

Cisco – CiscoSecure ACS UNIX Frequently Asked Questions

Table of Contents

<u>CiscoSecure ACS UNIX Frequently Asked Questions</u>	1
<u>Questions</u>	1
<u>General CSUnix Issues</u>	1
<u>Licensing and Software</u>	1
<u>System Configuration and Setup</u>	1
<u>Databases</u>	1
<u>GUI and Web Administration</u>	2
<u>Token Servers</u>	2
<u>User Profiles and Passwords</u>	2
<u>Accounting</u>	2
<u>Errors and Debugging</u>	3
<u>General</u>	3
<u>Licensing and Software</u>	3
<u>System Configuration and Setup</u>	5
<u>Databases</u>	7
<u>GUI and Web Administration</u>	10
<u>Token Servers</u>	11
<u>User Profiles and Passwords</u>	13
<u>Accounting</u>	14
<u>Errors and Debugging</u>	15
<u>Related Information</u>	17

CiscoSecure ACS UNIX Frequently Asked Questions

This document provides answers to some common questions about CiscoSecure ACS UNIX (CSUnix).

Questions

General CSUnix Issues

- Can my data be migrated between CSUnix and Cisco Secure ACS for Windows?
- Does CSUnix authenticate against an NT database, LDAP, or Novell's NDS?

Licensing and Software

- How do I update an expired license key?
- How do I find my version of Solaris and the IP address of my system?
- Where can I get software upgrades and patches for CSUnix?
- Can I "upgrade" from CSUnix to CiscoSecure for Windows NT or Cisco Access Registrar?
- How do I tell what version of CSUnix I'm running?
- How do I recycle (shut down and start) the CSUnix services?
- How can I find out where CSUnix is installed on my machine?
- How do I know what values were selected during the installation?
- What are the hardware and software requirements for my version of CSUnix?
- Are there any export restrictions on CSUnix?

System Configuration and Setup

- How do I change the IP address, hostname, or fully qualified domain name (FQDN) of the CSUnix server?
- I'm having problems with Domain Name System (DNS) on my network. How do I disable DNS IP-to-Hostname resolution on the CSUnix box so that it doesn't try to resolve names?
- How do I set the number of acceptable failed login attempts?
- How do I change the default port (set to 9900) that the database listens on?
- How do I view group or user profiles via the command-line interface?
- How do I change CSUnix's web page to run on a port other than 80?
- I forgot my password. How can I reset the Administrator profile?
- How can I tell what versions of the Acme Fast-track, Netscape Administration, and Netscape Communications servers are in use with CiscoSecure?

Databases

- How many users does the 500MB disk space requirement support using SQLAnywhere DB?
- When is the `csdblog_yy-mm-dd` file created?
- What is the highest number of users that can reasonably be maintained on a CSUnix server with SQLAnywhere? How many with Oracle Server or Sybase Server?
- How do I start the SQLAnywhere database manually?
- What value should I set for the database server connections?
- Is there a way I can view the database using SQL?

- How do I replicate the database using the default database software SQLAnywhere that comes with CSUnix?
- How do I back up the SQLAnywhere database using the dbbackup utility while the system is running (without shutting down CSUnix)?
- Can I have CSUnix primary and backup servers so that the devices can connect to the backup server if the primary server is down?
- Can I set up CSUnix in a distributed environment, with all administration done at the central site and the database distributed to local CSUnix servers for reliability?
- How does CSUnix interface with the database? Will it allow dynamic creation of accounts that can then be added to the CSUnix database?
- I currently have one database type in CiscoSecure, and I want to migrate user/group data to a different database type (for example, Oracle to Sybase, SQLAnywhere to Oracle). How do I do that?
- How do I determine the number of users that exist in the database per CSUnix server? What SQL command syntax should I use?
- What databases and/or database clients are compatible with my version of CSUnix?
- I have an existing database (or any relational database management system [RDBMS]) unrelated to CiscoSecure that contains my user information. Does CSUnix provide an import tool that will let me import this user information?

GUI and Web Administration

- How do I access the Netscape FastTrack administrative server?
- What browsers are compatible with my version of CSUnix?

Token Servers

- Can I add the Security Dynamics Incorporated (SDI) ACE server after installing CSUnix?
- Can I install SDI and CSUnix on the same machine?
- Can I use Challenge Handshake Authentication Protocol (CHAP) authentication with SDI?
- What is token-caching and how do I enable it?
- Does the functionality offered by CRYPTOAdmin supersede the support we have incorporated in our CSUnix products for CRYPTOCards? What are the differences?

