*e*Trust™ Single Sign-On

selang Command Reference Guide

r8

Computer Associates®

Second Edition

This documentation and related computer software program (hereinafter referred to as the "Documentation") is for the end user's informational purposes only and is subject to change or withdrawal by Computer Associates International, Inc. ("CA") at any time.

This documentation may not be copied, transferred, reproduced, disclosed or duplicated, in whole or in part, without the prior written consent of CA. This documentation is proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of this documentation for their own internal use, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the confidentiality provisions of the license for the software are permitted to have access to such copies.

This right to print copies is limited to the period during which the license for the product remains in full force and effect. Should the license terminate for any reason, it shall be the user's responsibility to return to CA the reproduced copies or to certify to CA that same have been destroyed.

To the extent permitted by applicable law, CA provides this documentation "as is" without warranty of any kind, including without limitation, any implied warranties of merchantability, fitness for a particular purpose or noninfringement. In no event will CA be liable to the end user or any third party for any loss or damage, direct or indirect, from the use of this documentation, including without limitation, lost profits, business interruption, goodwill, or lost data, even if CA is expressly advised of such loss or damage.

The use of any product referenced in this documentation and this documentation is governed by the end user's applicable license agreement.

The manufacturer of this documentation is Computer Associates International, Inc.

Provided with "Restricted Rights" as set forth in 48 C.F.R. Section 12.212, 48 C.F.R. Sections 52.227-19(c)(1) and (2) or DFARS Section 252.227-7013(c)(1)(ii) or applicable successor provisions.

Contents

Chapter 1: The selang Command Language

Chapter 2: selang Commands in the eTrust Environment

Chapter 3: selang Commands in the Windows Environment

Chapter 4: selang Commands in the Policy Model Environment

Chapter 5: Utilities

Chapter 6: eTrust Environment Classes and Properties

Chapter 7: Managing Policy Model Databases Remotely

Chapter 8: selang Commands in the UNIX Environment

Appendix A: Windows Values

Chapter

1

The selang Command Language

eTrust™ Single Sign-On (eTrust SSO) uses the eTrust™ Access Control data store. eTrust Access Control (eTrust AC) data store is administered through a command shell known as *selang*, the eTrust AC command language. This chapter contains a description of how to enter selang commands, a list of the commands by category, and other general information on the selang command language.

The following chapters provide a detailed description of the selang commands. selang works in several *environments*, and the commands for each are described in a separate chapter. Some commands are the same in the different environments, but they may have different parameters and arguments. You should, therefore, check the syntax carefully when beginning to work in a new environment.

The selang Command Shell

To invoke the selang command shell from Windows, run cmd.exe and change the directory to *eTrustACDir*\bin (where *eTrustACDir* is the directory where you installed eTrust AC, by default *system_directory*\Program Files\CA\eTrustAccessControl). Then type:

```
selang
```

You see the prompt:

```
eTrust>
```

When the prompt appears, you can enter selang commands. Enter commands separated with a semicolon (;). If you need to enter a command on more than one line, type a backslash (\) at the end of a line to continue typing the command on the next line.

If you would rather use a GUI than a command line interface, you can also access and update the eTrust AC and Windows databases using Policy Manager, as described in the *Getting Started* and in the *Administrator Guide*.

Working in Different Environments

In addition to working on the local eTrust AC database, selang can be used to modify the native Windows database, the local Policy Model database (PMDB), or a database on a remote host (Windows or UNIX) where eTrust AC is installed. To switch environments, use the "env" (environment) command, which is available in all environments.

To modify the local PMDB, type:

```
env pmd
```

The prompt changes to:

```
eTrust(pmd)>
```

From this point on, all selang commands operate on the PMDB.

To modify the local Windows database, type:

```
env nt
```

You see the prompt:

```
eTrust(nt)>
```

From this point on, selang commands modify the Windows database. To change back to the eTrust AC environment, type:

```
env eTrust
```

The prompt changes back to:

```
eTrust>
```

From this point on, all selang commands operate on the eTrust AC database instead of on the Windows database.

Tip: To change environments, you can also type the prefix only of the environment you want to change to. For example, to change to the eTrust environment, you could also type one of the following:

```
env e
env et
```

Or, to change to the PMD environment, you could also type one of the following:

```
env p
env pm
```

The selang command shells also support some common UNIX commands, allowing you to maintain the UNIX environment from within eTrust AC when you are connected to a UNIX machine. To enable UNIX commands, type:

```
env unix
```

For more information, see the chapter “selang Commands in the UNIX Environment” in the eTrust AC for UNIX *Reference Guide*.

The selang command shells operate on the local eTrust AC and PMDBs by default. To operate on the database of a different station, specify the hosts command before entering the selang commands. For more information, see the hosts command in the chapter “eTrust Environment Classes and Properties.”

Note: When you are entering the Native property of a command using env, the command is entered in both the Native environment and current environment.

Function Keys

A number of time saving shortcuts are included in the selang command shell. The following table describes the function keys that can be used with selang commands.

Key	Function
up arrow	Retrieves the previous command from the buffer. Pressing this key repeatedly calls commands higher in the buffer, which stores all commands entered in the session.
down arrow	Moves down in the buffer. Use this the same way as you use the up arrow key.
left arrow	Moves the cursor to the left in the command line. Toggle the Insert key to insert or overwrite text.
right arrow	Moves the cursor to the right in the command line
F1	Inserts the previous command, character by character.
F2	Displays a window with the instruction: “Enter char to copy up to:” When you enter a character from the previous command, selang enters the command up to the first instance of the character. If the character occurs more than once in the command, you can press F2 again to insert up to the next instance. Use Backspace to cancel.
F3	Enters the previous command (same as up arrow).

Key	Function
F4	Edits the previous instruction. Displays a window with the instruction: "Enter char to delete up to:" Use Backspace to cancel.
F5	Enters the previous command (same as up arrow).
F6	Enters a Ctrl Z (^Z) in the command line. This allows you to press Enter and continue entering the command on the next line.
F7	Displays a window listing the command history. You can use the up and down arrows to select any previous command. Use Esc to cancel.
F8	Enters the previous command, as the up arrow does, but with the cursor positioned at the beginning of the command line rather than at the end.
F9	Displays a window with the instruction: "Enter command number:" The number you enter inserts the command with the corresponding number in the F7 listing. Use Esc to Cancel

Help

You can get help at any time in the interactive selang command environment.

To enter selang online help, enter "?", "help", "h", "h *topic*", or "help *topic*" (where "*topic*" is a selang command or other topic related to the selang command shell).

The selang online help text appears on the screen. If you specified a topic, the help text that describes the topic appears; otherwise, the table of contents appears.

Tip: To display the help text for a command typed in the command line without deleting the text in the command line, type Ctrl+2.

For a complete description of the help command, see the help command in the Miscellaneous Commands section of this chapter.

Authorization

In order to use selang commands that change records in the eTrust or native operating system (native OS) database, you must have sufficient authority. For most commands, one of the following conditions must be met:

- You are the owner of the resource.
- You have the ADMIN attribute.
- The resource record is within the scope of a group in which you have the GROUP-ADMIN attribute.
- You have CREATE or MODIFY access authority in the ACL of the record in the ADMIN class.
- If your installation only allows management of the native Windows environment, you are a member of the eTrust AC Administrators group in the Windows database.

Exceptions to these general rules are noted in the description of the command.

selang Syntax Conventions

Each selang command performs a specific action on the eTrust AC database. The syntax of a selang command is:

```
commandname parameters
```

The command name tells eTrust AC which command to execute. You usually follow the command with one or more parameters that supply eTrust AC with additional information needed to execute the command.

The syntax of a selang parameter is:

```
parameterName[(arguments)]
```

The parameter name identifies the parameter to eTrust AC. Many parameters require arguments that provide eTrust AC with the information necessary to process the parameter. Some parameters accept more than one argument. When more than one argument is specified, separate the arguments with a comma or a space. The argument of a parameter may itself be a parameter.

To remove a record property when a string defines the argument, simply enter the property with empty parenthesis “()”. In some cases, you can use an asterisk (*) as an argument, to cover all possible values for that argument. If you use an asterisk, the asterisk does **not** override earlier or later commands that give specific values to the same argument. Moreover, if the argument is a file name, you can use a wildcard as part of a file name pattern. The wildcards are * (for zero or more characters) and ? (for one character).

The selang command language supports command and parameter prefixes. You need only enter the characters required to specify a unique command or parameter (that is, the prefix). You do not need to enter the command or parameter name in full.

For example, to enter the showusr command, type **showu**; eTrust AC identifies the command as the showusr command. In addition, every command has an abbreviated form consisting of one or more characters. For example, instead of typing the showusr command in full, you can type **su**.

In the UNIX environment, user-supplied information is case-sensitive and can consist of both lowercase and uppercase letters. For example, you may specify the full name of the user whose user ID is user53 as Mike Jones. Windows does not recognize case-sensitive information *but still saves it*. If you administer a remote Windows host from a UNIX workstation, UNIX will look for user-supplied information *as stored*. For example, if a user is identified in a Windows environment as Mike Jones, you may enter his name as mike jones when administering the local eTrust AC database. However, if you want to administer the database from a remote UNIX machine, you must enter his name as Mike Jones.

Command Conventions

The following conventions are used when explaining command syntax and user input.

Convention	Use
italic	Indicates a variable name or placeholder for which you must supply an actual value.
case sensitivity	System command and environment variable names may be case-sensitive depending on the requirements of your operating system. selang is sometimes case-sensitive. For example, class names must be entered in upper case. Generally, you can enter all selang commands and parameters in either lowercase or uppercase, unless otherwise noted.
no braces or brackets	Used with a mandatory item.
{ }	Encloses mandatory items used with the OR symbol (the vertical bar)
[ ]	Encloses an optional item.
| (OR)	Separates list items; choose one item.
\	When a command does not fit on one line, a backslash (\) at the end of a line of syntax indicates that the command continues on the next line; do not enter a backslash as part of the syntax. **Note:** A command continues on the next line exactly where you left off typing. If a space is required, as between a command and a parameter, you should add the space before you type the backslash. If you do not, and forget to start the next line with a space, selang returns an error.

Other Typographic Conventions

The eTrust AC documentation uses a few special conventions.

- Programming code is shown in this special font. For example:

  ```
  eTrust> nu
  ```

- The username *root* refers to the account with user ID number 0 (zero). The login name may be root, superuser, or any other name mapped to the same account.

- Bold text is also used for simple emphasis. For example:

  You should **never** tape your password to the monitor.

Command Line Options

The following is the help that is displayed for selang. It can be observed that some of the options do not appear in the description given and there are some extra options that do not appear in the actual syntax.

```
   selang <options>

Options:

 -c <command>              Execute <command> and exit.

 -d <dbdir>                Use database in <dbdir>.

 -f <input-file>           Read input from <input-file>.

 -h                        Display this text.

 -l                        Operate on a local database (sedlang).

 -o <output-file>          Write output to <output-file>.

 -p <policy-model-name>    Operate locally on a policy model.

 -r [<source-file>]        Read source file <source-file>. If no name specified
reads ~/.selangrc

 -s                        Silent mode (disable copyright message).

Note:

 When using the -c flags quote the command.

 The -c and -f options are mutually exclusive.

 The -d and -p options are mutually exclusive.

 The -d option can only be used to operate on a local database,

 There is no need to specify the -l option with -p or -d options.

 If the -h option is used all other options are ignored.
```

When invoking selang, some of the command line options available are:

-f *filename*

Reads the selang commands from the specified file instead of from the terminal. The selang command prompt does not appear, only the command currently being executed appears.

