



Table of Contents



Cisco Secure ACS Command-Line Database Utility

[Location of CSUtil.exe and Related Files](#)

[CSUtil.exe Syntax](#)

[CSUtil.exe Options](#)

[Backing Up Cisco Secure ACS with CSUtil.exe](#)

[Restoring Cisco Secure ACS with CSUtil.exe](#)

[Creating a CiscoSecure User Database](#)

[Creating a Cisco Secure ACS Database Dump File](#)

[Loading the Cisco Secure ACS Database from a Dump File](#)

[Compacting the CiscoSecure User Database](#)

[User and AAA Client Import Option](#)

[Importing User and AAA Client Information](#)

[User and AAA Client Import File Format](#)

[About User and AAA Client Import File Format](#)

[ONLINE or OFFLINE Statement](#)

[ADD Statements](#)

[UPDATE Statements](#)

[DELETE Statements](#)

[ADD_NAS Statements](#)

[DEL_NAS Statements](#)

[Import File Examples](#)

[Exporting User List to a Text File](#)

[Exporting Group Information to a Text File](#)

[Exporting Registry Information to a Text File](#)

[Decoding Error Numbers](#)

[Recalculating CRC Values](#)

[User-Defined RADIUS Vendors and VSA Sets](#)

[About User-Defined RADIUS Vendors and VSA Sets](#)

[Adding a Custom RADIUS Vendor and VSA Set](#)

[Deleting a Custom RADIUS Vendor and VSA Set](#)

[Listing Custom RADIUS Vendors](#)

[RADIUS Vendor/VSA Import File](#)

[About the RADIUS Vendor/VSA Import File](#)

[Vendor and VSA Set Definition](#)

[Attribute Definition](#)


[Enumeration Definition](#)

[Example RADIUS Vendor/VSA Import File](#)

Cisco Secure ACS Command-Line Database Utility

This appendix details the Cisco Secure ACS command-line utility, CSUtil.exe. Among its several

functions, CSUtil.exe enables you to add, change, and delete users from a colon-delimited text file. You can also use the utility to add and delete AAA client configurations.

 **Note** You can accomplish similar tasks using the ACS System Backup, ACS System Restore, Database Replication, and RDBMS Synchronization features. For more information on these features, see "[Establishing Cisco Secure ACS System Configuration.](#)"

This appendix contains the following topics:

- [Location of CSUtil.exe and Related Files](#)
- [CSUtil.exe Syntax](#)
- [CSUtil.exe Options](#)
- [Backing Up Cisco Secure ACS with CSUtil.exe](#)
- [Restoring Cisco Secure ACS with CSUtil.exe](#)
- [Creating a CiscoSecure User Database](#)
- [Creating a Cisco Secure ACS Database Dump File](#)
- [Loading the Cisco Secure ACS Database from a Dump File](#)
- [Compacting the CiscoSecure User Database](#)
- [User and AAA Client Import Option](#)
- [Exporting User List to a Text File](#)
- [Exporting Group Information to a Text File](#)
- [Exporting Registry Information to a Text File](#)
- [Decoding Error Numbers](#)
- [Recalculating CRC Values](#)
- [User-Defined RADIUS Vendors and VSA Sets](#)

Location of CSUtil.exe and Related Files

When you install Cisco Secure ACS in the default location, CSUtil.exe is located in the following directory:

```
C:\Program Files\CiscoSecure ACS vX.X\Utils
```


where *XX* is the version of your Cisco Secure ACS software. Regardless of where you install Cisco Secure ACS, CSUtil.exe is located in the `Utils` directory.

Files generated by or accessed by `CSUtil.exe` are also located in the `Utils` directory.

CSUtil.exe Syntax

The syntax for the CSUtil.exe command is as follows:

```
CSUtil.exe [-q] [-c] [-d] [-g] [-i filename] [[-p] -l filename] [-e -number] [-b filename] [-r filename] [-f] [-n] [-u] [-y] [-listUDV] [-addUDV slotfilename] [-delUDV slot]
```

 **Note** Most CSUtil.exe options require that you stop the CSAuth service. While the CSAuth service is stopped, Cisco Secure ACS does not authenticate users. To determine if an option requires that you stop CSAuth, see the "[CSUtil.exe Options](#)" section.

You can combine many of the options in a single use of CSUtil.exe. If you are new to using CSUtil.exe, we recommend performing only one option at a time, with the exception of those options, such as -p, that must be used in conjunction with other options.

Experienced CSUtil.exe users may find it useful to combine CSUtil.exe options, such as the following example, which would first import AAA client configurations and then generate a dump of all Cisco Secure ACS internal data:

```
CSUtil.exe -i newnases.txt -d
```

CSUtil.exe Options


CSUtil.exe can perform several actions. The options, listed below in alphabetical order, are detailed in later sections of this chapter.