User Profiles and Passwords

- What is the minimum/maximum number of allowable characters for a password in CSUnix?
- Will CSUnix allow me to change my password?
- Does CSUnix support password aging?
- Is there an attribute that would expire a user after a specified number of days of inactivity on an account?
- Does CSUnix enforce any restrictions on the password choices? In other words, does it disallow "easy" or "crackable" passwords?
- If a user profile is "locked," how can I unlock the profile from the command line?

Accounting

- Does CSUnix provide per-user account usage reports?
- What happens if CSUnix generates new accounting records while AcctExport is running?
- How do I know whether or not AcctExport was successful?
- If I enable Command Accounting, will the exact command entered into the router be recorded? For example, ip route 135.52.0.0 255.255.0.0 1.1.1.1?

- Is CallerID captured in accounting?

Errors and Debugging

- When debugging on my router, I get an error message that says "protocol garbled." What does this mean?
- What should I do if I get a "Security Error" when connecting to the advanced GUI?
- What should I do if I get the following "Too many open files" error messages in the startup log?
- I cannot start CSUnix, and I see "sem_init fail (libsec .8187)" in the `cs_startup.log` file. What should I do?
- When I try to use CSUnix, I get an error message that says "TAC+: Received insane data from server." What should I do?
- The console of the Cisco Secure server is getting flooded with the following error message: "CiscoSecure: ERROR – RADIUS: Can't locate server profile SERVER.#, using defaults." What should I do?
- How do I get protocol logging information and more detailed debugging down to the byte-level? I already changed the "config_logging_configuration" variable in the `CSU.cfg` file, but I'm still not getting protocol logging.
- How do I find out the number of files that a process has open?

Related Information

General

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

A. There are currently no supported tools for migrating users from one product to the other.

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 2000/NT (CSNT). Cisco Access Registrar supports Lightweight Directory Access Protocol (LDAP).

Licensing and Software

Q. How do I update an expired license key?

A. For details on obtaining a license key, refer to Licensing Issues for CiscoSecure UNIX.

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

A.

◇ Use the **uname -a** command to obtain the solaris version.

◇ Use the **ifconfig -a** command to obtain the IP address.

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

A. Registered users who have logged in can obtain Software upgrades from Cisco's Software Center. Software patches are available from the Special File Access area, using the the access code **cspatchunix**.

Users who do not have a valid Cisco ID can obtain software upgrades and patches from the Technical Assistance Center (TAC) via e-mail and telephone through the Cisco Worldwide Contacts.

Q. Can I "upgrade" from CSUnix to CiscoSecure for Windows NT or Cisco Access Registrar?

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

Q. How do I tell what version of CSUnix I'm running?

A. Run the following command:

\$BASE/CSU/CiscoSecure -v

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

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

◆ Type **/etc/rc0.d/K80CiscoSecure** to shut down, then type **/etc/rc2.d/S80CiscoSecure** to restart.

or

◆ Type **\$BASE/utlils/kcs** to shut down, then type **\$BASE/utlils/scs** to restart.

After services are restarted, the following command should show at least an entry for every service:

\$BASE/utlils/psg

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

A. To determine the installation location, run the following command:

pkginfo -l CSCEacs

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

A. The installation log is stored in **\$BASE/logfiles/cs_install.log**. 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 and is also summarized in the Cisco Compatibility Table.

Q. Are there any export restrictions on CSUnix?

A. No. In fact, CSUnix is bundled with the exportable version of Netscape's 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 server's IP address, hostname, and FQDN are stored in a host of files; these files can differ depending on version. For this reason, the supported method for changing an IP address, hostname, or FQDN is to uninstall the software and then reinstall with the desired settings. This operation does *not* affect the database; users and groups are retained.

Follow the steps below 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; SQLAnywhere can be backed up by copying the **csecure.db** and **csecure.log** files to a safe place. This is a precaution only, as the tables do not get dropped during the uninstallation/reinstallation process. In addition, keep a copy of the **\$BASE/config/CSU.cfg** file, because this contains device information.
3. Uninstall the software with the **pkgrm CSCEacs** command. This should leave the **csecure.db** and **csecure.log** files in place.
4. Ensure that name resolution works with the **hostname**, **nslookup**, and **ifconfig** commands. An example is shown below.

```
# 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 with the **pkgadd -d /<path_to_software>** command and indicate that this is an upgrade install.