-h — Displays a list of selang commands and options.

-l — Specifies that selang is to operate on the default database, *eTrustACDir*\data. This option is only valid when the eTrust AC service (seosd) is not running.

-o *filename* — Writes the output of selang to the specified file instead of displaying it on the terminal. Each time selang is invoked, the file is created again; therefore, if you use the same file name again in the selang command, you overwrite the existing file.

-p *pmdbName* — Specifies the path and name of the PMDB on which selang is to operate. This database must be on the local machine. This option is not valid if either sepmdd or seosd is running. (Use the hosts command in selang to update a PMDB when seosd is running.) For a more detailed description, see the hosts command in the chapter “selang Commands in the eTrust Environment.”

-t *terminalName* — Writes the input of selang to *fileName* instead of to the command line. This option can only be used when also using the -o option.

For example, to write the input and output of selang to the same file, type:

```
selang –o -v fileName
```

To read the input from *fileName1* and write the commands and the output to *fileName2*, type:

```
selang -f fileName1 -o -v fileName2
```

Tip: To save time, create a batch file containing all the commands required to implement the security policy of the site.

For a complete list of the options available with selang, see the chapter “Utilities.”

Organization of the Command Reference Material

In the following chapters, the detailed descriptions of the commands are organized as follows:

- **Purpose**—Explains what the command does.
- **Authorization**—Lists the permissions required to use the command.
- **Syntax**—Describes the format of the command and any required or optional arguments. The syntax descriptions consist of the following elements:

- Keywords and required punctuation. Keywords must be entered as shown. Note that some keywords have an abbreviated form that you can use instead of typing the keyword in full.
- Variable parameters (in *italics*). You must replace each variable with a valid expression, as described in the description of the parameter.
- Positional parameters—keywords or variables that must occur in the order specified in the syntax—appear in the first line of the command syntax.
- Optional elements, enclosed in square brackets ([ ]). For example, consider the following command:

  ```
  newusr userName [auditor]
  ```

  This command shows that for newusr, the *userName* parameter is required but the *auditor* parameter is optional. Sometimes, optional clauses contain other optional clauses. **Square brackets are used only for describing command syntax and are not to be typed**. Do not confuse them with parentheses (), which are actually elements of selang commands.
- Lists (enclosed in braces, with options separated by vertical bars). For example, the following command:

  ```
  newfile name \ [audit({none|all|success|failure})]
  ```

  means to follow the audit parameter with one and only one of the choices shown—none, all, success, or failure. **The braces and vertical bars are used only for describing command syntax and are not to be typed**.

A list describing the arguments follows the command syntax.

- **Notes**—Discusses techniques for using the command and notes any special cases you should know about.
- **See Also**—Refers to related commands and applicable sections of the eTrust AC documentation.
- **Examples**—Contains examples on using the command.

selang Commands by Category

This section contains a complete list of selang commands arranged by the following categories:

- Commands for managing users
- Commands for managing groups
- Commands for managing resources
- Miscellaneous commands

Some commands appear in more than one category. The environment in which the command appears is also listed. The native environment is not listed, since it conforms to the rules of either the NT or UNIX environments, depending on the operating system of the host to which you are connected.

User Commands

Command	Environment	Description
authorize	eTrust, NT	Sets the authority a specific user has when accessing a specific resource.
authorize-	eTrust, NT	Removes the authority previously given to a specific user when accessing a specific resource.
chusr	eTrust, NT, UNIX	Changes existing user settings in the eTrust AC or native OS database.
editusr	eTrust, NT, UNIX	Adds a new user to, or changes an existing user in, the eTrust AC or native OS database.
join	eTrust, NT, UNIX	Joins a user to a group.
join-	eTrust, NT, UNIX	Removes a user from a group.
newusr	eTrust, NT, UNIX	Adds a new user to the eTrust AC or native OS database.
rename	eTrust, NT	Renames an object in the database. eTrust AC does not allow the management of resources that exceed 255 characters. Therefore, the maximum length of an object name is 255 characters. This limitation also applies to the native environment.
rmusr	eTrust, NT, UNIX	Removes users from the eTrust AC or native OS database.

Command	Environment	Description
showusr	eTrust, NT, UNIX	Lists the properties of user records in the eTrust AC or native OS database.
xaudit	NT	Sets auditing criteria and begins logging access events.
xaudit-	NT	Removes auditing criteria and stops logging access events.

Group Commands

Command	Environment	Description
authorize	eTrust, NT	Sets the authority a specific group has when accessing a specific resource.
authorize-	eTrust, NT	Removes the authority previously given to a specific group when accessing a specific resource.
chgrp	eTrust, NT, UNIX	Changes existing group settings in the eTrust AC or native OS database.
editgrp	eTrust, NT, UNIX	Adds a new group to, or changes an existing group in, the eTrust AC or native OS database.
join	eTrust, NT, UNIX	Joins a user to a group.
join-	eTrust, NT, UNIX	Removes a user from a group.
newgrp	eTrust, NT, UNIX	Adds a new group to the eTrust AC or native OS database.
rmgrp	eTrust, NT, UNIX	Removes a group from the eTrust AC or native OS database.
showgrp	eTrust, NT, UNIX	Lists the properties of group records in the eTrust AC or native OS database.
xaudit	NT	Sets auditing criteria and begins logging access events.
xaudit-	NT	Removes auditing criteria and stops logging access events.

Resource Commands

Command	Environment	Description
authorize	eTrust, NT	Sets the authority a specific accessor has when accessing a specific resource.
authorize-	eTrust, NT	Removes the authority previously given to a specific accessor when accessing a specific resource.
chfile	eTrust, NT, UNIX	Changes the definition of a file record in the eTrust AC or native OS database.
chres	eTrust, NT, UNIX	Changes existing resource settings in the eTrust AC or native OS database.
editfile	eTrust, NT	Adds a new file record (to the eTrust environment only) or changes an existing file record.
editres	eTrust, NT, UNIX	Adds a new resource record to, or changes an existing resource record in, the eTrust AC or native OS database.
newfile	eTrust	Adds a new file record to the database.
newres	eTrust, NT, UNIX	Adds a new resource record to the eTrust AC or native OS database.
rename	eTrust, NT	Renames an object in the database. eTrust AC does not allow the management of resources that exceed 255 characters. Therefore, the maximum length of an object name is 255 characters. This limitation also applies to the native environment.
rmfile	eTrust	Removes a file resource record from the eTrust AC database.
rmres	eTrust, NT	Removes a resource record from the eTrust AC or Windows database.
showfile	eTrust, NT, UNIX	Lists the properties of file records in the eTrust AC or native OS database.
showres	eTrust, NT, UNIX	Lists the properties of resource records in the eTrust AC or native OS database.
xaudit	NT	Sets auditing criteria and begins logging access events.

Command	Environment	Description
xaudit-	NT	Removes auditing criteria and stops logging access events.

Miscellaneous Commands

Command	Environment	Description
env	eTrust, NT, UNIX, PMD	Sets the security environment selang is operating on.
find	eTrust, NT, UNIX	Lists the classes in the environment. Lists the records in a class.
help	eTrust, NT, UNIX, PMD	Displays the help screen.
history	eTrust, NT, UNIX, PMD	Displays the commands issued previously in the session.
hosts	eTrust, NT, UNIX, PMD	Shows the host to which the selang commands are sent, or set the hosts to which all subsequent commands are sent.
list	eTrust, NT, UNIX	Lists the records in a class. This is the same as the find command.
ruler	eTrust	Sets the properties that display every time a particular command is executed.
search	eTrust, NT, UNIX	Lists the records in a class. This is the same as the find command.
setoptions	eTrust	Sets or displays the global options that control the behavior of the database.
source	eTrust	Executes the commands in a particular file.

Chapter 2

selang Commands in the eTrust Environment

This chapter contains a complete reference to all commands available in the eTrust environment of the selang command shell, arranged alphabetically. When working in the eTrust environment, you use the selang commands to add, delete, modify, and list the users and groups in the local Windows host. See the chapter "The selang Command Language" for general information about the different selang environments, getting help, command syntax, and overall organization of the commands.

allow

Purpose

Specifies whether or not designated users can log into specified eTrust Single Sign-On applications.

The allow command grants or denies users permissions to log into eTrust Single Sign-On applications. The allow command is an alias of the authorize command.

The command can deal with individual users, user groups, simple applications, application groups and all types or eTrust Access Control resources.

- The effect on a extends automatically to cover all the group's members, unless the group rule is overridden by a more specific individual rule.
- The effect on access to an application group extends automatically to cover all the applications included in that application group, unless the application groups rule is overridden by a more specific rule.

When the eTrust Single Sign-On Client software is started, application names appear in the Single Sign-On Tools or Toolbar for all the applications that the user is allowed to access. The user may be allowed as an individually, as a member ofa group, or because the application is accessible by default.

To use the command, you must have sufficient authority. Any of the following conditions is sufficient if true:

- You have the ADMIN attribute.
- The resource record is within the scope of a group in which you have the GROUP-ADMIN attribute.
- You are the owner of the resource record.
- You have the MODIFY access authority for this record in the ADMIN class..

Syntax

```
{allow} {appl | gappl} application-name
        [access( all | execute | none)]
        [gid(group-name...)]
        [id(user-name... | group-name...)]
        [uid({user-name...|*})]
or:
{allow- | al-} {appl | gappl} application-name
        [gid(group-name...)]
        [id(user-name... | group-name...)]
        [uid({user-name...|*})]
```

Arguments

APPL | GAPPL

Specifies whether you are using the allow command on a simple eTrust Single Sign-On application or on an application group.

applpName

The name of the application. When specifying more than one application, enclose the list in parentheses and separate the application names with spacesor commas.

An application can be a simple application or an application group, buta list must consist either entirely of simple applications or entirely of application groups.

eTrust Single-Sign processes each application record independently in accordance with the specified parameters. If an error occurs during processing of an application, eTrust Single Sign-On issues a message and continue to the next application in the list.

When possible, you should avoid using spaces and special characters in resource names. If the resource name does containspecial characters, the resource name has to be quoted and parenthesized. Or, you can make the characters literal by preceding them with a backslash.

access

Specifies whether access is being granted or denied.

Login access is granted if the values ‘execute’ or ‘all’ are used. Login access is denied if the value ‘none’ is used. This ‘none’ argument is useful for overriding permission that derives either from a defaces value or a group membership.

gid

Specifies user groups to be affected by the command.

id Specifies accessors (users or user groups) to be affected by the command.

uid Specifies users to be affected by the command.

authorize

Purpose

The authorize command maintains the lists of users and groups authorized to access a particular resource. Using authorize, you can change a list to:

- Permit access to a resource for specific eTrust AC users or groups.
- Block access to a resource for specific eTrust AC users or groups.
- Change the level of access authority to a resource for specific users or groups.

The authorize- command removes the access authority to a resource by deleting the accessors from the standard access control list. This leaves the default access to determine accessors' ability to access a particular resource.