- **-b**—Backup system to a specified filename. For more information about this option, see the ["Backing Up Cisco Secure ACS with CSUtil.exe" section](#).
- **-c**—Recalculate database CRC values. For more information about this option, see the ["Recalculating CRC Values" section](#).
- **-d**—Export all Cisco Secure ACS internal data to a file named `dump.txt`. Using this option requires that you stop the CSAuth service. For more information about this option, see the ["Creating a Cisco Secure ACS Database Dump File" section](#).
- **-e**—Decode internal Cisco Secure ACS error numbers to ASCII message. For more information about this option, see the ["Decoding Error Numbers" section](#).
- **-g**—Export group information to a file named `groups.txt`. Using this option requires that you stop the CSAuth service. For more information about this option, see the ["Exporting Group Information to a Text File" section](#).
- **-i**—Import user or AAA client information from a file named `import.txt` or a specified file. For more information about this option, see the ["Importing User and AAA Client Information" section](#).
- **-l**—Load all Cisco Secure ACS internal data from a file named `dump.txt` or named file. Using this option requires that you stop the CSAuth service. For more information about this option, see the ["Loading the Cisco Secure ACS Database from a Dump File" section](#).
- **-n**—Create CiscoSecure user database and index. Using this option requires that you stop the CSAuth service. For more information about this option, see the ["Creating a CiscoSecure User Database" section](#).
- **-p**—Reset password aging counters during database load, to be used only in conjunction with the -l option. For more information about this option, see the ["Loading the Cisco Secure ACS Database from a Dump File" section](#).
- **-q**—Run CSUtil.exe without confirmation prompts.
- **-r**—Restore system from a specified backup filename. For more information about this option, see the ["Restoring Cisco Secure ACS with CSUtil.exe" section](#).
- **-u**—Export user information, sorted by group membership, to a file named `users.txt`. Using this option requires that you stop the CSAuth service. For more information about this option, see the ["Exporting User List to a Text File" section](#).
- **-y**—Dump Windows NT/2000 Registry configuration information to a file named `setup.txt`. For more information about this option, see the ["Exporting Registry Information to a Text File" section](#).
- **-addUDV**—Add a user-defined RADIUS vendor-specific attribute (VSA). For more information about this option, see the ["Adding a Custom RADIUS Vendor and VSA Set" section](#).
- **-delUDV**—Delete a user-defined RADIUS VSA. For more information about this option, see the ["Deleting a Custom RADIUS Vendor and VSA Set" section](#).
- **-listUDV**—List all user-defined RADIUS VSAs currently defined in Cisco Secure ACS. For

more information about this option, see the ["Listing Custom RADIUS Vendors" section](#).

Backing Up Cisco Secure ACS with CSUtil.exe

You can use the `-b` option to create a system backup of all Cisco Secure ACS internal data. The resulting backup file has the same data as the backup files produced by the ACS Backup feature found in the HTML interface. For more information about the ACS Backup feature, see the ["Cisco Secure ACS Backup" section](#).

 **Note** During the backup, all services are automatically stopped and restarted. No users are authenticated while the backup is occurring.

To back up Cisco Secure ACS with CSUtil.exe, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the ["Location of CSUtil.exe and Related Files" section](#).

Step 2 Type:


```
CSUtil.exe -b filename
```

where *filename* is the name of the backup file. Press **Enter**.

Result: CSUtil.exe displays a confirmation prompt.

Step 3 To confirm that you want to perform a backup and to halt all Cisco Secure ACS services during the backup, type **Y** and press **Enter**.

Result: CSUtil.exe generates a complete backup of all Cisco Secure ACS internal data, including user accounts and system configuration. This process may take a few minutes.

 **Note** CSUtil.exe displays the error message Backup Failed when it attempts to backup components of Cisco Secure ACS that are empty, such as when no administrator accounts exist. These apply only to the components that are empty, not to the overall success or failure of the backup.

Restoring Cisco Secure ACS with CSUtil.exe


You can use the `-r` option to restore all Cisco Secure ACS internal data. The backup file from which you restore Cisco Secure ACS can be one generated by the CSUtil.exe `-b` option or by the ACS Backup feature in the HTML interface.

Cisco Secure ACS backup files contain two types of data:

- User and group data

- System configuration

You can restore either user and group data or system configuration, or both. For more information about the ACS Backup feature, see the "[Cisco Secure ACS Backup](#)" section.

 **Note** During the backup, all services are automatically stopped and restarted. No users are authenticated while the restoration is occurring.

To restore Cisco Secure ACS with CSUtil.exe, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the "[Location of CSUtil.exe and Related Files](#)" section.

Step 2 Perform the applicable restoration command:

- To restore all data (user and group data, and system configuration), type:

```
CSUtil.exe -r all filename
```

where *filename* is the name of the backup file. Press **Enter**.

- To restore only user and group data, type:

```
CSUtil.exe -r users filename
```

where *filename* is the name of the backup file. Press **Enter**.

- To restore only the system configuration, type:


```
CSUtil.exe -r config filename
```

where *filename* is the name of the backup file. Press **Enter**.

Result: CSUtil.exe displays a confirmation prompt.


Step 3 To confirm that you want to perform a restoration and to halt all Cisco Secure ACS services during the restoration, type **Y** and press **Enter**.

Result: CSUtil.exe restores the specified portions of your Cisco Secure ACS data. This process may take a few minutes.

 **Note** If the backup file is missing a database component, CSUtil.exe displays an error message. Such an error message applies only to the restoration of the missing component. The absence of a database component in a backup is usually intentional and indicates that the component was empty in Cisco Secure ACS at the time the backup was created.

Creating a CiscoSecure User Database

You can use the -n option to create a CiscoSecure user database.

 **Note** Using the -n option requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.



Caution Using the -n option erases all user information in the CiscoSecure user database. Unless you have a current backup or dump of your CiscoSecure user database, all user accounts are lost when you use this option.

To create a CiscoSecure user database, follow these steps:

Step 1 If you have not performed a backup or dump of the CiscoSecure user database, do so now before proceeding. For more information about backing up the database, see the ["Backing Up Cisco Secure ACS with CSUtil.exe" section](#).

Step 2 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the ["Location of CSUtil.exe and Related Files" section](#).

Step 3 If the CSAuth service is running, type:

```
net stop csauth
```

and press **Enter**.

Result: The CSAuth service stops.

Step 4 Type:

```
CSUtil.exe -n
```

and press **Enter**.

Result: CSUtil.exe displays a confirmation prompt.

Step 5 To confirm that you want to initialize the CiscoSecure user database, type **Y** and press **Enter**.

Result: The CiscoSecure user database is initialized. This process may take a few minutes.

Step 6 To resume user authentication, type:

```
net start csauth
```

and press **Enter**.

Creating a Cisco Secure ACS Database Dump File

You can use the `-d` option to dump all the contents of the CiscoSecure user database into a text file. In addition to providing a thorough, eye-readable, and compressible backup of all Cisco Secure ACS internal data, a database dump can also be useful for the Cisco Technical Assistance Center (TAC) during troubleshooting.