```

New CiscoSecure install          no
.
.
.
SQLAnywhere DB directory        /opt/CSCOacs/sybase
                                {where the csecure.* files are}
Drop existing database tables    no

```

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

Q. I'm having problems with Domain Name System (DNS) on my network. How do I disable DNS IP-to-Hostname resolution on the CSUnix box so that it doesn't try to resolve names?

A. By default, CSUnix will try to resolve the incoming IP of the client device to a fully qualified domain name (FQDN) and will then compare the FQDN to entries in the **CSU.cfg** file. If DNS in the network is not working properly, this can cause slow authentication and odd problems. To prevent CSUnix from attempting resolution, back up the **\$BASE/config/CSU.cfg** file, then modify by adding the following line to the beginning section with the other **NUMBER** entries:

```
NUMBER config_get_names_from_dns = 0;
```

Save the revised file, then recycle the server.

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

A. To set this value on a global basis for all users, open the **\$BASE/config/CSU.cfg** file and set the following value:

```
NUMBER config_max_failed_authentication = #;
```

where # represents the number of failed attempts permitted. In versions 2.3.5.1 or later, this value can be set on a per-user or per-group basis.

This value also has to be enabled in the **\$BASE/config/CSU.cfg** file, as shown below.

```
!--- The system takes the global settings by default, so turn off the global
!--- maximum bad authentications to allow per-user or per-group maximum:
NUMBER config_allow_global_max_failed_login_session_enable = 0;
```

In the user or group profile, add the following line:

```
set server max-failed-login-count=#
```

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

A. CSUnix has not been tested for interoperability with other software. Running multiple applications on the same server is not supported, and issues of performance problems and port conflicts other than the dataserver port can be encountered. If you wish to run multiple instances of the database, shut down the CSUnix processes and modify the following files to use a port other than 9900:

- ◆ **\$BASE/CSU/libdb.conf**

- ◆ **\$BASE/FastAdmin/turbo.conf**

- ◆ \$BASE/config/CSCConfig.ini

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

A. Issue the following commands in the \$BASE/CLI directory.

- ◆ To view user profiles, type `./ViewProfile -p 9900 -u username`.
- ◆ To view group profiles, type `./ViewProfile -p 9900 -g groupname`.

Q. How do I change CSUnix's web page to run on a port other than 80?

A. CSUnix has not been tested for interoperability with other software. Running multiple applications on the same server is not supported, and issues of performance problems and port conflicts other than the dataserver port can be encountered. If you wish to run multiple web servers, shut down the CSUnix processes and modify the following files to use a port other than 80:

- ◆ In the file `$BASE/ns-home/httpd-servername/config`, modify the value **Port 80** to be **Port xx**.
- ◆ In the file `$BASE/FastAdmin/turbo.conf`, modify the value `NS_PATH=server/cs/` to be `NS_PATH=server:xx/cs`.

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

A. You can reset your password by running the following commands from the command line:

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

Replace `<password>` with your new password.

Q. How can I tell what versions of the Acme Fast-track, Netscape Administration, and Netscape Communications servers are in use with CiscoSecure?

A. The Acme server used by CiscoSecure is version 1.7, dated November 13, 1996 (which is modified for Cisco). To determine the Netscape server versions, issue the following commands:

