters for passwords are alphabetic letters (A through Z and a through z) and numerals (0 through 9). Refer to the user guide for more information about password restrictions.

Q. If a user profile is "locked," how can I unlock the profile from the command line?

A. Complete these steps in order to issue the **DBClient** command to manually unlock a profile:

1. Issue this command at the command line:

```
$BASEDIR/DBClient/DBClient -p 9900
```

\$BASE represents the directory in which CSUnix is installed.

2. Enter these values when you are prompted.

```
username:  
admin_name
```

```
!-- Enter your administrator user name in place of admin_name.
```

```
password:  
admin_password
```

```
!-- Enter the administrator password in place of admin_password.
```

3. Type **unlock** and press **Enter**.
4. Type **user** = *user_name* . Replace *user_name* with the name of the user profile that you want to unlock.
5. Press **Enter** twice.
6. Type **exit** and press **Enter** to close the Command Prompt window.

Accounting

Q. Does CSUnix provide per-user account usage reports?

A. CSUnix does not provide such reports, but this information can be extracted from the database. The accounting information as provided by the network access server (NAS) is stored and can be extracted into a text file using the **AcctExport** utility. Once the account information is extracted from the database, a script can be created to parse the data and generate the necessary per-user report. When you issue the **AcctExport** *target* command, it removes accounting records from the database and places them in *target*.

Q. What happens if CSUnix generates new accounting records while the AcctExport command runs?

A. New records are not affected since the **AcctExport** command gathers the maximum ID numbers in the tables before it starts its export operation.

Q. How do I know whether or not the AcctExport command is successful?

A. If you issue the **AcctExport** command from the command-line, it returns the message **Successfully done**. If you access the **AcctExport** command from a program, an exit code of 0 indicates success, while an exit code of 1 indicates failure.

Q. If I enable Command Accounting, does CSUnix record the exact command entered into the router? For example, does it record a specific command like `ip route 135.52.0.0 255.255.0.0 1.1.1.1`?

A. When you issue the `aaa accounting command 15 start-stop tacacs+` command on the router, the full syntax of commands is recorded in the AAA server. This information can be retrieved from the database with the `AcctExport` command.

Some example records of accounting commands are shown here.

```
lab-i52.cisco.com dphillip tty18 170.69.200.7 start server=ciscosecure-sun
time=10:09:56 date=05/19/97 task_id=74 service=shell

lab-i52.cisco.com dphillip tty18 170.69.200.7 stop server=ciscosecure-sun
time=10:09:58 date=05/19/97 task_id=75 service=shell
priv-lvl=15 cmd=configure terminal <cr>

lab-i52.cisco.com dphillip tty18 170.69.200.7 stop server=ciscosecure-sun
time=10:10:03 date=05/19/97 task_id=76 service=shell
priv-lvl=15 cmd=ip route 1.1.1.1 255.255.255.255 Serial 0 <cr>
```

Q. Is CallerID captured in accounting?

A. Yes, CallerID is stored in the `rem_addr` field. It can contain both the Calling Line Identification (CLID) and Dialed Number Information Service (DNIS), which are separated by a forward slash (/).

Errors and Debugging

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

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

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

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

Q. While the CSUnix installs on the Solaris Core 8, it generates errors. Why is this?

A. Verify that package files are not missing from the core install:

```
/usr/lib/libX11.so.4, a symlink pointing to /usr/openwin/lib/libX11.s0.4
/usr/lib/libXext.so.0, a symlink pointing to /usr/openwin/lib/libXext.so.0
/usr/ucblib/libucb.so.1
```

Q. CSUnix receives the syslog message 'ERROR - unable to get name of NAS 134.' What does this mean?

A. If there is a Content Switching Server involved, go to it and remove `tacacs` from the server. Add `tacacs frequency 0` then add `tacacs` back to that server. This is similar to an attack and one of these resolves this issue.

Issue these commands in order to disable TACACS keepalives on the CSS server:

```
CSS(config)# no tacacs-server 10.152.4.24 49
CSS(config)# tacacs-server frequency 0
CSS(config)# tacacs-server 10.152.4.24 49 primary
```

Q. When I debug on my router, I receive a 'protocol garbled' error message. What does this mean?

A. You probably do not have a valid license key in the **CSU.cfg** file. Without the key, when CSUnix reaches four ports, it writes an error to the **\$BASE/logfiles/cs_startup.log** file (where **\$BASE** represents the directory in which CSUnix is installed). It then sends a `Licensed number of ports exceeded` message to the router. The router interprets this message as `protocol garbled`. For more details on licensing, refer to Licensing Issues for Cisco Secure UNIX.