The authorize and authorize- commands have different forms for various sets of classes. These sets are:

- HOST, GHOST, HOSTNET, and HOSTNP
- TCP
- All remaining classes

The seven types of access control lists are:

- ACL—Standard access control list that contains the user names and group names authorized to access the resource and the level of access granted to each.
- NACL—Negative access control list that contains the user names or group names that are not authorized to access the resource.
- PACL—Program access control list that depends upon the accessing program. Each PACL contains the user names and group names, the level of access, and the name of the program or shell script the user must execute in order to access the particular resource.
- INET-ACL—Internet access control list
- CACL—Conditional access control list
- CALACL—Calendar access control, a resource ACL that depends upon the Unicenter® TNG calendar

- AZNACL—The authorization ACL, an ACL that allows access to a resource based on the resource description

Classes that do not appear in the following table have no access control lists and cannot be controlled by the authorize command.

Class	ACL/ NACL	CALACL	PACL	INET-ACL	CACL	AZNACL
ADMIN	X	X	X			
APPL	X	X				X
AUTHHOST	X	X				X
CONNECT	X	X	X			
CONTAINER	X	X	X			
FILE	X	X	X			
GAPPL	X	X				X
GAUTHHOST	X	X				X
GHOST				X		
GSUDO	X	X				
GTERMINAL	X	X				
HOLIDAY	X	X				
HOST				X		
HOSTNET				X		
HOSTNP				X		
LOGINAPPL	X	X				
MFTERMINAL	X	X	X			
PROCESS	X	X	X			
PROGRAM	X	X				
SECFILE			X			
SUDO	X	X	X			
SURROGATE	X	X	X			
TCP	X	X	X		X	
TERMINAL	X	X	X			
UACC	X	X				
USER_DIR	X					X

Syntax

```
{authorize | auth} class-name record-name
        [uid({user-name...|*})]
        [gid(group-name...)]
        [access(access-value)]
        [via(pgm(program-names...))]
        [nt]
or:
{authorize- | auth-} class-name record-name {uid | gid}(name...) [nt]
or:
{authorize | auth} class-name record-name
        [uid({user-name...|*})]
        [gid(group-name...)]
        [access(access-value) | deniedaccess(access-value)]
        [calendar(calendar-name)]
or:
{authorize- | auth-} class-name record-name {uid | gid}(name...)
        [calendar(calendar-name)]
        [access-]
        [deniedaccess-]
or:
{authorize | auth} class-name station-name
        service(service-name | service-number | service-number-range)
        [access(read|none)]
or:
{authorize- | auth-} class-name station-name
        service(service-name | service-number | service-range)
or:
{authorize | auth} TCP tcp-service-name
        [host(host-name...)]
        [ghost(ghost-name...)]
        [hostnp(hostnp-name...)]
        [hostnet(hostnet-name...)]
        [uid({user-name...|*})]
        [gid(group-name...)]
        [access(read | none | write)]
or:
{authorize- | auth-} TCP tcp-service-name
        [host(host-name...)]
        [ghost(ghost-name...)]
        [hostnp(hostnp-name...)]
        [hostnet(hostnet-name...)]
        [uid({user-name...|*})]
        [gid(group-name...)]
or:
{authorize | auth} WAC-class-name resource-name
        [user_attr(user-attribute)]
        [attr_va(attribute-val)]
        {user_dir(user-directory)}
        {access(WAC-access)}
        {response_yes(granted-response)}
        {response_no(denied-response)}
```

Arguments

className

The name of the class to which *resourceName* belongs.

Note: *ClassName* can be one of the following Windows resources:

- FILE
- PRINTER

- SHARE
- DISK
- COM
- REGKEY

resourceName

The name of the resource record whose access control list you are modifying. Specify only one resource record.

stationName

The record name within the indicated class:

- HOST- Name of single station.
- GHOST- Name of a group of hosts as defined in the database by the GHOST command.
- HOSTNET - Name of a group of hosts as defined by a set of mask and match values for the IP address.
- HOSTNP - Name of a group of hosts as defined by a name pattern.

For hosts that cannot be resolved, enter the IP address range

access(*authority*)

Specifies the access authority you want the accessors you identify in the uid or gid parameters to have to the resource. If you do not specify the *via* parameter, the access authority is set in the resource's standard access control list. If you do specify the *via* parameter, the access authority is set in the resource's conditional access control list.

authority is the access authority, whose values depend on the class the record belongs to:

- For the ADMIN class, valid values are all, create, delete, join, modify, none, password, and read.
- For the FILE class, valid values are create, delete, execute, none, read, rename, sec, update, utime, and write.
- For the HOLIDAY class, valid values are all, read, and none. A read value permits the user to log in during the specified holiday. If you do not specify an access authority, the default is none.
- For the PROGRAM, SUDO, and GSUDO classes, valid values are all, none, and execute.
- For the TCP class, the valid values are all, none, read, and write. A read value allows access from remote hosts or host groups. A write value permits users or groups to access specific hosts or host groups.
- For the TERMINAL and GTERMINAL classes, valid values are all, none, read, and write. A read value permits the user or group to log in to the terminal. A write value permits the user or group to administer the terminal.

- For all other classes, valid values are all, none, and read. (The value *all* represents the entire group of access values, other than *none*, for a particular class.)

If you omit the access parameter, eTrust AC assigns the implicit access specified in the UACC property of the record that represents the resource class in the UACC class.

deniedaccess(*accessvalue*)

Specifies the negative access authority that you want accessors, who you identify in the uid or gid parameters, to have to the resource.

The denied *accessvalue* can be: all, create, delete, join, modify, none, password, or read.

Note: You can only use *accessValue* with the authorize command, not with authorize-.

ghost(*ghostName*)

Specifies the eTrust AC host group whose access authority to the resource you are setting. For more information, see GHOST class in the chapter “eTrust Environment Classes and Properties” in this guide.

ghostName is the name of one or more eTrust AC host groups. When entering more than one host group, separate the names with a space or a comma.

gid(*groupName*)

Specifies the eTrust AC group or groups whose access authority to the resource you are setting.

groupname is the name of one or more eTrust AC groups. When entering more than one group, separate the names with a space or a comma.

host(*hostName*)

Specifies the eTrust AC host whose access authority to the resource you are setting. For more information, see HOST class in the chapter “eTrust Environment Classes and Properties” in this Guide.

hostName is the name of one or more eTrust AC hosts. When entering more than one host, separate the names with a space or a comma.

hostnet(*hostnetName*)

Specifies the eTrust AC hostnet object whose access authority to the resource you are setting. For more information, see HOSTNET class in the chapter “eTrust Environment Classes and Properties” in this guide.

hostnetName is the name of one or more eTrust AC hostnet objects. When entering more than one hostnet object, separate the names with a space or a comma.

hostnp(*hostnpName*)
Specifies the eTrust AC hostnp object whose access authority to the resource you are setting. For more information, see HOSTNP class in the chapter "eTrust Environment Classes and Properties" in this guide.

hostnpName is the name of one or more eTrust AC hostnp objects. When entering more than one hostnp object, separate the names with a space or a comma.

nt
Adds values to the system ACLs in Windows. This parameter is only valid for the FILE class.

service(*serviceName*|*serviceNumber*|*serviceNumberRange*)
Specifies the services the local host provides to the station(s) specified by *stationName*.

serviceName is the name of the service.

serviceNumber is the number of the service. Must be an unsigned short integer (from 0-65535).

serviceNumberRange is a range of service numbers.

tcp(*tcpServiceName*)
Specifies the eTrust AC TCP object whose access authority you are setting. For more information, see TCP Class in the chapter "eTrust Environment Classes and Properties" in this guide.

tcpServiceName is the name of the TCP service record.

uid(*username*)
Specifies the eTrust AC users whose access authority to the resource you are setting.

username is the user name of one or more eTrust AC users. When specifying more than one user, separate the user names with a space or a comma. To specify all users who are defined to eTrust AC, enter an asterisk (*) for *userName*.

via pgm(*pgmName*)
Sets a conditional access rule. The specified access applies only when the resource is accessed from the indicated program or shell script. A shell script must have #!\bin\sh as its first line. If the value *pgmName* specifies a program or shell script not defined in the PROGRAM class, eTrust AC automatically creates a PROGRAM record to protect it.

Generic PACL is an extension to PACL. By placing a wildcard character inside the program name in the PACL, a program that matches the mask created by the wildcard character can access a file protected by the PACL. If a program matches several masks, the longest mask takes precedence.

Notes

- eTrust AC uses all the relevant lists when it checks a user's authority to access a resource. For more information about the lists, see the *Administrator Guide*.
- You can maintain any single list with a single authorize command. Changing more than one list requires you to issue authorize again.
- You cannot define multiple access rights for multiple users and groups with one authorization rule. You must separate the rules.

Examples

User *admin* with the ADMIN attribute wants to allow user Joe execute access to the sensitive file d:\projects\projectA\secrets.

Known	Command
The user *admin* has the ADMIN attribute. The user Joe is defined to eTrust AC. The record *\projects\projectA\secrets* in the FILE class represents the file d:\projects\projectA\secrets.	authorize FILE d:\projects\projectA\secrets uid(Joe) access(execute)

The user "*admin*" wants to remove the read access authority to the file d:\products\new from all the users in the RESEARCH group.

Known	Command
user *admin* has the ADMIN attribute The group RESEARCH and the file d:\products\new are defined in the Windows database.	authorize– FILE d:\products\new gid(RESEARCH)

The user "*admin*" wants to remove user Joe's execute authority to the sensitive file d:\projects\projectA\secrets.

Known	Command
user *admin* has the ADMIN attribute The user Joe and the file d:\projects\projectA\secrets are defined in the Windows database.	authorize– FILE d:\projects\projectA\secrets uid(Joe)

chappl | editappl | newappl

Purpose

The newappl command defines a new eTrust Single Sign-On application. The chappl command changes the definition of an eTrust Single Sign-On application. The editappl command does the work of the chappl commanf, except that if the application does not exist, editappl creates the application.

Syntax

```
{chappl   | ca} application-name | (application-names...)
or
{editappl | ea} application-name | (application-names...)
   [audit(none | all | success | failure )]
   [caption(caption-name) | caption-]
   [comment('installation defined data') | comment-]
   [container | container-]
   [defaccess( all | execute | none )]
   [disable| disable-]
   [gacc(access-value)]
   [hidden | hidden-]
   [host(host-name) | host-]
   [iconfile(iconfile-name) | iconfile-]
   [iconid(iconid-number) | iconid-]
   [item(application-name ...) | item-(application-name ...)]
   [login_type( none | otp | pwd | ticket )]
   [master(application-name) | master-]
   [mon_file(monitor-file-name)]
   [notify(user-name) | notify-]
   [owner(user-name or group-name)]
   [postcmd(command-name | ; command-names...) | postcmd-]
   [precmd(command-name | ; command-names...) | precmd-]
   [ptrecord(quoted-string)]
   [pwd_autogen | pwd_autogen-]
   [pwd_sync | pwd_sync-]
   [pwpolicy(policy-name) | pwpolicy-]
   [restrictions(days( day-data ) time(hhmm:hhmm | anytime) ) | restrictions-]
   day-data: {[mon] [tue] [wed] [thu] [fri] [sat] [sun]} | anyday | weekdays
   [script(script-name) | script-]
   [sensitive | sensitive-]
   [tktkey(ticket-key)]
   [tktrecord(ticket-record)]
   [uacc(access-value)]
   [warning | warning-]
   [cmdline(command line) | cmdline-]
   [pgmdir(program directory) | pgmdir-]
```

Arguments

applName

Specifies one or more application. When listing more than one application, enclose the list of application in parentheses and separate them with spaces or commas.

eTrust Single Sign-On process each application record independently in accordance with the specified parameters. If an error occurs during the processing of an application, eTrust Single Sign-On issues a message and continues to the next application in the list.

audit

Specifies which access events are logged. To use the audit parameter, you must have the AUDITOR attribute.