```
$BASEDIR/ns-home/admserv/ns-admin -v Netscape Communications Corporation Netscape-Ad
$BASEDIR/ns-home/bin/httpd/ns-httpd -v Netscape Communications Corporation Netscape-
```

Databases

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

A. This amount of space 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 regenerated approximately every 24 hours.

Q. *What is the highest number of users that can reasonably be maintained on a CSUnix server with SQLAnywhere? How many with 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 10 AV pairs. With this many users, maintenance is faster using the Command Line Interface (CLI) utilities rather than the HTML interface or Java-based advanced graphical user interface (GUI). Note that browsing via the GUI may be very slow; using the "Find" option in the advanced GUI or the "Edit/View" function in HTML can be a little faster.

Q. *How do I start the SQLAnywhere database manually?*

A. To start the SQLAnywhere engine manually, ensure that the following environment variables are set up for the root user:

Using c-shell:

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

Then start the SQLAnywhere engine with the following command:

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

In command shown above, `$BASE/SQLANY` represents the location of the SQLAnywhere database file.

Q. *What value should I 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 graphical user interface (GUI) when they are running and are accessing the database. As a rule of thumb, the number of database connections should equal the peak authentications per second plus at least three for other Access Control Server (ACS) tasks, plus approximately 25% for growth.

There are other factors that need to be considered, however. If you are using CLI online, then you need to add the number of parallel CLI connections that are being used. For each parallel CLI connection, you should add an additional database connection. With CSUnix 2.3, enabling accounting buffering uses up to eight database connections. Please note that the number of database connections depends on how CSUnix is used, so the above information should be used only as a guideline.

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

A. Yes, you can use ISQL interface or the command line ExecSQL. For details, refer to Using ISQL to View the CiscoSecure Database. This document explains the database structure, gives an example of records, illustrates typical queries, and shows how to execute the queries through the command line interface (CLI) [ExecSQL] or the SQLAnywhere GUI (ISQL). Also discussed are ViewProfile and DBClient.

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

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

There are two methods to make an SQLAnywhere database copy:

- ◆ 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 and target servers. Permissions and ownership of the files need to be the same on the source and target servers.

or

- ◆ The **dbbackup** utility can be run while the source server is up to create the backup database files (**csecure.db** and **csecure.log**) to copy to the target server while the target server's services are shut down. Permissions and ownership of the files need to be the same on the source and target servers.

Q. How do I back up the SQLAnywhere database using the dbbackup utility while the system is running (without shutting down CSUnix)?

A. Setting the environmental variables necessary to run dbbackup will depend on the shell run. Whichever shell is in use, output of the **env** command must show that the following variables have been set. This example shows the c-shell:

```
setenv SQLANY $BASE/SYBSsa50
setenv LD_LIBRARY_PATH $SQLANY/lib
set path=($path $SQLANY/bin)
dbbackup -c "ENG=csecure; UID=DBA; PWD=SQL" -x <target directory>
```

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

A. Yes, this is determined at the device level. Most Cisco devices allow for failover in the event that 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. The user information must be available at the various servers in the event of a failover.

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

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

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

A. CSUnix offers a CLI (Command Line Interface) to manage users/groups. CLI or the graphical user interface (GUI) access are preferred choices over any direct interface through SQL to the database for managing profiles.

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

A. Use the following procedure to export the users to a flat file that is imported back into CSUnix.

1. Execute the following command to export the users into a flatfile of *<exportfilename>* in *<filepath>*:

```
$BASEDIR/utls/CSexport -p <filepath> -d <exportfilename>
```

2. Execute the following commands to import the users from this flat file:

```
◇ $BASEDIR/utls/CSimport -t -p <filepath> -s <importfilename> to run CSimport  
in test mode
```

```
◇ $BASEDIR/utls/CSimport -c -p <filepath> -s <importfilename> to commit the  
changes to the database
```

In these commands, *<exportfilename>* is the exported filename, *<importfilename>* is the imported filename, and *<filepath>* is the directory in which the file is located.

Note: Prior to version 2.3.6.1, this procedure only imports TACACS profiles; as of version 2.3.6.1, the procedure also works for RADIUS profiles.

Q. How do I determine the number of users that exist in the database per CSUnix server? What SQL command syntax should I use?

A. From the \$BASE/utls/bin directory (where \$BASE represents where CSUnix is installed), execute the following command:

```
./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 and/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 CiscoSecure ACS UNIX Compatibility.

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

A. CSUnix does not provide a tool for importing users from an existing non-CiscoSecure database. Since 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 be imported in CSUnix using CSimport (for TACACS+) or CSmigrate (for RADIUS).

GUI and Web Administration

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

A. Access to the FastTrack administrative server is usually by browser on `http://<name_of_server>:64000`.

Enter your username and password as shown below.

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

If the password does not work, edit the **admpw** file in **\$BASEDIR/ns-home/admserv/** directory. Reset the password by editing the following line in the file.

```
admin:GuBqifMleNxmY
```

Remove the encrypted password text after the colon and save the file. This will allow you to log in with an empty password.

If you get "Unauthorized host" messages, follow the steps below:

1. Edit the **ns-admin.conf** file in the **admserv** or **admin-serv** directory under **\$BASEDIR/ns-home/**.
2. Delete the "Hosts" and "Addresses" lines in the file. (Note that either one of these files might not be present).

Note: Do not confuse the **Addresses** line, which you should delete, with the **Address** line, which you should NOT delete.

3. Save the file, then restart the administration server by executing **stop-admin** then **start-admin** in **\$BASEDIR/ns-home/**.

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 CiscoSecure ACS UNIX Compatibility.

Token Servers

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

A. Yes. Prior to attempting integration with CSUnix, it is a good idea to do an SDI client test authentication to ensure that SDI is working by itself. To enable the SDI, shut down CSUnix and add a stanza to the **CSU.cfg** file as shown below, then restart CSUnix.