Using the `-l` option, you can reload the Cisco Secure ACS internal data from a dump file created by the `-d` option. For more information about the `-l` option, see the ["Loading the Cisco Secure ACS Database from a Dump File" section](#).

Note Using the `-d` option requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

To dump all Cisco Secure ACS internal data into a text file, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the ["Location of CSUtil.exe and Related Files" section](#).

Step 2 If the CSAuth service is running, type:

```
net stop csauth
```

and press **Enter**.

Result: The CSAuth service stops.

Step 3 Type:

```
CSUtil.exe -d
```

Press **Enter**.

Result: CSUtil.exe displays a confirmation prompt.

Step 4 To confirm that you want to dump all Cisco Secure ACS internal data into `dump.txt`, type **Y** and press **Enter**.

Result: CSUtil.exe creates the `dump.txt` file. This process may take a few minutes.

Step 5 To resume user authentication, type:


```
net start csauth
```

and press **Enter**.

Loading the Cisco Secure ACS Database from a Dump File

You can use the `-l` option to overwrite all Cisco Secure ACS internal data from a dump text file. This option replaces the existing all Cisco Secure ACS internal data with the data in the dump text file. In effect, the `-l` option initializes all Cisco Secure ACS internal data before loading it from the dump text file. Dump text files are created using the `-d` option. While the `-d` option only produces dump text files that are named `dump.txt`, the `-l` option allows for loading renamed dump files. For more information about creating dump text files, see the ["Creating a Cisco Secure ACS Database Dump File" section](#).

You can use the `-p` option in conjunction with the `-l` option to reset password-aging counters.

 **Note** Using the `-l` option requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

To load all Cisco Secure ACS internal data from a text file, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the ["Location of CSUtil.exe and Related Files" section](#).

Step 2 If the CSAuth service is running, type:

```
net stop csauth
```

and press **Enter**.


Result: The CSAuth service stops.

Step 3 Type:

```
CSUtil.exe -l filename
```

where *filename* is the name of the dump file you want CSUtil.exe to use to load Cisco Secure ACS internal data. Press **Enter**.

Result: CSUtil.exe displays a confirmation prompt for overwriting all Cisco Secure ACS internal data with the data in the dump text file.

 **Note** Overwriting the database does not preserve any data; instead, after the overwrite, the database contains only what is specified in the dump text file.

Step 4 To confirm that you want to replace all Cisco Secure ACS internal data, type **Y** and press **Enter**.

Result: CSUtil.exe initializes all Cisco Secure ACS internal data, and then loads Cisco Secure ACS with the information in the dump file specified. This process may take a few minutes.

Step 5 To resume user authentication, type:

```
net start csauth
```

and press **Enter**.


Compacting the CiscoSecure User Database

Like many relational databases, the CiscoSecure user database handles the deletion of records by marking deleted records as deleted but not removing the record from the database. Over time, your CiscoSecure user database may be substantially larger than is required by the number of users it contains. To reduce the CiscoSecure user database size, you can compact it periodically.

Compacting the CiscoSecure user database consists of using in conjunction three CSUtil.exe options:

- **-d**—Export all Cisco Secure ACS internal data to a text file named `dump.txt`.
- **-n**—Create a CiscoSecure user database and index.
- **-l**—Load all Cisco Secure ACS internal data from a text file. If you do not specify the file name, CSUtil.exe uses the default file name `dump.txt`.

Additionally, if you want to automate this process, consider using the `-q` option to suppress the confirmation prompts that otherwise appear before CSUtil.exe performs the `-n` and `-l` options.

 **Note** Compacting the CiscoSecure user database requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

To compact the CiscoSecure user database, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the ["Location of CSUtil.exe and Related Files" section](#).

Step 2 If the CSAuth service is running, type:

```
net stop csauth
```

and press **Enter**.

Result: The CSAuth service stops.

Step 3 Type:

```
CSUtil.exe -d -n -l
```

Press **Enter**.

Tip If you include the `-q` option in the command, CSUtil.exe does not prompt you for



confirmation of initializing or loading the database.

Result: If you do not use the -q option, CSUtil.exe displays a confirmation prompt for initializing the database and then for loading the database. For more information about the effects of the -n option, see the "[Creating a CiscoSecure User Database](#)" section. For more information about the effects of the -l option, see the "[Loading the Cisco Secure ACS Database from a Dump File](#)" section.

Step 4 For each confirmation prompt that appears, type **Y** and press **Enter**.

Result: CSUtil.exe dumps all Cisco Secure ACS internal data to `dump.txt`, initializes the CiscoSecure user database, and reloads all Cisco Secure ACS internal data from `dump.txt`. This process may take a few minutes.

Step 5 To resume user authentication, type:

```
net start csauth
```

and press **Enter**.

User and AAA Client Import Option

The -i option enables you to update Cisco Secure ACS with data from a colon-delimited text file. You can also update AAA client definitions.

For user accounts, you can add users, change user information, or delete users. For AAA client definitions, you can add or delete AAA clients.

This section contains the following topics:

- [Importing User and AAA Client Information](#)
- [User and AAA Client Import File Format](#)

Importing User and AAA Client Information

To import user or AAA client information, follow these steps:

Step 1 If you have not performed a backup or dump of Cisco Secure ACS, do so now before proceeding. For more information about backing up the database, see the "[Backing Up Cisco Secure ACS with CSUtil.exe](#)" section.

Step 2 Create an import text file. For more information about what an import text file can or must contain, see the "[User and AAA Client Import File Format](#)" section.

Step 3 Copy or move the import text file to the same directory as CSUtil.exe. For more information about the location of CSUtil.exe, see the "[Location of CSUtil.exe and Related Files](#)" section.

Step 4 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe.

Step 5 Type:

```
CSUtil.exe -i filename
```

where *filename* is the name of the import text file you want CSUtil.exe to use to update Cisco Secure ACS. Press **Enter**.