- ALL - eTrust Single Sign-On logs both authorized an unauthorized access attempts.
- FAILURE - eTrust Single Sign-On logs unauthorized access attempts. This is the default.
- NONE - eTrust Single Sign-On does not write any records in the log file.
- SUCCESS - eTrust Single Sign-On logs authorized access.

caption

Specifies the caption that will appear under the application's icon on the eTrust Single Sign-On user's desktop. Default is the name you supply for applName. The value can be a string up to 47 characters in length. If the string contains any blanks or special characters enclose it in single quotes, or precede each character with a backslash.

caption-

Cancels the user-specified caption, returning the default caption (the name you supplied as applName)

comment

Adds a comments string to the application record, or replaces its comment with a new one. This is a alphanumeric string of up to 255 characters. If the string contains blanks, enclose it in single quotation marks.

comment-

Deletes the comment string from the application record.

container

Specifies that the application is a container application. Instead of performing a script when selected by the eTrust Single Sign-On user, a container application displays a new submenu, containing all the contained application of the selected application.

container-

Specifies that the application is not a container.

defaccess

Specifies the default access authority for this application. The default access authority is granted when no access rule for the application or application group includes the user or user group.

If the argument is either 'execute' or 'all', users not covered by the access rules are permitted to run the application. If the argument is 'none', then users not covered by the access rules are forbidden to run the application.

disable

Prevents the application from executing.

disable-

Cancels the “disable” property and thus allows te application to execute.

hidden

Specifies that the application is not to appear in the eTrust Single Sign-On users application list even if access is granted. The attribute is useful mainly for master applications – applications that supply passwords to other applications.

hidden-

Specifies that the application is to appear in the application list of eTrust Single Sign-On users who are authorized to use it.

host

A value passed to the script and intended to specifiy where the application resides. This is a string value and is normally the name of the host. No check of this value is performed. The name will be available to the script as the $_HOST variable.

host-

Cancels the effect of the host parameter, so that the script receives no value for the $_HOST variable.

iconfile

Specifies the file containing the icon to represent the applications in the eTrust Single Sign-On user’s application list. The file must be available on the client workstation when the eTrust Single Sign-On client software is started. This is a string value and can be a .bmp, .dll, .exe or .ico file.

iconfile-

Cancels the effect of the iconfile parameter. The application will be represented by the default icon on each end user’s workstation.

iconid

Specifies the ID of the icon for the application, if the icon file contains more than one icon. This is a numeric value.

item

Adds one or more applications to a container application. The added application may be an executable application, or it may be a container application itself.

This parameter is meanful only for a container application record being changed by chappl or by editappl

The value is string containing either one or multiple application names. Each application must already exist in the database. If you list more than on, separate them with commas or spaces and enclose the list in parenteses.

item-

Removes an application from a container application. This parameter is meaningful only if the record being changed by chappl or editappl describes a container application.

login_type

Specifies the type of login for accessing the application. This value must contain:

- NONE – Login uses no password.
- OTP – Login uses One Time Password.

- PWD – Login uses a plain password.
- TICKET – Login uses tickets generated by the Policy Server.

master

Specifies the application's master application. When an application requests a password, the password is fetched from the master application. Any change to the application password will be made on the master application.

master-

Cancels the effect of the master application.

notify

Instructs eTrust Single Sign-On to send notification messages whenever the application is successfully accessed. The notification messages are sent to the users identified by *mailAddress*.

Notification takes place only when the Log Routing System is active. The notification messages are sent either to the screen or to the mail box of the users, depending on the setup of the Log Routing System.

The user who is to receive notify messages should log in frequently to respond to the unauthorized access attempts described in each message.

notify-

Specifies that no one is notifies when eTrust Single Sign-On grants access to the application. Only use this parameter with the chappl or editappl command.

owner

Assigns an eTrust Single Sign-On user or group as the owner of the application record. The owner is always permitted to update and delete the application record. The owner has unrestricted access to the application, provided the owner's security level, security level, and security category authorities are sufficient to allow access to the application.

The values used are either user name or user group name. A record can only be edited by the group's administrator. If the group's name is identical to a username, then the username will be the owner.

postcmd

Specifies one or more commands to be executed by the eTrust Single Sign-On Client after the application's script.

string

One or more commands in eTrust Single Sign-On's scripting language.

- If the string contains any blanks, enclose it in single quotes. For example – `('sso msgbox -msg "Hello World!"')`
- If it contains more than one command, use the semicolon as a separator and enclose the whole string in single or double quotes inside parentheses. For example –`('sso msgbox -msg "Hello World!";sso msgbox -msg "How are you?"')`
- If it contains single quotes, precede each by a backslash and enclose in double quotes. For example –`('sso msgbox -msg "What\’s new?"’)`

postcmd-

Specifies that *no* particular command is to be executed by the eTrust Single Sign-On Client *after* the application's script.

precmd

Specifies one or more commands to be executed by the eTrust Single Sign-On Client before the application's script. The commands can initialize variables for the script.

string

One or more eTrust Single Sign-On scripting commands. For format considerations, see postcmd (above).

precmd-

Specifies that no particular command is to be executed by the eTrust Single Sign-On Client before the application's script.

pwd_autogen

Activates automatic password generation for the application. When the password to the application expires for an eTrust Single Sign-On user that has automatic password generation enabled, the eTrust Single Sign-On Server automatically generates a new password with no involvement of the user.

pwd_autogen-

Deactivates automatic password generation for the application. Even if the password to the application expires for an eTrust Single Sign-On user that has automatic password generation enabled, the eTrust Single Sign-On Server will not automatically generate a new password.

pwd_sync

Activates password synchronization for the application. When the password to the application is changed for a user that has password synchronization enabled, the change is also made for all other applications that have password synchronization enabled.

pwd_sync-

Deactivates password synchronization for the application. When the password for the application is changed for a user, other applications are not affected even if the user has password synchronization enabled.

pwpolicy

Specifies the password policy for the application. A password policy is a resource that belongs to the PWPOLICY class. It provides the rules for checking a new password's validity.

policyName

The name of an existing password policy in the database.

restrictions

Specifies the days of the week and the hours in the day when the application is accessible to users.

If day and time restrictions are both in effect, then access is permitted only during the specified hours of the specified days.

If you edit a record that already includes day and time restrictions, and you omit the `days` argument or the `time` argument, the corresponding restriction is left unchanged; it is not erased.

If a container has any restrictions (days, time), then its own icon is not displayed, but its applications may be, depending on their own restrictions.

days

Specifies the days on which the application can be accessed by users. The `days` argument takes the following sub-arguments:

`anyday`— Allow users access to the application on any day.

`weekdays` — Allow users access to the application only on weekdays — Monday through Friday.

`Mon, Tue` , etc. — Allow users access to the application only on the specified days. You can specify the days in any order. If more than one day is specified, separate the days with a space or a comma.

time

Specifies the time period during which the application can be accessed by users. The `time` argument takes the following sub-arguments:

`anytime`— Allow users access to the application at any time of the day.

`startTime:endTime` — Allow the user to access the application only during the specified time period. The format of both `startTime` and `endTime` is `hhmm`, where `hh` is the hour in 24-hour notation (00 through 23) and mm is the minutes (00 through 59). Note that 2400 is not a valid time value.

If `endTime` is smaller than `startTime`, the time period is considered to extend across midnight. Otherwise it is considered to take place on a single day.

If the client is in a different time zone from the server, adjust the time values by translating the start and end times for the client to the equivalent local times for the server. For example, if the server is in New York and the client is in Los Angeles, to allow access to the application from 8:00 a.m. to 5:00 p.m. in Los Angeles, specify time`(1100:2000)`.

restrictions-

Cancels the effect of the restrictions parameter.

script

Specifies the eTrust Single Sign-On script containing the login sequence for the application. The file resides on the eTrust Single Sign-On Server and is sent to the eTrust Single Sign-On Client when requested.

filename

The name of the eTrust Single Sign-On script file. The file must reside in the directory specified by the ScriptsPath token in the [ssod] section of the ssod.ini file.

script-

Specifies that the application will be invoked directly (that is, without the use of a script).

sensitive

Specifies that the application is a sensitive application. When the eTrust Single Sign-On user selects the application, re authentication will be required after a pre-determined amount of time, ensuring that no intruder accesses the application from an unattended workstation.

sensitive- Specifies that the application is not a sensitive application. Once the eTrust Single Sign-On Client is authenticated, logging in to the application requires no further authentication.

warning Specifies that, even if an accessor's authority is insufficient to access the application, eTrust Single Sign-On is to allow access to the application and write a warning message in the audit file.

warning- Specifies that if an accessor's authority is insufficient to access the application, eTrust Single Sign-On is to deny the user access to the application rather than writing a warning message.

check

Purpose

This command allows you to determine if a user has access privileges to a particular resource.

Notes:

- This command checks access according to the resource ACL and default access property. However, it does not support PACLs; that is, it does not indicate whether the user can access a resource by means of a specific program. For more information about PACLs, see the chapter "Introduction" in the *Administrator Guide*.
- This command is not available when seos is down.

Authorization

To use the check command you must be an administrator with the ADMIN attribute. A process with the SERVER attribute can also use the command. For more information on the SERVER attribute, see the chapter "Planning Your Implementation" in the *Administrator Guide*.

Syntax

```
check className {resourceName | (resourcenames…)} \
    [uid (userName)] \
    [access (authority)]
```

Arguments

className

The name of the class to which *resourceName* belongs.

resourceName

The name of the resource record.

access(*authority*)

Specifies the access authority that eTrust AC checks for the accessor as identified by the uid parameter. See the *authorize* command for details.

uid(*userName*)

Specifies the name of the eTrust AC user whose authority to access *resourceName* is to be verified. When specifying more than one *userName*, separate the user names with a space or a comma. To specify all users who are defined to eTrust AC, enter an asterisk (*) for *userName*.

Example

To determine whether the user named Administrator has access to the resource in the FILE class, execute the following check command. The output resembles the following:

```
eTrust selang v5.2 - eTrust command line interpreter
Copyright 2003 Computer Associates International, Inc.
eTrust> check FILE c:\temp\testfile.txt uid(Administrator) access(w)
(localhost)
Access to FILE c:\temp\testfile.txt GRANTED
Access to FILE c:\temp\testfile.txt DENIED
Stage: Resource OWNER check
eTrust>
```

checklogin

Purpose

The checklogin command determines user login privileges, whether a password check is needed, and whether a terminal access check is needed.

Note: This command is not available when seos is down.

Authorization

To use the checklogin command you must be an administrator with the ADMIN attribute. A process with the SERVER attribute can also use the command. For more information on the SERVER attribute, see the chapter “Planning Your Implementation” in the *Administrator Guide*.