Q. What do I need to do if I receive a 'Security Error' message when I connect to the advanced GUI?

A. Edit the **\$BASE/config/CSConfig.ini** file (where **\$BASE** represents the directory in which CSUnix is installed), and change the line **ValidateClients = true** to **ValidateClients = false**. Recycle the services so that the change takes effect. This setting tells CSUnix not to check the IP address of the incoming administrator.

If there is a need to check IP addresses, leave the **ValidateClients = true** line unchanged and include lines in the file that are similar to this output:

```
[Valid Clients]
100=chicago.cisco.com
102=1.2.3.4
```

Q. What do I need to do if I receive a 'Too many open files' error message in the startup log?

A. These error messages indicate that there are too few Solaris file descriptors available.

```
Jan 21 19:44:54 secs1 : (Too many open files)
Jan 21 19:53:17 secs1 CiscoSecure: ERROR - error on accept: (Too many open files)
```

In order to correct and prevent these errors, modify CSUnix configuration files as shown in these steps.

1. Increase the **ulimit** value to **4096** in the **\$BASE/bin/DBServer.sh** file (where **\$BASE** represents the directory in which CSUnix is installed), as shown here.

```
ulimit -n 4096
```

2. Increase the **ulimit** value to **256** in the **\$BASE/bin/AcmeServer.sh** file, as shown here.

```
ulimit -n 256
```

3. Set the **ulimit** value to **unlimited** in the **/etc/rc2.d/S80CiscoSecure** file, as shown here.

```
ulimit -n unlimited
```

Q. What do I need to do if I cannot start CSUnix and I see a 'seminit fail (libsec .8187)' message in the cs_startup.log file?

A. Check the permissions on the **/tmp** directory. They must be set to read, write, and execute (**rwX**) for users, groups, and other. The output from the **ls -ld /tmp** command returns something similar to this:

```
drwxrwxrwt 6 sys sys 317 Jul 8 12:00 /tmp
```

Note: The `seminit fail (libsec .8187)` message is a Netscape error message.

Q. What do I need to do if I try to use CSUnix and I receive a 'TAC+: Received unsane data from server' error message?

A. This means that there is either a key mismatch between the network access server (NAS) and CSUnix or there is a problem with the Domain Name System (DNS) or the Network Information Service (NIS).

In order to test your configuration, replace the NAS IP address or name with empty double quotes ("") in the **CSU.cfg** file. This replacement enables CSUnix to communicate with any client with a correct key. An example of the lines in the **CSU.cfg** file before and after the replacement is shown here.

◆ Before:

```
NAS config_nas_config = {
{
"192.91.124.172", /* NAS name can go here */
```

◆ After:

```
NAS config_nas_config = {
{
", /* NAS name can go here */
```

Also try to disable DNS in the **CSU.cfg** file by adding this line to the beginning section with the other **NUMBER** entries:

```
NUMBER config_get_dns_names = 0
```

Refer to the user guide for more details.

Q. What do I need to do if the console of the Cisco Secure server is flooded with the 'Can't locate server profile' error message?

A. This error message is usually cosmetic and is likely to occur when the database is copied from one server to another. If there is a server profile on the source server but no server profile on the target server, this message is generated.

In order to prevent this error, you can add the profile for the CSUnix server itself in the Advanced GUI. Or, if you do not use RADIUS, you can disable RADIUS with this procedure:

1. Backup the **/etc/rc2.d/S80CiscoSecure** file.
2. Edit the **/etc/rc2.d/S80CiscoSecure** file by inserting **-R** into the line shown here.

```
cd $BASE/CSU; $BASE/CSU/CiscoSecure -R -f $BASE/config/CSU.cfg  
>>$BASE/logfiles/cs_startup.log 2>&1
```

3. Restart the CSUnix services.

Q. How do I get protocol logging information and more detailed debugging down to the byte-level? I already changed the "config_logging_configuration" value in the CSU.cfg file, but I still do not get protocol logging.

A. Protocol debug information is not sent to the syslog. Instead, this information is written to standard error. In the normal configuration, the CSUnix server closes the standard error file descriptor, which causes the protocol debugs to get thrown into the bit bucket.

In order to see protocol-level debugs, you need to start the CSUnix server with the `-c -x` command-line options. This causes the AAA server to run in the foreground and keeps its standard output and standard error file descriptors open. You then see the protocol debugs on the console. These debugs can also be captured to a file using UNIX standard error redirection.

Q. How do I find out the number of files that a process has open?

A. Issue this command at the command line:

```
/usr/proc/bin/pfiles process_ID
```

Replace *process_ID* with the process ID number.

Related Information

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

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

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: May 14, 2009

Document ID: 4186