Result: CSUtil.exe displays a confirmation prompt for updating the database.

Step 6 To confirm that you want to update Cisco Secure ACS with the information from the import text file specified, type **Y** and press **Enter**.

Result: Cisco Secure ACS is updated with the information in the import text file specified. This process may take a few minutes.

If the import text file contained AAA client configuration data, CSUtil.exe warns you that you need to restart CSTacacs and CSRADIUS in order for these changes to take effect.

Step 7 To restart CSRADIUS, follow these steps:

a. Type:

```
net stop csradius
```

and press **Enter**.

Result: The CSRADIUS service stops.

b. To start CSRADIUS, type:

```
net start csradius
```

and press **Enter**.

Step 8 To restart CSTacacs, follow these steps:

a. Type:

```
net stop cstacacs
```

and press **Enter**.

Result: The CSTacacs service stops.

b. To start CSTacacs, type:

```
net start cstacacs
```

and press **Enter**.

User and AAA Client Import File Format

The import file can contain six different line types. At least two are required. This section contains an overview topic, topics for each of the six line types, and an example section:

- [About User and AAA Client Import File Format](#)
- [ONLINE or OFFLINE Statement](#)
- [ADD Statements](#)
- [UPDATE Statements](#)
- [DELETE Statements](#)
- [ADD_NAS Statements](#)
- [DEL_NAS Statements](#)
- [Import File Examples](#)

About User and AAA Client Import File Format

Each line of a CSUtil.exe import file is a series of colon-separated tokens. Some of the tokens are followed by values. Values, like tokens, are colon-delimited. For tokens that require values, CSUtil.exe expects the value of the token to be in the colon-delimited field immediately following the token.

ONLINE or OFFLINE Statement

CSUtil.exe requires an ONLINE or OFFLINE token in an import text file. The file must begin with a line that contains only a ONLINE or OFFLINE token. The ONLINE and OFFLINE tokens are described in [Table E-1](#).

Table E-1 *ONLINE/OFFLINE Statement Tokens*

Token	Required	Value Required	Description
ONLINE	Either ONLINE or OFFLINE must be present	—	The CSAuth service remains active while CSUtil.exe imports the text file. CSUtil.exe performance is slower when run in this mode, but Cisco Secure ACS continues to authenticate users during the import.
OFFLINE	Either ONLINE or OFFLINE must be present	—	The CSAuth service is stopped while CSUtil.exe imports the text file. Although CSUtil.exe performance is fastest in this mode, no users are authenticated during the import. If you need to import a large amount of user information quickly, consider using the OFFLINE token. While performing an import in the OFFLINE mode stops authentication during the import, the import is much faster. For example, importing 100,000 users in the OFFLINE mode takes less than one minute.

ADD Statements

ADD statements are optional. Only the ADD token and its value are required to add a user to Cisco Secure ACS. The valid tokens for ADD statements are listed in [Table E-2](#).


 **Note** CSUtil.exe provides no means to specify a particular instance of an external user database type. If a user is to be authenticated by an external user database and Cisco Secure ACS has multiple instances of the specified database type, CSUtil.exe assigns the user to the first instance of that database type. For example, if Cisco Secure ACS has two LDAP external user databases configured, CSUtil.exe creates the user record and assigns the user to the LDAP database that was added to Cisco Secure ACS first.

Table E-2 ADD Statement Tokens

Token	Required	Value Required	Description
ADD	Yes	username	Add user information to Cisco Secure ACS. If the username already exists, no information is changed.
PROFILE	No	group number	Group number to which the user is assigned. This must be a number from 0 to 499, not a name. If you do not use the PROFILE token or fail to provide a group number, the user is added to the default group.
CHAP	No	CHAP password	Require a CHAP password for authentication.
SENDAUTH	No	sendauth password	Require a TACACS+ sendauth password.
CSDB	No	password	Authenticate the username with the CiscoSecure user database.
CSDB_UNIX	No	UNIX-encrypted password	Authenticate the username with the CiscoSecure user database, using a UNIX password format.
EXT_NT	No	—	Authenticate the username with a Windows NT/2000 external user database.
EXT_NDS	No	—	Authenticate the username with a Novell NDS external user database.
EXT_SDI	No	—	Authenticate the username with an RSA external user database.
EXT_ANPI	No	—	Authenticate the username with an AXENT external user database.
EXT_	No	—	Authenticate the username with a CRYPTOCARD

CRYPTO			external user database.
EXT_ODBC	No	—	Authenticate the username with an ODBC external user database.
EXT_LDAP	No	—	Authenticate the username with a generic LDAP external user database.
EXT_ENIGMA	No	—	Authenticate the username with a SafeWord external user database.
EXT_LEAP	No	—	Authenticate the username with a LEAP proxy RADIUS server external user database.
EXT_ACTV	No	—	Authenticate the username with an ActivCard external user database.
EXT_VASCO	No	—	Authenticate the username with a Vasco external user database.
EXT_RADIUS	No	—	Authenticate the username with a RADIUS token server external user database.

For example, the following ADD statement would create an account with the username "John", assign it to Group 3, and specify that John should be authenticated by the CiscoSecure user database with the password "closedmondays":

```
ADD:John:PROFILE:3:CSDB:closedmondays
```

UPDATE Statements

UPDATE statements are optional. They make changes to existing user accounts. Only the UPDATE token and its value are required by CSUtil.exe, but if no other tokens are included, no changes are made to the user account. The valid tokens for UPDATE statements are listed in [Table E-3](#).

Table E-3 UPDATE Statement Tokens

Token	Required	Value Required	Description
UPDATE	Yes	username	Update user information to Cisco Secure ACS.
PROFILE	No	group number	Group number to which the user is assigned. This must be a number from 0 to 499, not a name.
CHAP	No	CHAP password	Require a CHAP password for authentication.