Syntax

```
checklogin userName  \
[password(userPassword)] \
            [terminal(loginTerminalName)]
```

Arguments

Password(*userPassword*)

The password, if specified, which eTrust AC checks against the operating system password, and against the database, if password checking is enabled.

Terminal(*loginTerminalName*)

When specified, eTrust AC checks this terminal to determine if a user has login privileges from it.

userName

The user name of one or more eTrust AC users. When entering more than one user, separate the user names with a space or a comma. To specify all users who are defined to eTrust AC, enter an asterisk (*) for *userName*.

Examples

- To determine whether user Frank has login privileges from terminal remotehost to the localhost, execute the following checklogin command. The output resembles the following:

  ```
  eTrust> checklogin frank terminal(remotehost)
          (localhost)
  Login by USER frank to host localhost is GRANTED
  ```

- To verify user Frank’s password, execute the following checklogin command. The output resembles the following:

  ```
  eTrust> checklogin frank password(111) (localhost)
  Given password does not match OS password
  eTrust> checklogin frank password(moonshine)
  (localhost)
  WARNING: Access Control password check is disabled
  Login by USER frank to host localhost is GRANTED
  Stage: Resource class global universal access
  ```

- Now, to verify user Frank's password against the one in the database, execute the following commands. The output resembles the following:

```
eTrust> so class+(PASSWORD) (localhost)
Successfully updated Access Control options
eTrust> checklogin frank password(moonshine)
terminal(tack)
(localhost)
Login by USER frank to host localhost is GRANTED
Stage: Resource class global universal access
eTrust>
```

chfile / editfile / newfile

Purpose

The chfile command modifies one or more records in the FILE class, the newfile command creates one or more records in the FILE class, and the editfile command creates or modifies one or more records in the FILE class.

Tip: You can create a database record for a file that does not yet exist. If you do, selang returns the message: INFO: *filename* is not found on the file system

Syntax

```
{chfile   | cf} file-name | (file-names...)
or
{editfile | ef} file-name | (file-names...)
or
{newfile | nf} file-name | {file-names…}
   [audit(none | all | success | failure)]
   [category(category-names...) | category-(category-names...)]
   [comment('installation defined data') | comment-]
   [defaccess(global-access-value)]
   [gen_prop(property-name) [ {gen_flag | gen_op}(flag)] gen_val(property-values
...)]
   [gowner(group-name)]
   [label(seclabel-name) | label-]
   [level(seclevel-num) | level-]
   [notify(notify-address) | notify-]
   [owner(user-name or group-name)]
   [restrictions(days( day-data ) time(hhmm:hhmm | anytime) ) | restrictions-]
   day-data: {[mon] [tue] [wed] [thu] [fri] [sat] [sun]} | anyday | weekdays
   [warning | warning-]
```

Arguments

audit[(all|none|success|failure)]

Specifies which access events are logged. To use the audit parameter in the chfile command, you must have the AUDITOR attribute.

- **all**—eTrust AC logs both authorized accesses and detected unauthorized access attempts.
- **none**—eTrust AC does not write any records in the log file.
- **success**—eTrust AC logs authorized accesses to the resource.
- **failure**—eTrust AC logs detected unauthorized access attempts. This is the default value.

calendar(*calendarName*)

Specifies Unicenter TNG calendar objects, which represent time restrictions in Unicenter TNG. eTrust AC maintains a list of these objects for management purposes only, but doesn't protect them.

calendarName is the name of one or more Unicenter TNG calendar records defined in the CALENDAR class. When assigning more than one calendar, separate the calendar names with a space or a comma.

calendar-(*calendarName*)

Removes one or more Unicenter TNG calendar records from the user record. Use this parameter only with the chusr or editusr command.

category(*categoryName*)

Assigns a security category to the record.

categoryName is the name of one or more security category records defined in the CATEGORY class. When entering more than one name, separate the names with a space or a comma.

category-(*categoryName*)

Deletes one or more security categories from the resource record. The specified security categories are deleted from the resource record, regardless of whether the CATEGORY class is active.

Only use this parameter with the chres or editres command.

comment(*string*)

Adds a comment string to the record. If you previously added a comment string to the record, the new string specified here replaces the existing string.

string is an alphanumeric string of up to 255 characters. If the string contains any blanks, enclose the entire string in single quotation marks.

comment-(*string*)

Deletes the comment string from the resource record. Only use this parameter with the chres or editres command.

defaccess(*accessAuthority*)

Specifies the default access authority for the file. The default access authority is the authority granted to any accessor that requests access to the file, but is not in the access control lists of the file. Users not defined in the database also receive default access authority.

Specify one of the following values for *accessAuthority*: all, chmod, chown, control, create, delete, none, read, rename, sec, update, utime, or write. For more information on access authorities, see the *Administrator Guide*.

fileName

For the command chfile, *filename* is the name of the file record you are modifying. You **must** specify at least one file name.

For the command newfile, *filename* is the name of the file added to class FILE.

If you are adding a record to, or changing a record in, class FILE using a generic file name, use the wildcard expressions permitted in selang. For more information, see the chapter "Utilities." When defining or changing more than one record, enclose the list of file names in parentheses and separate the file names with a space or a comma.

For the command editfile, the name must conform to the rule of the command newfile or chfile, depending on whether the record already exists or not.

gowner(*groupName*)

Assigns an eTrust AC group (*groupName*) as the owner of the record. The group owner of the file record has unrestricted access to the file, provided the group owner's security level, security label, and security category authorities are sufficient to allow access to the file. The group owner of the file may always update and delete the file record. For more information, see the *Administrator Guide*.

label(*labelName*)

Assigns a security label to the record (where *labelName* is the name of a security label record defined in the SECLABEL class). A security label represents an association between a particular security level and zero or more security categories. If the resource record currently contains a security label, the security label specified here replaces the current security label. For a complete discussion on how to implement security label checking, see the *Administrator Guide*.

label-(*labelName*)

Deletes the security label defined in the file record (where *labelName* is the name of a security label record defined in the SECLABEL class). Only use this parameter with the chfile or editfile command.

level(*number*)

Assigns a security level to the resource record. The level must be a positive integer between 1 and 255. If a security level was assigned previously to the resource record, the new value replaces the existing value. See the *Administrator Guide*.

level-(*number*)

Stops eTrust AC from performing security level checking for the resource. Only use this parameter with the chfile or editfile command.

notify(*mailAddress*)

Instructs eTrust AC to send notification messages to the users identified by *mailAddress* whenever the file represented by the resource record is successfully accessed.

Notification takes place only when the Log Routing System is active. The notification messages are sent either to the screen or to the mailbox of the users, depending on the setup of the Log Routing System.

Each time eTrust AC sends a notification message, it writes an audit record in the audit log. For information on filtering and viewing audit records, see the chapter "Utilities" in this guide.

A user who receives notify messages should log in frequently to respond to the unauthorized access attempts described in each message.

mailAddress can be a user name, an email address of a user, or if an alias is specified, the email address of a mail group.

notify-(*mailAddress*)

Specifies that no one is notified when eTrust AC grants access to the file represented by the record. Only use this parameter with the chfile or editfile command.

owner ({*userName*|*groupName*})

Assigns an eTrust AC user (*userName*) or group (*groupName*) as the owner of the file record. The owner of the file record has unrestricted access to the file, provided the owner's security level, security label, and security category authorities are sufficient to allow access to the file. The owner of the file may always update or delete the file record. For more information, see the *Administrator Guide*.

restrictions([days] [time])

Specifies the days of the week and the hours in the day when users may access the file.

If you omit the days argument and specify the time argument, the time restriction applies to any day-of-week restriction already indicated in the record. If you omit time and specify days, the day restriction applies to any time restriction already indicated in the record. If you specify both days and time, the users may access the system only during the specified time period on the specified days.

- [Days] specifies the days on which users may access the file. The days argument takes the following sub-arguments:
  - anyday—Allow users access to the file on any day.
  - weekdays—Allow users access to the resource only on weekdays—Monday through Friday.
  - Mon, Tu**e**, **Wed**, **Thu**, **Fri**, **Sat**, **Sun**—Allow users access to the resource only on the specified days. You can specify the days in any order. If you specify more than one day, separate the days with a space or a comma.
- [Time] specifies the period during which users may access the resource. The time argument takes the following sub-arguments:
  - **anytime**—Allow users access to the resource at any time of the day.
  - **startTime:endTime**—Allow access to the resource only during the specified period. The format of both startTime and endTime is *hhmm*, where *hh* is the hour in 24-hour notation (00 through 23) and *mm* is the minutes (00 through 59). Note that 2400 is not a valid time value. startTime must be less than endTime, and both times must occur on the same day. If the terminal is in a different time zone from the processor, adjust the time values by translating the start and end times for the terminal to the equivalent local times for the processor. For example, if the processor is in New York and the terminal is in Los Angeles, to allow access to the terminal from 8:00 a.m. to 5:00 p.m. in Los Angeles, specify time (1100:2000).

restrictions-([days] [time])

Deletes any restrictions that limit the users' ability to access the file.

warning

Commands eTrust AC to write a warning message in the audit log rather than deny access to the file when an accessor's authority is insufficient to access the file.

warning-

Terminates a previous warning command. eTrust AC denies the user access to the file rather than writing a warning message when an accessor's authority is insufficient to access the file. Only use this parameter with the chfile or editfile command.

Generic File Protection

Generic file protection enables you to apply a particular access rule to all the files that fit a specified file name pattern (regular expression). The generic access rule protects any file resource with a name matching that wildcard pattern. Should a resource match more than one generic access rule, eTrust AC uses the closest of the matches for that resource.

With generic file protection, you do not need to define more than a handful of security rules in order to protect most of the files that need protection in a Windows system.

eTrust AC, however, does *not* accept the following patterns:

- *
- \tmp*
- \etc*

Note: If more than one file name is specified, eTrust AC processes each file record independently in accordance with the specified parameters. If an error occurs while processing a file, eTrust AC issues a message and continues processing with the next file in the list.

See Also

The authorize, rmfile, and showfile commands in this chapter.

Examples

The security administrator, who has the ADMIN attribute, wants to restrict access to the d:\winnt\win.ini file by allowing only read access to all users except members of the Administrators group. There are currently no entries in the ACL of the record.

Known	Command
The security administrator has the ADMIN attribute. The file d:\winnt\win.ini is defined in the database. There are currently no entries in the ACL of the record.	chfile d:\winnt\win.ini defaccess(read) owner(Administrators)

chgrp / editgrp / newgrp

Purpose

The chgrp command changes the definition of an eTrust AC group. If the group is also defined to Windows, the chgrp command can be used to change the group's Windows definition. You can change the definition of more than one group with a single chgrp command.

The editgrp command either adds a new group to the database like the newgrp command or changes the definition of an existing eTrust AC group like the chgrp command.

The newgrp command defines a new group to eTrust AC by adding a record for the new group to the database and, optionally, establishes a relationship between the new group and a specified administrative parent group or member group.