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

The above information can also be configured via the CSUnix "AAA/General" interface. In the **Authentication Methods** section of the General tab, check the **Secure Dynamic (ACE Server)** button.

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

Q. Can I install SDI and CSUnix on the same machine?

A. Yes, if TACACS+ and/or RADIUS are disabled in SDI. SDI can use the same authentication protocols on the same ports, so errors can occur if both are running simultaneously.

Q. Can I use Challenge Handshake Authentication Protocol (CHAP) authentication with SDI?

A. Yes, although the way that the passcode is entered is different. For more information, refer to CiscoSecure 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 a limited period of time and may not be reused within that period of time. This can cause problems for ISDN or multilink users; the initial token authentication is successful, but subsequent reauthentications can fail since the user interface does not give users the opportunity to input additional tokens. When token-caching is used, the reauthentication requests are still sent to CSUnix, and CSUnix sends back a 'PASS' if the session or timeout conditions are met.

Token caching must be enabled in the user or group profile, as shown below.

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

Use the command below to control how long the password will remain 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.

Use the following command to set the specified amount of time during which the password will be valid.

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

Q. Does the functionality offered by CRYPTOAdmin supersede the support we have incorporated in our CSUnix products for CRYPTOCards? How do they differ?

A. The CRYPTOCard server bundled with CSUnix provides only token card support, whereas CRYPTOAdmin is a user-friendly management tool used for setting up tokens and users. CRYPTOAdmin works with CSUnix and provides a client GUI, which doesn't come bundled with CSUnix. CSUnix contains CRYPTOCard's toolkit, however, so CRYPTOAdmin effectively complements CSUnix. Refer to the CRYPTOCard web site for more details on CRYPTOAdmin.

User Profiles and Passwords

Q. What is the minimum/maximum number of allowable characters for a password in CSU?

A. The database will store up to 255 characters for password values. The GUI interface will enforce the minimum and the maximum. For more information, check the **Help** link on the CSUnix GUI, which describes the password rules.

Q. Will CSUnix allow me to change my password?

A. Yes, you can change your password through the via Terminal (shell) login or through the CSUnix GUI.

1. **Terminal (shell) login** – To change your password, telnet into the router and enter your username when prompted. When asked for your password, hit ENTER. The message "Change password sequence" appears. Type your old password, then follow the prompts to type and confirm your new password. Note that this changes only the clear-text password.
2. **CSUnix GUI** – To change your password using the HTML interface, use the URL **http://[hostname]/cs** and log in with your assigned username and web-privilege password. Note that using this method will automatically change **all** of your assigned passwords; there is no provision to selectively change only some of your passwords. Changing the user password through the web requires the line: **privilege = web "<actual_password>" 1** in the user profile.

Q. Does CSUnix support password aging?

A. CSUnix does support password aging, but only through the telnet interface. If a user profile contains an **until** date for the password and if the **CSU.cfg** file has the **config_warning_period X** and **config_expiry_period Y** values defined, the user will get an expiration message via telnet **X** days prior to the **until** date. When the user hits ENTER at the password prompt and completes the password-change sequence, the **until** date will be incremented by **Y** days. An example profile is shown below, with a brief explanation.

```
>./ViewProfile -p 9900 -u abcde123
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 is set with the **config_warning_period 5** and **config_expiry_period 30** values, then the user will receive telnet warnings on August 3 (five days prior to August 8). If the user changes the password with the telnet interface on August 6, the **until** date in the profile will be reset for 30 days, resulting in a new expiration date of September 5.

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

A. Password aging is the closest option; see above for more details. If a user does not log in for longer than the password expiration, the account expires. Note that this only works for terminal mode login, since password changing is not supported using PPP.

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 policy (such as checking a dictionary or remembering older passwords). The principal restriction is that passwords must be a minimum length of six alphanumeric characters for a password. The only valid characters for passwords are alphabetic letters (**A** to **Z**, **a** to **z**) and numerals 0 to 9. Refer to the user guide for more information on password restriction.

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

A. You can use DBClient to unlock a profile manually by following the steps below.

1. From the command line, run **\$BASEDIR/DBClient/DBClient -p 9900**.

username: *superuser* (your admin user)

password: *changeme* (your admin password)

2. Type **unlock** and press RETURN.

3. Type **user = username**, where *username* is the user profile you want to unlock.

4. Press RETURN twice, then type **exit**.

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. Using the **AcctExport <target>** command will remove accounting records from the database and place them in <target>.

Q. What happens if CSUnix generates new accounting records while AcctExport is running?

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

Q. How do I know whether or not AcctExport was successful?

A. If you run AcctExport from the command-line, the user interface will say **Successfully done**. If you access AcctExport through program, an exit code of **0** indicates success, while a code of **1** indicates failure.

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

A. With **aaa accounting command 15 start–stop tacacs+** defined on the router, the exact command is recorded in the AAA server. This information can be retrieved from the database with the AcctExport utility.

Here are some accounting snippets:

```
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, it's in the **rem_addr** field. The **rem_addr** field can contains both the Calling Line Identification (CLID) and Dialed Number Information Service (DNIS), which are separated by a "/" character.

Note: DNIS information for ISDN calls is only available in Cisco IOS® Software Releases 11.2(6.2)F and later. DNIS for modem calls on a 5200 is sent in Cisco IOS Software Releases 11.1 and 11.2 and later. CLID is available for ISDN and modem calls in Cisco IOS® Software Releases 11.1 and 11.2 and later.

Errors and Debugging

Q. When debugging on my router, I get an error message that says "protocol garbled." 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 log and sends a message to the router that says "Licensed number of ports exceeded." (The router interprets this as "protocol garbled.") You can see this error on the CSUnix server in the **\$BASEDIR/logfiles/cs_startup.log** file. For more details on licensing, refer to Licensing Issues for CiscoSecure UNIX.

Q. What should I do if I get a "Security Error" when connecting to the advanced GUI?

A. Edit the **\$BASE/config/CSConfig.ini** file and change the line "ValidateClients = true" to be "ValidateClients = false". Recycle the services so that the change will take effect. This tells CSUnix not to check the IP address of the incoming administrator.

If there is a need to check IP addresses, lines in the file would read as follows:

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

Q. What should I do if I get the following error messages in the startup log?

```
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)
```

A. This error means that there are too few available Solaris file descriptors. To correct and prevent, modify files as shown below.

1. Increase the ulimit value in the following files:

```
$BASE/bin/DBServer.sh ulimit -n 4096
```

```
$BASE/bin/AcmeServer.sh: ulimit -n 256
```

2. Add a line to the following file:

```
/etc/rc2.d/S80CiscoSecure: ulimit -n unlimited
```

Q. I cannot start CSUnix, and I see "semint fail (libsec .8187)" in the cs_startup.log file. What should I do?

A. Check the permissions in the /tmp directory. The permissions on /tmp need to be set to "read," "write," and "execute" (rwx) for users, groups, and other. The output of the **ls -ld /tmp** command should return something similar to "drwxrwxrwt 6 sys sys 317 Jul 8 12:00 /tmp".

Note: This is a Netscape error message.

Q. When I try to use CSUnix, I get an error message that says "TAC+: Received unsane data from server." What should I do?

A. This generally means that there is either a key mismatch between the NAS and CSUnix or there is a DNS/NIS problem.

To test your configuration, replace the NAS IP address or name with an empty ("") in the **CSU.cfg** file. This replacement will enable CSUnix to communicate with any client as long as the key is correct. An example is shown below.

Change IP address

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

to ""

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

You can also try disabling DNS in the **CSU.cfg** file ("NUMBER config_get_dns_names = 0"). Refer to the user guide for more details.

Q. The console of the Cisco Secure server is getting flooded with the following error message: "CiscoSecure: ERROR - RADIUS: Can't locate server profile SERVER.#, using defaults." What should I

do?

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 for the target server, this message will be generated. To prevent this, you can add the profile for the CSUnix Server itself in the Advanced GUI, or you can disable the RADIUS service if you are not using RADIUS.

If you aren't using RADIUS, you can modify the startup script to start without the RADIUS part of the code.

To do this, back up and then modify the `/etc/rc2.d/S80CiscoSecure` file by adding `-R` to the following line as indicated below. (Note that the syntax is shown on two lines because of spacing considerations.)

Change

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

to

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

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" variable in the CSU.cfg file, but I'm still not getting protocol logging.

A. Protocol debug information isn't 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. 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 should then see the protocol debugs on the console. These debugs could 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. At the command line, type `/usr/proc/bin/pfiles (pid)`.

Related Information

- [Cisco Secure UNIX Support Page](#)
- [Documentation for Cisco Secure ACS for UNIX](#)

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

Updated: Dec 17, 2002

Document ID: 4186