SENDAUTH	No	sendauth password	Require a TACACS+ sendauth password.
CSDB	No	password	Authenticate the username with the CiscoSecure user database.
CSDB_UNIX	No	UNIX- encrypted password	Authenticate the username with the CiscoSecure user database, using a UNIX password format.
EXT_NT	No	—	Authenticate the username with a Windows NT/2000 external user database.
EXT_NDS	No	—	Authenticate the username with a Novell NDS external user database.
EXT_SDI	No	—	Authenticate the username with a RSA external user database.
EXT_ANPI	No	—	Authenticate the username with an AXENT external user database.
EXT_CRYPTO	No	—	Authenticate the username with a CRYPTOCARD external user database.
EXT_ODBC	No	—	Authenticate the username with an ODBC external user database.
EXT_LDAP	No	—	Authenticate the username with a generic LDAP external user database.
EXT_ENIGMA	No	—	Authenticate the username with a SafeWord external user database.
EXT_LEAP	No	—	Authenticate the username with a LEAP proxy RADIUS server external user database.
EXT_ACTV	No	—	Authenticate the username with an ActivCard external user database.
EXT_VASCO	No	—	Authenticate the username with a Vasco external user database.
EXT_RADIUS	No	—	Authenticate the username with a RADIUS token server external user database.

For example, the following UPDATE statement causes CSUtil.exe to update the account with

username "John", assign it to Group 50, specify that John should be authenticated by a UNIX-encrypted password, with a separate CHAP password "goodoldchap":

```
UPDATE:John:PROFILE:50:CSDB_UNIX:3A13qf9:CHAP:goodoldchap
```

DELETE Statements

DELETE statements are optional. The DELETE token and its value are required to delete a user account from Cisco Secure ACS. The DELETE token, detailed in [Table E-4](#), is the only token in a DELETE statement.

Table E-4 UPDATE Statement Tokens

Token	Required	Value Required	Description
DELETE	Yes	username	The name of the user account that is to be deleted.

For example, the following DELETE statement causes CSUtil.exe to permanently remove the account with username "John" from the CiscoSecure user database:

```
DELETE:John
```

ADD_NAS Statements

ADD_NAS statements are optional. The ADD_NAS, IP, KEY, and VENDOR tokens and their values are required to add a AAA client definition to Cisco Secure ACS. The valid tokens for ADD_NAS statements are listed in [Table E-5](#).

Table E-5 ADD_NAS Statement Tokens

Token	Required	Value Required	Description
ADD_NAS	Yes	AAA client name	The name of the AAA client that is to be added.
IP	Yes	IP address	The IP address of the AAA client being added.
KEY	Yes	shared secret	The shared secret for the AAA client.
VENDOR	Yes	See Description	The authentication protocol the AAA client uses. For RADIUS, this includes the VSA. The valid values are listed below. Quotation marks are required due to the spaces in the protocol names. "TACACS+ (Cisco IOS)"

			"RADIUS (IETF)" "RADIUS (Cisco IOS/PIX)" "RADIUS (Ascend)" "RADIUS (Cisco VPN 3000)" "RADIUS (Cisco VPN 5000)" "RADIUS (Cisco Aironet)" "RADIUS (Cisco BBSM)" "RADIUS (Nortel)" "RADIUS (Juniper)"
NDG	No	NDG name	The name of the Network Device Group to which the AAA client is to be added.
SINGLE_CON	No	Y or N	For AAA clients using TACACS+ only, the value set for this TOKEN specifies whether the Single Connect TACACS+ AAA Client option is enabled. For more information, see the "Adding and Configuring a AAA Client" section .
KEEPALIVE	No	Y or N	For AAA clients using TACACS+ only, the value set for this token specifies whether or not the Log Update/Watchdog Packets from this Access Server option is enabled. For more information, see the "Adding and Configuring a AAA Client" section .

For example, the following ADD_NAS statement causes CSUtil.exe to add a AAA client with the name "SVR2-T+", using TACACS+ with the single connection and keep alive packet options enabled:

```
ADD_NAS:SVR2-T+:IP:IP address:KEY:shared secret:VENDOR:"TACACS+ (Cisco
IOS)":NDG:"East Coast":SINGLE_CON:Y:KEEPALIVE:Y
```

DEL_NAS Statements

DEL_NAS statements are optional. The DEL_NAS token, detailed in [Table E-6](#), is the only token in a DEL_NAS statement. DEL_NAS statements delete AAA client definitions from Cisco Secure ACS.

Table E-6 DEL_NAS Statement Tokens

Token	Required	Value Required	Description
-------	----------	----------------	-------------

DEL_NAS	Yes	AAA client name	The name of the AAA client that is to be deleted.
---------	-----	-----------------	---

For example, the following DEL_NAS statement causes CSUtil.exe to delete a AAA client with the name "SVR2-T+":

```
DEL_NAS:SVR2-T+
```


Import File Examples

The following is an example import text file:

```
OFFLINE
ADD:user01:CSDB:userpassword:PROFILE:1
ADD:user02:EXT_NT:PROFILE:2
ADD:chapuser:CSDB:hello:CHAP:chappw:PROFILE:3
ADD:mary:EXT_NT:CHAP:achappassword
ADD:joe:EXT_SDI
ADD:vanessa:CSDB:vanessaspasword
ADD:juan:CSDB_UNIX:unixpassword
UPDATE:foobar:PROFILE:10
DELETE:paul
ADD_NAS:SVR2-T+:IP:209.165.202.136:KEY:A87il032bzig:VENDOR:"TACACS+ (Cisco
IOS)":NDG:"East Coast"
DEL_NAS:SVR16-RAD
```

Exporting User List to a Text File

You can use the `-u` option to export a list of all users in the CiscoSecure user database to a text file named `users.txt`. The `users.txt` file organizes the users by group. Within each group, users are listed by the order of the creation of the user account in the CiscoSecure user database. For example, if accounts were created for Pat, Dana, and Lloyd, in that order, `users.txt` lists them in that order as well, rather than alphabetically.