Syntax

```
{chgrp   | cg} group-name | (group-names ...)
or
{editgrp | eg} group-name | (group-names ...)
or
{newgrp | ng} group-name | (group-names…)
   [audit(none | all | success | failure | loginsuccess | loginfail  | trace) |
audit-]
   [comment('installation defined data') | comment- ]
   [expire | expire(mm/dd/yy[yy][@hh:mm]) | expire-]
   [gen_prop(property-name) [ {gen_flag | gen_op}(flag)] gen_val(property-values
...)]
   [gowner(group-name)]
   [grace(number-of-grace-logins) | grace-]
   [homedir(full-path)]
   [inactive(num-inactive-days) | inactive-]
   [interval(maximum-password-change-interval) | interval-]
   [maxlogins(maximum-number-of-logins) | maxlogins-]
   [mem(group-name) | mem+(group-name) | mem-(group-name)]
   [min_life(minimum-password-change-interval) | min_life-]
   [name('full-name')]
   [owner(user-name or group-name)]
   [parent(group-name) | parent-]
   [pmdb(PolicyModel-name) | pmdb-]
   [restrictions(days( day-data ) time(hhmm:hhmm | anytime) ) | restrictions-]
   day-data: {[mon] [tue] [wed] [thu] [fri] [sat] [sun]} | anyday | weekdays
   [resume | resume(mm/dd/yy[yy][@hh:mm]) | resume-]
   [shellprog(full-path)]
   [suspend | suspend(mm/dd/yy[yy][@hh:mm]) | suspend-]
   [nt| nt( nt-group-attributes  )]
   nt-group-attributes :
   [comment('installation defined data')]
```

Note: Several parameters are relevant only when a group functions as a profile group for a user. The following list indicates these parameters.

Arguments

audit(*mode*)

Turns on the trace audit for this command. Specify a *mode*s of: none, all, success, failure, loginsuccess, or loginfail.

audit-

Turns off the trace audit for this command.

comment(*string*)

Adds to the group record a comment string of up to 255 alphanumeric characters. If the string contains any blanks, enclose the entire string in single quotation marks. The string replaces any existing string that you added previously.

comment-

Deletes the comment string, if any, from the group record. Use this parameter only with the chgrp or editgrp command.

expire(*date*)

Sets the date on which the accounts of the group members expire. If you do not specify a date, the user accounts expire immediately, provided the users are not currently logged in. If the users are logged in, the accounts expire when the users log out. This parameter applies only to profile groups.

Specify the expiration date, and optional time, in the following format: *mm/dd/yy [yy][@HH:MM].* Year can be either 2 or 4 digits.

Note: You cannot enable expired user records by specifying the resume parameter with a resume date. Use the expire- parameter to enable expired user records.

expire-

For the newgrp command, defines user accounts that do not have an expiration date. For the chgrp and editgrp commands, removes the expiration date from the user accounts. This parameter applies only to profile groups.

fullname(*fullname*)

Specifies the full name of the group. Enter an alphanumeric string of up to 47 characters. If the string contains any blanks, enclose the string in single quotation marks.

gowner(*groupName*)

Assigns an eTrust AC user or group as the owner of the group record. When you specify more than one group name, enclose the names in parentheses and separate the group names with a space or a comma. If you add a group to the database and omit this parameter, you are the owner of the group record.

grace(*numberOfGraceLogins*)
Sets the maximum number of logins that are permitted before the users are suspended. The number of grace logins must be between 0 and 255. After the number of grace logins is reached, the users are denied access to the system and must contact the system administrator to select a new password. If grace is set to zero, the users cannot log in. This parameter applies only to profile groups.

grace-
Deletes the grace login setting for the group. Use this parameter only with the chgrp or editgrp command. This parameter applies only to profile groups.

groupName
Specifies the name of the group whose properties you are adding, changing, or editing. For the command newgrp, each group name must be unique and must not currently exist in the database. However, a group and a user can share the same name.

history
Specifies the number of stored passwords. You can eliminate the history file with history-.

HomeDir(*fullPath*)
Specifies the full path of the users' home directories. If the homedir you specify ends with a slash, *userName* is concatenated to the specified path.

inactive(*numInactiveDays*)
Specifies the number of days that must pass before the system changes users to inactive status. When the number of days is reached, users cannot log in. This parameter applies only to profile groups.

Enter a positive integer or zero. If inactive is set to zero, the effect is the same as using the inactive- parameter.

Note: In the user record, inactive users are not marked. To identify inactive users, you must compare the Last Accessed Time value with the Inactive Days value.

inactive-
Changes the users' status from inactive to active. Use this parameter only with the chgrp or editgrp command. This parameter applies only to profile groups.

interval(*maximumPasswordChangeInterval*)
Sets the number of days that must pass after the password was set or changed before the system prompts the user for a new password. Enter a positive integer or zero. An interval of zero disables password interval checking for the group so that the password does not expire. The default set by the setoptions command is not used. Set an interval of zero only for users with low security requirements.

When the specified number of days is reached, eTrust AC informs the user that the current password has expired. The user can immediately renew the password or continue using the old password until the number of grace logins is reached. After the number of grace logins is reached, the user is denied access to the system and must contact the system administrator to select a new password. This parameter applies only to profile groups.

interval-

Cancels the password interval setting for the group. If canceled, any value in the user record is used. Otherwise, the default set by the setoptions command is used. Enter this parameter only with the chgrp or editgrp command. This parameter applies only to profile groups.

maxlogins(*maximumNumberOfLogins*)

Sets the maximum number of terminals users can log in to at the same time. A value of 0 (zero) means that users can log in from any number of terminals concurrently. If this parameter is not specified, any value in the user record is used. Otherwise, the global maximum logins setting is used. This parameter applies only to profile groups.

Note: If maxlogins is set to 1, you cannot run selang. You must shut down eTrust AC, change the maxlogins setting to greater than one, and start eTrust AC again.

maxlogins-

Deletes the group’s maximum login setting. If this parameter is not specified, any value in the user record is used. Otherwise, the global maximum logins setting is used. Use this parameter only with the chgrp or editgrp command. This parameter applies only to profile groups.

mem(*GroupName*) | mem+(*GroupName*)

Adds members groups (or child groups) to the group in eTrust AC. The member groups (*GroupName*) must already be defined in eTrust AC. If you are adding more than one member group, separate the group names with a comma. If a group name contains a space, enclose it in quotation marks.

mem-(*GroupName*)

Removes member groups from this group. The member groups (*GroupName*) must already be defined in eTrust AC. If you are removing more than one member group, separate the group names with a comma. If a group name contains a space, enclose it in quotation marks.

min_life(*minimumPasswordChangeInterval*)

The minimum number of days that must pass before users are allowed to change the password again. This parameter applies only to profile groups.

min_life-

Deletes the min_life setting of a group. If this parameter is not specified and the min_life parameter is set in a user record, the value in the user record is used. Otherwise, the global min_life setting is used. Use this parameter only with the chgrp or editgrp command. This parameter applies only to profile groups.

owner(*Name*)

Assigns an eTrust AC user or group as the owner of the group record. If you are adding a group to the database and you omit this parameter, you are the owner. See the *Administrator Guide* for more information.

parent(*groupName*)

Assigns an existing eTrust AC group as the parent group of the group record. See the *Administrator Guide* for more information on parent/child relationships.

parent-

Deletes the link between a group and its parent group. Use this parameter only with the chgrp or editgrp command.

password

Assigns a password to this group.

rules

Specifies rules for the password:

- **alpha(*minimumAlphaCharacters*)**—Minimum Number of Alphabetic Characters.
- **alphanum(*minimumAlphanumericCharacters*)**—Minimum Number of Characters.
- **min_len(*minimumPasswordLength*)**—Minimum Password Length.
- **max_len(*maximumPasswordLength*)**—Maximum Password Length.
- **lowercase(*minimumLowercaseCharacters*)**—Minimum Number of Lowercase of Characters.
- **max_rep(*maximumRepetitiveCharacters*)**—Maximum Number of Repeated Characters.
- **namechk | namechk-** —Check Password Against Name.
- **numeric(*minimumNumericCharacters*)**—Minimum Number of Numeric Characters.
- **oldpwchk | oldpwchk-** —Check Password Against Old Password.
- **special(*minimumSpecialCharacters*)**—Minimum Number of Special Characters.
- **uppercase(*minimumUppercaseCharacters*)**—Minimum Number of Uppercase of Characters.

password-

Deletes the need for a password for this group.

pmdb(*PolicyModelName*)

Specifies that when a user in the group changes a password with the utility sepass, the new password is propagated to the specified Policy Model. Enter the fully qualified name of the PMDB.

The password is not sent to the Policy Model defined in the parent_pmd or passwd_pmd token in the [seos] section of seos.ini. This parameter applies only to profile groups.

pmdb-

Removes the pmdb attribute from the group record. Use this parameter only with the chgrp or editgrp command. This parameter applies only to profile groups.

restrictions(days(*dayData*) time(*timeData*))

Specifies when members of the group are allowed to log in to the system. eTrust AC does not force a user off the system if the login period expires while the user is logged in. Also, the login restrictions do not apply to batch jobs; a user can run a background process at any time. This parameter applies only to profile groups.

If you omit the days argument and specify the time argument, the time restriction applies to any day-of-week restriction already indicated in the group record. If you omit time and specify days, the day restriction applies to any time restriction already indicated in the group record. If you specify both days and time, the members of the group are allowed to log in to the system only during the specified time period on the specified days.

- **days(*dayData*)**—Specifies the days on which users can log in to the system. The days argument takes the following sub-arguments:
  - **anyday**—Lets users log in on any day.
  - **weekdays**—Lets users log in only on weekdays—Monday through Friday.
  - **mon tue wed thu fri sat sun**—Lets users log in only on the specified days. You can specify the days in any order. If more than one day is specified, separate the days with a space or a comma.
- **time(*timeData*)**—Specifies the period during which users can log in to the system. The time argument takes the following sub-arguments:
  - **anytime—**Lets users log in at any time of the day.
  - ***startTime*:*endTime***—Lets users log in only during the specified period. The format of both *startTime* and *endTime* is *hhmm*, where *hh* is the hour in 24-hour notation (00 through 23) and *mm* is the minutes (00 through 59). Note that 2400 is not a valid time value. If *endTime* is a smaller number than *endTime*, the period is considered to extend across midnight. Otherwise, it is considered to take place on a single day.

  If the terminal is in a different time zone from the processor, adjust the time values by translating the start and end times for the terminal to the equivalent local times for the processor. For example, if the processor is in New York and the terminal is in Los Angeles, to allow access to the terminal from 8:00 a.m. to 5:00 p.m. in Los Angeles, specify time(1100:2000).

restrictions-

Deletes any restrictions that limit the users' ability to log in to the system from the group record. If this parameter is not specified and the restrictions parameter is set in a user record, the value in the user record is used. Use this parameter only with the chgrp or editgrp command. This parameter applies only to profile groups.

resume(*date*)

Enables user records that were disabled by specifying the suspend parameter. Enter a date, and optional time, in the following format: *mm/dd/yy[@HH:MM]*.

If you specify both the suspend parameter and the resume parameter, the resume date must fall after the suspend date. If you omit *date*, the user records are resumed immediately upon execution of the chgrp command. See the *Administrator Guide* for more information. This parameter applies only to profile groups.

resume-

Erases the resume date, and time if used, from the group record. Consequently, the status of the users is changed from active (enabled) to suspended. Use this parameter only with the chgrp or editgrp command. This parameter applies only to profile groups.

shellprog(*fullPath*)

Specifies the full path of the initial program or shell that is executed after the user invokes the login or su command. *FullPath* is a character string.

supgroup(*Group'sSuperiorGroup*)

Specifies a supergroup (or parent group).

suspend(*date*)

Disables user records, but leaves them defined in the database. Enter a date, and optional time, in the following format: *mm/dd/yy[@HH:MM]*.