 **Note** Using the `-u` option requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

To export user information from the CiscoSecure user database into a text file, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the ["Location of CSUtil.exe and Related Files" section](#).

Step 2 If the CSAuth service is running, type:

```
net stop csauth
```

and press **Enter**.

Result: The CSAuth service stops.

Step 3 Type:

```
CSUtil.exe -u
```

and press **Enter**.

Result: CSUtil.exe exports information for all users in the CiscoSecure user database to a file named `users.txt`.


Step 4 To resume user authentication, type:

```
net start csauth
```

and press **Enter**.

Exporting Group Information to a Text File

You can use the `-g` option to export group configuration data, including device command sets, from the CiscoSecure user database to a text file named `groups.txt`. The `groups.txt` file is useful primarily for debugging purposes while working with the TAC.

 **Note** Using the `-g` option requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

To export group information from the CiscoSecure user database to a text file, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the ["Location of CSUtil.exe and Related Files" section](#).

Step 2 If the CSAuth service is running, type:

```
net stop csauth
```

and press **Enter**.

Result: The CSAuth service stops.

Step 3 Type:

```
CSUtil.exe -g
```

and press **Enter**.

Result: CSUtil.exe exports information for all groups in the CiscoSecure user database to a file named `groups.txt`.

Step 4 To resume user authentication, type:

```
net start csauth
```

and press **Enter**.

Exporting Registry Information to a Text File

You can use the `-y` option to export Windows Registry information for Cisco Secure ACS. CSUtil.exe exports the Registry information to a file named `setup.txt`. The `setup.txt` file is primarily useful for debugging purposes while working with the TAC.

To export registry information from Cisco Secure ACS to a text file, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the "[Location of CSUtil.exe and Related Files](#)" section.

Step 2 Type:

```
CSUtil.exe -y
```

and press **Enter**.

Result: CSUtil.exe exports Windows Registry information for Cisco Secure ACS to a file named `setup.txt`.


Decoding Error Numbers

You can use the `-e` option to decode error numbers found in Cisco Secure ACS service logs. These are error codes internal to Cisco Secure ACS. For example, the CSRADIUS log could contain a message similar to the following:

```
CSRADIUS/Logs/RDS.log:RDS 05/22/2001 10:09:02 E 2152 4756 Error -1087 authenticating  
geddy - no NAS response sent
```

In this example, the error code number that you could use CSUtil.exe to decode is "-1087":

```
C:\Program Files\CiscoSecure ACS vx.x\Utils: CSUtil.exe -e -1087  
CSUtil v3.0(1.14), Copyright 1997-2001, Cisco Systems Inc  
Code -1087 : External database reported error during authentication
```

 **Note** The `-e` option applies to Cisco Secure ACS internal error codes only, not to Windows error codes sometimes captured in Cisco Secure ACS logs, such as when Windows NT/2000 authentication fails.

For more information about Cisco Secure ACS service logs, see the "[Service Logs](#)" section.


To decode an error number from a Cisco Secure ACS service log, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the "[Location of CSUtil.exe and Related Files](#)" section.

Step 2 Type:

```
CSUtil.exe -e -number
```


where *number* is the error number found in the Cisco Secure ACS service log. Press **Enter**.

 **Note** The hyphen (-) before number is required.

Result: CSUtil.exe displays the text message equivalent to the error number specified.

Recalculating CRC Values

The -c option is for use by the TAC. Its purpose is to resolve CRC (cyclical redundancy check) value conflicts between files manually copied into your Cisco Secure ACS directories and the values recorded in the Windows Registry.

 **Note** Do not use the -c option unless a Cisco representative requests that you do.

User-Defined RADIUS Vendors and VSA Sets


This section provides information and procedures about user-defined RADIUS vendors and VSAs. It contains the following topics:

- [About User-Defined RADIUS Vendors and VSA Sets](#)
- [Adding a Custom RADIUS Vendor and VSA Set](#)
- [Deleting a Custom RADIUS Vendor and VSA Set](#)
- [Listing Custom RADIUS Vendors](#)
- [RADIUS Vendor/VSA Import File](#)

About User-Defined RADIUS Vendors and VSA Sets


In addition to a set of predefined RADIUS vendors and vendor-specific attributes (VSAs), Cisco Secure ACS supports RADIUS vendors and VSAs that you define. CSUtil.exe provides the mechanism for adding and deleting your custom RADIUS vendors and VSAs. Vendors you add must be IETF-compliant; therefore, all VSAs that you add must be sub-attributes of IETF RADIUS attribute number 26.

You can define up to ten custom RADIUS vendors, numbered 0 (zero) through 9. CSUtil.exe allows only one instance of any given vendor, as defined by the vendor's unique IETF ID number and by the vendor name.

 **Note** If you intend to replicate user-defined RADIUS vendor and VSA configurations, user-defined RADIUS vendor and VSA definitions to be replicated must be identical on the primary and secondary Cisco Secure ACS servers, including the RADIUS vendor slots that the user-defined RADIUS vendors occupy. For more information about database replication, see the ["CiscoSecure Database Replication" section](#).

Adding a Custom RADIUS Vendor and VSA Set

You can use the `-addUDV` option to add up to ten custom RADIUS vendors and VSA sets to Cisco Secure ACS. Each RADIUS vendor and VSA set is added to one of ten possible user-defined RADIUS vendor slots.

 **Note** While `CSUtil.exe` adds a custom RADIUS vendor and VSA set to Cisco Secure ACS, all Cisco Secure ACS services are automatically stopped and restarted. No users are authenticated while this process is occurring.

Before You Begin

- Define a custom RADIUS vendor and VSA set in a RADIUS vendor/VSA import file. For more information, see the .
- Determine the RADIUS vendor slot to which you want to add the new RADIUS vendor and VSAs. For more information, see the ["Listing Custom RADIUS Vendors" section](#).