A user cannot use a suspended user account to log in to the system. If *date* is specified, the user records are suspended on the specified date. If *date* is omitted, the user records are suspended immediately upon execution of the chgrp command. This parameter applies only to profile groups.

suspend-

Erases the suspend date from the user records, changing the status of the users from disabled to active (enabled). Use this parameter only with the chgrp or editgrp command. This parameter applies only to profile groups.

unix(*groupidNumber*)

Sets group attributes on UNIX.

- For the command chgrp, this parameter changes the group's attributes in the local UNIX system.
- For the command editgrp, this parameter adds a group or changes the group's attributes, depending on whether the record already exists or not. This parameter applies only to profile groups.
- For the command newgrp, this parameter adds a group to the local UNIX system and to the database. To add the group to UNIX using the default attributes, specify the unix parameter without any arguments. To set a UNIX attribute explicitly, specify the relevant argument.

The *groupidNumber* is a decimal number. You cannot specify a group ID of zero. If you omit the number, eTrust AC finds the largest current group ID and sets the ID of the group to this number plus one. eTrust AC creates group ID numbers in the same way when adding or modifying more than one group at a time. The token AllowedGidRange in the seos.ini file may define certain unavailable numbers.

For alternatives to this parameter, see the *Administrator Guide.*

userlist*(userName)*

Assigns members to the group. *UserName* is the user name of one or more UNIX users. When assigning more than one user, separate the user names with a comma or a space. For the chgrp and editgrp commands, the member list specified here replaces any member list that is currently defined for the group.

See Also

The rmgrp, showgrp, and join commands in this chapter.

Examples

- The admin user Sally wants to remove the home directory and the shell program specifications for the group profile stored in the record of the group NewEmployee.

Known	Command
The user Sally is the owner of the NewEmployee group record.	editgrp NewEmployee \\ homedir() \\ shellprog()

To remove any record property, if the property is defined by a string, type the property with either the “-” sign or empty parenthesis “()”.

- The user Bob wants to change the parent group and owning group for the group Sales from ACCOUNTS to PAYROLL.

Known	Command
The user Bob has the ADMIN attribute.	chgrp Sales \\ parent(PAYROLL)\\ owner(PAYROLL)

- The user admin1 wants to change the parent group of group projectB from divisionA to divisionB and assign the group RESEARCH as the new owner.

Known	Command
The user admin1 has the ADMIN attribute.	chgrp projectB \ parent(divisionB) \ owner(RESEARCH)

- The user Admin1 wants to add the group ProjectA as a child group of the group RESEARCH. The user Admin1 is to be the owner of the ProjectA group.

Known	Command	Defaults
The user Admin1 has the ADMIN attribute.	newgrp ProjectA parent(RESEARCH)	owner(Admin1)

chres / editres / newres

Purpose

The newres command defines a new resource to an eTrust AC class. The chres command modifies one or more resource records that belong to an eTrust AC class. The editres command either defines a new resource or modifies an existing resource.

In eTrust AC for Windows, the following classes can be administered using the chres, editres, and newres command: ADMIN, AGENT, AGENT_TYPE, APPL, AUTHHOST, CALENDAR, CATEGORY, CONNECT, CONTAINER, DOMAIN, FILE, GAPPL, GAUTHHOST, GFILE, GHOST, GSUDO, GTERMINAL, HOLIDAY, HOST, HOSTNET, HOSTNP, MFTERMINAL, OU, PROCESS, PROGRAM, PWPOLICY, REGKEY, RESOURCE-DESC, RESPONSE-TAB, SECFILE, SECLABEL, SPECIALPGM, SUDO, SURROGATE, TCP, TERMINAL, UACC, USER-ATTR, USER-DIR and any user defined class.

Note: You cannot use the chres or editres command to modify users or groups.

The following table lists the newres and chres parameters that apply for each class.

Class	**Properties**											
	audit	**calendar**	**category**	**comment**	**defaccess**	**label**	**level**	**notify**	**owner**	**restrictions[-]**	**warning**	***other***
ADMIN	X	X	X	X	X	X	X	X	X	X	X	
AGENT				X					X			
AGENT-TYPE				X					X			
APPL	X	X		X				X	X		X	DAYTIME, HOST
AUTHHOST	X	X	X	X		X	X		X		X	
CALENDAR				X					X			
CATEGORY				X					X			
CONNECT	X	X	X	X	X	X	X	X	X	X	X	
CONTAINER	X	X		X					X		X	MEM
DOMAIN	X	X	X			X	X	X	X		X	MEM
FILE	X	X	X	X	X	X	X	X	X	X	X	
GAPPL	X			X					X			MEM
GAUTHHOST	X			X					X			MEM
GFILE	X	X		X				X	X		X	DAYTIME, MEM
GHOST	X	X		X					X	X	X	MEM
GSUDO		X		X	X				X			MEM
GTERMINAL		X		X	X				X	X		MEM
HOLIDAY	X		X	X	X	X	X	X	X	X	X	DATES
HOST	X	X		X					X	X	X	
HOSTNET	X	X		X					X		X	MASK, MATCH
HOSTNP	X	X		X					X	X	X	
MFTERMINAL	X	X	X	X		X	X	X	X		X	DAYTIME
PROCESS	X	X	X	X	X	X	X	X	X	X	X	
PROGRAM	X	X	X	X	X	X	X	X	X	X	X	TRUST[-]

Class	Properties										
	audit	calendar	category	comment	defaccess	label	level	notify	owner	restrictions[-]	warning	*other*
PWPOLICY				X					X			
REGKEY	X	X		X				X	X		X	DAYTIME
RESOURCE-DESC				X					X			
RESPONSE-TAB				X					X			
SECFILE				X					X			TRUST[-]
SECLABEL			X	X			X		X			
SEOS		X	X	X		X	X					
SPECIALPGM				X					X			
SUDO	X	X	X	X	X	X	X	X	X	X	X	TARGUID PASSWORD
SURROGATE	X	X	X	X	X	X	X	X	X	X	X	
TCP	X		X	X	X	X	X	X	X	X	X	
TERMINAL	X	X	X	X	X	X	X	X	X	X	X	
UACC	X		X	X	X				X			
USER-ATTR									X		X	
USER-DIR	X			X					X			

Syntax

```
{chres   | cr} class-name resource-name | (resource-names...)
or
{editres | er} class-name resource-name | (resource-names...)
or
{newres | nr} class-name resource-name | (resource-names…)
[audit(none | all | success | failure)]
[caption(caption-name) | caption-]
[category(category-names...) | category-(category-names...)]
[comment('installation defined data') | comment-]
[container | container-]
[dates(mm/dd/[yy[yy]][@hh:mm][-mm/dd/[yy[yy]][@hh:mm]]...) |
dates-(mm/dd/[yy[yy]][@hh:mm][-mm/dd/[yy[yy]][@hh:mm]]...)]
[defaccess(global-access-value)]
[disable| disable-]
[flags(flags)]
flags:{[Ctime] [Mtime] [Mode] [Size] [Device] [Inode] [Crc] [Owner] [Group]} |
All | None
```

```
[gacc(access-value)]
[gen_prop(property-name) [ {gen_flag | gen_op}(flag)] gen_val(property-values
...)]
[gowner(group-name)]
[hidden | hidden-]
[host(host-name) | host-]
[iconfile(iconfile-name) | iconfile-]
[iconid(iconid-number)]
[item(application-name ...) | item-(application-name ...)]
[label(seclabel-name) | label-]
[level(seclevel-num) | level-]
[login_type( none | otp | pwd | ticket )]
[mask(inet-address) match(inet-address)]
[master(application-name) | master-]
[mem+(member-names ...) | mem-(member-names...) ]
[notify(notify-address) | notify-]
[owner(user-name or group-name)]
[password | password-]
[postcmd(command-name | ; command-names...) | postcmd-]
[precmd(command-name | ; command-names...) | precmd-]
[pwd_autogen | pwd_autogen-]
[pwd_sync | pwd_sync-]
[pwpolicy(policy-name)]
[restrictions(days( day-data ) time(hhmm:hhmm | anytime) ) | restrictions-]
day-data: {[mon] [tue] [wed] [thu] [fri] [sat] [sun]} | anyday | weekdays
[script(script-name) | script-]
[sensitive | sensitive-]
[targuid(user-name)]
[trust | trust-]
[uacc(access-value)]
[warning | warning-]
[agent_type]
[of_resource]
[resaccess]
[resp_list | resp_list+ | resp_list-]
[db_field]
[field_id]
[predef | predef- | predef+]
[user_dir]
[addcategory]
[auth_method]
[base_path]
[cont_format]
[properties]
[user_format]
```

Arguments

audit

Indicates which access events are logged. Specify one of the following attributes:

- **all**—eTrust AC logs both authorized and unauthorized access attempts.
- **failure**—eTrust AC logs unauthorized access attempts. This is the default value.
- **none**—eTrust AC does not write any records in the log file.
- **success**—eTrust AC logs authorized access attempts.

calendar(*calendarName*) Specifies Unicenter TNG Calendar objects, which represent time restrictions in Unicenter TNG. eTrust AC maintains a list of these objects for management purposes only, but doesn't protect them. When assigning more than one calendar, separate the calendar names with a space or a comma.

calendar-(*calendarName*) Deletes one or more Unicenter TNG calendar records from the resource record. Use this parameter with the chres or editres command only.

category(*categoryName*) Assigns to the resource one or more security category records that are defined in the CATEGORY class. When assigning more than one security category, separate the security category names with a space or a comma.

If you specify the category parameter when the CATEGORY class is not active, eTrust AC updates the resource definition in the database; however, the updated category assignment has no effect until the CATEGORY class is activated again. For more information about security category checking, see the *Administrator Guide*.

category-(*categoryName*)

Deletes one or more security categories from the resource record. When removing more than one security category, separate the security category names with a space or a comma.

The specified security categories are deleted from the resource record, regardless of whether the CATEGORY class is active. Use this parameter only with the chres or editres command.

className The name of the class to which the resource belongs. To list the resource classes defined to eTrust AC, use the find command. See the find command in this chapter.

comment(*string*) Adds an alphanumeric string of up to 255 characters to the resource record. If the string contains any blanks, enclose the entire string in single quotation marks. The string replaces any existing string defined previously.

For the SUDO class, this string has a special meaning. For details, see Defining SUDO Records in this section.

comment-(*string*) Deletes the comment string from the resource record. Use this parameter only with the chres or editres command.

container(*containerName*)

Represents CONTAINER objects, a generic grouping class. See CONTAINER class in the chapter "eTrust Environment Classes and Properties" for details.

containerName is the name of one or more CONTAINER records defined in the CONTAINER class. When assigning more than one CONTAINER, separate the names with a space or a comma.

container-(*containerName*)

Deletes one or more CONTAINER records from the resource record. Use this parameter with the chres or editres command only.

dates(*time-period*)

Specifies one or more periods when users cannot log in, such as holidays. If more than one time period is specified, separate the periods with a space. Use the following format:

mm/dd[/yy[yy]][@hh:mm][-mm/dd] \ [/yy[yy]][@hh:mm]

If you do not specify a year, (or you specify a year before 1990), it means the period or holiday is annual. You can specify the year with two digits or four digits, for example: 98 or 1998.