To add a custom RADIUS VSA to Cisco Secure ACS, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing `CSUtil.exe`. For more information about the location of `CSUtil.exe`, see the ["Location of CSUtil.exe and Related Files" section](#).

Step 2 Type:

```
CSUtil.exe -addUDV slot-number filename
```

where *slot-number* is an unused Cisco Secure ACS RADIUS vendor slot and *filename* is the name of a RADIUS vendor/VSA import file. *filename* can include a relative or absolute path to the RADIUS vendor/VSA import file. Press **Enter**.


For example, to add the RADIUS vendor defined in `d:\acs\myvsa.ini` to slot 5, the command would be:

```
CSUtil.exe -addUDV 5 d:\acs\myvsa.ini
```

Result: `CSUtil.exe` displays a confirmation prompt.


Step 3 To confirm that you want to add the RADIUS vendor and halt all Cisco Secure ACS services during the process, type **Y** and press **Enter**.

Result: `CSUtil.exe` halts Cisco Secure ACS services, parses the vendor/VSA input file, and adds the new RADIUS vendor and VSAs to Cisco Secure ACS. This process may take a few minutes. After it is complete, `CSUtil.exe` restarts Cisco Secure ACS services.

 **Note** We recommend that you archive RADIUS vendor/VSA import files. During upgrades, the Utils directory, where CSUtil.exe is located, is replaced, including all its contents. Backing up RADIUS vendor/VSA import files ensures that you can recover your custom RADIUS vendors and VSAs after reinstallation or upgrading to a later release.

Deleting a Custom RADIUS Vendor and VSA Set

You can use the `-delUDV` option to delete a custom RADIUS vendor from Cisco Secure ACS.

 **Note** While CSUtil.exe deletes a custom RADIUS vendor from Cisco Secure ACS, all Cisco Secure ACS services are automatically stopped and restarted. No users are authenticated while this process is occurring.

Before You Begin

Verify that, in the Network Configuration section of the Cisco Secure ACS HTML interface, no AAA client uses the RADIUS vendor. For more information about configuring AAA clients, see the ["AAA Client Configuration" section](#).

Verify that your RADIUS accounting log does not contain attributes from the RADIUS vendor you want to delete. For more information about configuring your RADIUS accounting log, see the ["RADIUS Accounting Log" section](#).


To delete a custom RADIUS vendor and VSA set from Cisco Secure ACS, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the ["Location of CSUtil.exe and Related Files" section](#).

Step 2 Type:

```
CSUtil.exe -delUDV slot-number
```

where *slot-number* is the slot containing the RADIUS vendor that you want to delete. Press **Enter**.

 **Note** For more information about determining what RADIUS vendor a particular slot contains, see the ["Listing Custom RADIUS Vendors" section](#).

Result: CSUtil.exe displays a confirmation prompt.

Step 3 To confirm that you want to halt all Cisco Secure ACS services while deleting the custom RADIUS vendor and VSAs, type **Y** and press **Enter**.

Result: CSUtil.exe displays a second confirmation prompt.

Step 4 To confirm that you want to delete the RADIUS vendor, type **Y** and press **Enter**.

Result: CSUtil.exe halts Cisco Secure ACS services, deletes the specified RADIUS vendor from Cisco Secure ACS. This process may take a few minutes. After it is complete, CSUtil.exe restarts Cisco Secure ACS services.

Listing Custom RADIUS Vendors

You can use the -listUDV option to determine what custom RADIUS vendors are defined in Cisco Secure ACS. This option also enables you to determine which of the ten possible custom RADIUS vendor slots are in use and which RADIUS vendor occupies each used slot.

To list all custom RADIUS vendors defined in Cisco Secure ACS, follow these steps:

Step 1 On the Cisco Secure ACS server, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see the ["Location of CSUtil.exe and Related Files" section](#).

Step 2 Type:

```
CSUtil.exe -listUDV
```

Press **Enter**.

Result: CSUtil.exe lists each user-defined RADIUS vendor slot in slot number order. CSUtil.exe lists slots that do not contain a custom RADIUS vendor as "Unassigned". An unassigned slot is empty. You can add a custom RADIUS vendor to any slot listed as "Unassigned".

RADIUS Vendor/VSA Import File

To import a custom RADIUS vendor and VSA set into Cisco Secure ACS, you must define the RADIUS vendor and VSA set in an import file.

We recommend that you archive RADIUS vendor/VSA import files. During upgrades, the `utils` directory, where CSUtil.exe is located, is replaced, including all its contents. Backing up RADIUS vendor/VSA import files ensures that you can recover your custom RADIUS vendors and VSAs after reinstallation or upgrading to a later release.

This section details the format and content of RADIUS VSA import files. It includes the following topics:

- [About the RADIUS Vendor/VSA Import File](#)
- [Vendor and VSA Set Definition](#)
- [Attribute Definition](#)
- [Enumeration Definition](#)
- [Example RADIUS Vendor/VSA Import File](#)

About the RADIUS Vendor/VSA Import File

RADIUS Vendor/VSA import files use a Windows .ini file format. Each RADIUS vendor/VSA import file comprises three types of sections, detailed in [Table E-7](#). Each section comprises a section header and a set of keys and values. The order of the sections in the RADIUS vendor/VSA import file is irrelevant.

Table E-7 RADIUS VSA Import File Section Types

Section	Required	Number	Description
Vendor and VSA set definition	Yes	1	Defines the RADIUS vendor and VSA set. For more information, see the "Vendor and VSA Set Definition" section .
Attribute definition	Yes	1 to 255	Defines a single attribute of the VSA set. For more information, see the "Attribute Definition" section .
Enumeration	No	0 to 255	Defines enumerations for attributes with integer data types. For more information, see the "Enumeration Definition" section .

Vendor and VSA Set Definition

Each RADIUS vendor/VSA import file must have one vendor and VSA set section. The section header must be "[User Defined Vendor]". [Table E-8](#) lists valid keys for the vendor and VSA set section.

Table E-8 Vendor and VSA Set Keys

Keys	Required	Value Required	Description
Name	Yes	Vendor name	The name of the RADIUS vendor.
IETF Code	Yes	An integer	The IETF-assigned vendor number for this vendor.
VSA <i>n</i> (where <i>n</i> is the VSA number)	Yes—you can define 1 to 255 VSAs	Attribute name	<p>The name of a VSA. For each VSA named here, the file must contain a corresponding attribute definition section.</p> <p>Attribute names must be unique within the RADIUS vendor/VSA import file, and within the set of all RADIUS attributes in Cisco Secure ACS. To facilitate this, we recommend that you prefix the vendor name to each attribute name, such as "widget-encryption" for an encryption-related attribute for the vendor Widget. This also makes accounting logs easier to understand.</p>

For example, the following vendor and VSA set section defines the vendor "Widget", whose IETF-assigned vendor number is 9999. Vendor Widget has 4 VSAs (thus requiring 4 attribute definition sections):

```
[User Defined Vendor]
Name=Widget
IETF Code=9999
VSA 1=widget-encryption
VSA 2=widget-admin-interface
VSA 3=widget-group
VSA 4=widget-admin-encryption
```

Attribute Definition

Each RADIUS vendor/VSA import file must have one attribute definition section for each attribute defined in the vendor and VSA set section. The section header of each attribute definition section must match the attribute name defined for that attribute in the vendor and VSA set section. [Table E-9](#) lists the valid keys for an attribute definition section.

Table E-9 Attribute Definition Keys

Keys	Required	Value Required	Description
Type	Yes	See Description.	<p>The data type of the attribute. It must be one of the following:</p> <p>STRING</p> <p>INTEGER</p> <p>IPADDR</p> <p>If the attribute is an integer, the Enums key is valid.</p>
Profile	Yes	See Description.	<p>The attribute profile defines if the attribute is used for authorization or accounting (or both). At least one of the following two values must be present in the Profile key definition:</p> <p>IN—The attribute is used for accounting. After you add the attribute to Cisco Secure ACS, you can configure your RADIUS accounting log to record the new attribute. For more information about RADIUS accounting logs, see the "RADIUS Accounting Log" section.</p> <p>OUT—The attribute is used for authorization.</p> <p>In addition, you can use the value "MULTI" to allow several instances of the attribute per RADIUS message.</p>

			<p>Combinations are valid. For example:</p> <p>Profile=MULTI OUT</p> <p>or</p> <p>Profile=IN OUT</p>
Enums	No (only valid when the TYPE value is INTEGER)	Enumerations section name	<p>The name of the enumeration section.</p> <p>Several attributes can reference the same enumeration section. For more information, see the "Enumeration Definition" section.</p>

For example, the following attribute definition section defines the widget-encryption VSA, which is an integer used for authorization, and for which enumerations exist in the Encryption-Types enumeration section:

```
[widget-encryption]
Type=INTEGER
Profile=OUT
Enums=Encryption-Types
```

Enumeration Definition

Enumeration definitions enable you to associate a text-based name for each valid numeric value of an integer-type attribute. In the Group Setup and User Setup sections of the Cisco Secure ACS HTML interface, the text values you define appear in lists associated with the attributes that use the enumerations. Enumeration definition sections are required only if an attribute definition section references them. Only attributes that are integer-type attributes can reference an enumeration definition section.

The section header of each enumeration definition section must match the value of an Enums key that references it. An enumeration definition section can be referenced by more than one Enums key, thus allowing for reuse of common enumeration definitions. An enumeration definition section can have up to 1000 keys.

[Table E-10](#) lists the valid keys for an enumeration definition section.

Table E-10 Enumerations Definition Keys

Keys	Required	Value Required	Description
<i>n</i> (See Description.)	Yes	String	<p>For each valid integer value of the corresponding attribute, an enumerations section must have one key.</p> <p>Each key defines a string value associated with an integer value. Cisco Secure ACS uses these string values in the HTML interface.</p>

			<p>For example, if 0 through 4 are valid integer values for a given attribute, its enumeration definition would contain the following:</p>
--	--	--	--

```
0=value0
1=value1
2=value2
3=value3
4=value4
```

For example, the following enumerations definition section defines the Encryption-Types enumeration, which associates the string value 56-bit with the integer 0 and the string value 128-bit with the integer 1:

```
[Encryption-Types]
0=56-bit
1=128-bit
```

Example RADIUS Vendor/VSA Import File

The example RADIUS vendor/VSA import file, below, defines the vendor Widget, whose IETF number is 9999. The vendor Widget has 5 VSAs. Of those attributes, 4 are for authorization and one is for accounting. Only one attribute can have multiple instances in a single RADIUS message. Two attributes have enumerations for their valid integer values and they share the same enumeration definition section.

```
[User Defined Vendor]
Name=Widget
IETF Code=9999
VSA 1=widget-encryption
VSA 2=widget-admin-interface
VSA 3=widget-group
VSA 4=widget-admin-encryption
VSA 5=widget-remote-address

[widget-encryption]
Type=INTEGER
Profile=OUT
Enums=Encryption-Types

[widget-admin-interface]
Type=IPADDR
Profile=OUT

[widget-group]
Type=STRING
Profile=MULTI OUT

[widget-admin-encryption]
Type=INTEGER
Profile=OUT
Enums=Encryption-Types

[widget-remote-address]
Type=STRING
Profile=IN

[Encryption-Types]
0=56-bit
1=128-bit
```

2=256-bit

[HOME](#) [CONTENTS](#) [PREVIOUS](#) [NEXT](#) [GLOSSARY](#) [FEEDBACK](#) [SEARCH](#) [HELP](#)

Posted: Mon Jan 20 21:48:02 PST 2003

All contents are Copyright © 1992--2002 Cisco Systems, Inc. All rights reserved.

[Important Notices](#) and [Privacy Statement](#).