If you do not specify a start time then the start of the day (midnight) is used; if you do not specify an end time then the end of the day (midnight) is used. The format of the hours and the minutes is *hh:mm*, where *hh* is the hour in 24-hour notation (00 through 23) and *mm* is the minutes (00 through 59).

If you do not specify an interval of time (for example, 12/25@14:00-12/25@17:00), but only a day and a month (12/25), then the holiday lasts for one whole day.

If you are issuing the command in a different time zone from where the holiday occurs, translate the period to your local time. For example, if you are in New York and Los Angeles has a half-day holiday, you must enter 09/14/98@18:00-09/14/98@20:00. This prevents the users from logging in from 3:00 p.m. to 5:00 p.m. in Los Angeles.

defaccess(*accessAuthority*)

Specifies the default access authority for the resource. The default access authority is the authority granted to any accessor not in the resource's access control list that requests access to the resource. The default access is also applied to users who are not defined in the database. The access authority values depend on the class the resource belongs to:

- For the ADMIN class, valid values are *all*, *create*, *delete*, *join*, *modify*, *none*, *password*, and *read*.
- For the FILE class, valid values are *all*, *chdir*, *chmod*, *chown*, *control*, *create*, *delete*, *execute*, *none*, *read*, *rename*, *sec*, *update*, *utime*, and *write*.
- For the HOLIDAY class, valid values are *all*, *read*, and *none*. The value *read* permits the user to log in during the specified holiday. If you do not specify an access authority, the default is *none*.
- For the PROGRAM, SUDO, and GSUDO classes, valid values are *all*, *none*, and *execute*.
- For the TCP class, the valid values are *all*, *none*, *read*, and *write*. The value *read* allows access from remote hosts or host groups. The value *write* permits users or groups to access specific hosts or host groups.

- For the TERMINAL and GTERMINAL classes, valid values are *all*, *none*, *read*, and *write*. The value *read* permits the user or group to log in to the terminal. The value *write* permits the user or group to administer the terminal.
- For all other classes, valid values are *all*, *none*, and *read*. (The value *all* represents the entire group of access values, other than *none*, for a particular class.)

If you omit the *access* parameter, eTrust AC assigns the implicit access specified in the UACC property of the record that represents the resource's class in the UACC class.

See the *Administrator Guide* for more information on access authorities.

flags(*flagName*)

Defines how the resource is to be trusted and how to check it for trusted status. Available flags are Ctime, Mtime, Mode, Size, Device, Inode, Crc, and Own/All/None.

gowner(*groupName*)

Assigns an eTrust AC group as the owner of the resource record. The group owner of the resource record has unrestricted access to the resource, provided the group owner's security level, security label, and security category authorities are sufficient to allow access to the resource. The group owner of the resource is always permitted to update and delete the resource record. See the *Administrator Guide* for more information.

label(*labelName*)

Assigns a security label record that is defined in the SECLABEL class.

label-

Deletes the security label from the resource record. Use this parameter only with the chres or editres command.

level(*number*)

Assigns a security level to the resource record. Enter a positive integer between 1 and 255. If a security level was previously assigned to the resource record, the new value replaces the existing value. For a complete discussion on how to implement security level checking, see the *Administrator Guide*.

level-

Stops eTrust AC from performing security level checking for the resource. Use this parameter only with the chres or editres command.

mask|match (*inet-address*)

The *mask* and *match* parameters are applicable only to the HOSTNET class. They are required when adding a record to the class with the newres and editres commands and are optional when using chres.

Use *mask* and *match* together to define which hosts belong to the HOSTNET record. When a bitwise AND is performed on the *mask* and the IP address of a host, and the result equals *match*, then the host is a member of the HOSTNET record.

For example, specifying mask(255.255.255.0) and match(192.16.133.0) includes all hosts with IP addresses of the format 192.16.133. anything.

mem(*resourceName*)

Adds members to a resource group. The member resource must already be defined in eTrust AC and protected by it. If you are adding more than one member, separate the resource names with a comma.

The mem parameter applies only to resource records of the CONTAINER, GFILE, GSUDO, GTERMINAL, or GHOST class.

- The CONTAINER class defines a group of objects from other resource classes.
- The GFILE class contains groups of files that define access based on name pattern.
- The GSUDO class contains resource records that define groups of commands.
- The GTERMINAL class contains resource records that define groups of terminals.
- The GHOST class contains resource records that define groups of hosts.

The mem parameter adds records of several types to the CONTAINER object you are adding or modifying, FILE resource records to the GFILE record you are adding or modifying, SUDO resource records to the GSUDO record you are adding or modifying, TERMINAL resource records to the GTERMINAL resource record you are adding or modifying, or HOST resource records to the GHOST resource record you are adding or modifying.

Note: If you are using the mem parameter for CONTAINER resources, you must also included the of_class parameter.

mem-(*resourceName*)

Removes member resources from a resource group. If you are removing more than one member resource, separate the resource names with a space or a comma. Use this parameter only with the chres or editres command.

notify(*mailAddress*)

Instructs eTrust AC to send notification messages whenever the resource represented by the resource record is accessed. Enter a user name, an email address of a user, or the email address of a mail group if an alias is specified.

Notification takes place only when the Log Routing System is active. The notification messages are sent either to the screen or to the mailbox of the users, depending on the setup of the Log Routing System.

Each time a notification message is sent, an audit record is written in the audit log. For information on filtering and viewing audit records, see the *Administrator Guide*.

The recipient of notify messages should log in frequently to respond to the unauthorized access attempts described in each message.

notify-

Specifies that no one is notified when the resource represented by the resource record is successfully accessed. Use this parameter only with the chres or editres command.

of_class(*className*)

Specifies the resource type for the record you are adding to the CONTAINER class with the mem parameter.

owner(*userName*|*groupName*)

Assigns an eTrust AC user or group as the owner of the resource record. The owner of the resource record has unrestricted access to the resource, provided the owner's security level, security label, and security category authorities are sufficient to allow access to the resource. The owner of the resource is always permitted to update and delete the resource record. For more information, see the *Administrator Guide*.

password

Specifies, for the SUDO class, that the sesudo command will require the original user's password.

password-

Cancels the password parameter, so that the sesudo command will no longer require the original user's password. Use this parameter with the chres or editres command only. If the password parameter was not used previously, then this parameter is unnecessary.

resourceName

The name of the resource record to modify or add. When changing or adding more than one resource, enclose the list of resource names in parentheses and separate the resource names with a space or a comma. At least one resource name must be specified.

eTrust AC processes each resource record independently in accordance with the specified parameters. If an error occurs while processing a resource, eTrust AC issues a message and continues processing with the next resource in the list.

restrictions([days] [time])

Specifies the days of the week and the hours in the day when users may access the file.

If you omit the days argument and specify the time argument, the time restriction applies to any day-of-week restriction already indicated in the record. If you omit time and specify days, the day restriction applies to any time restriction already indicated in the record. If you specify both days and time, the users may access the system only during the specified time period on the specified days.

- [Days] specifies the days on which users may access the file. The days argument takes the following sub-arguments:

  - **anyday**—Allow users access to the file on any day.
  - **weekdays**—Allow users access to the resource only on weekdays—Monday through Friday.
  - **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, **Sun**—Allow users access to the resource only on the specified days. You can specify the days in any order. If you specify more than one day, separate the days with a space or a comma.

- [Time] specifies the period during which users may access the resource. The time argument takes the following sub-arguments:
  - **anytime**—Allow users access to the resource at any time of the day.
  - **startTime:endTime**—Allow access to the resource only during the specified period. The format of both startTime and endTime is *hhmm*, where *hh* is the hour in 24-hour notation (00 through 23) and *mm* is the minutes (00 through 59). Note that 2400 is not a valid time value. startTime must be less than endTime, and both times must occur on the same day. If the terminal is in a different time zone from the processor, adjust the time values by translating the start and end times for the terminal to the equivalent local times for the processor. For example, if the processor is in New York and the terminal is in Los Angeles, to allow access to the terminal from 8:00 a.m. to 5:00 p.m. in Los Angeles, specify time (1100:2000).

restrictions-([days] [time])

Deletes any restrictions that limit the users' ability to access the file.

targuid(*username*)

Specifies the name of the user whose authority will be borrowed by the SUDO class for executing the command. Default is Administrator.

warning

Specifies that, even if an accessor's authority is insufficient to access the resource, eTrust AC is to allow access to the resource. However, eTrust AC writes a warning message in the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

warning-

Deletes warning access. If an accessor's authority is insufficient to access the resource, eTrust AC denies the user access to the resource and does not write a warning message. Only use this parameter with the chres or editres command.

Defining SUDO Records

A record in the SUDO class stores a command script so that users can run the script with borrowed permissions. The ability to borrow permissions is tightly controlled by the SUDO record, as well as by the sesudo command that executes the scripts.

Note: The sesudo command cannot execute interactive processes when the SeOS Task Delegation service runs under a user account other than the SYSTEM account on a machine where Terminal Services are installed.

In a SUDO record, the comment property is used for a special purpose, and often it is known by its alternate name: the data property.

The data property's value is the command script, with the optional addition of one or more script parameter values that are to be prohibited or permitted. The entire data property value must be enclosed in single quotes, and executables should be referenced by their complete path names in order to prevent Trojan horses from taking their place.

This is the format for the data property:

```
data('cmd[;[prohibited-values][;permitted-values]]')
```

Because the lists of prohibited and permitted values are optional, a simple data property value can be the following:

```
newres SUDO NET data(net use)
```

The simple value in the command means that the command sesudo NET will execute the command 'net use'. No particular script parameter values are prohibited; all are permitted.

Wildcards and powerful variables give you flexibility in specifying prohibited and permitted parameters. The wildcards you can use are the standard Windows wildcards.

If you append a list of *prohibited* parameter values to the script:

- Separate the script from the prohibited parameter values with a semicolon, but keep them all inside the single quotes. For example, if you want to prevent the user from using -start but you permit the user to use all other parameters, enter the following command:

  ```
  newres SUDO scriptname data('cmd;-start')
  ```

  where *cmd* represents your script.

  Alternatively, if you do not allow any parameter values, but rather want all parameters defaulted, define the SUDO record as follows:

  ```
  newres SUDO scriptname data('cmd;*')
  ```

- If a script parameter has more than one prohibited value, use the space character as a separator. For example, if you want to prevent the user from using -start and -stop but you permit the user to use all other parameters, enter the following command:

  ```
  newres SUDO scriptname data(‘cmd;-start -stop’)
  ```

- If more than one script parameter has prohibited values, use the pipe character (|) as a separator between sets of prohibited values. For example, if you want to prevent the user from using -start and -stop for the script’s first parameter and from using any existing Windows user name for the second parameter (see the previous list of variables), enter the following command:

  ```
  newres SUDO scriptname data(‘cmd;-start -stop | $u’)
  ```

  If the script has more parameters than you list, then your last set of prohibited parameters applies to all the remaining parameters.

If you append a list of *permitted* parameter values to the script,

- The sesudo utility will enforce two checks: Not only must the parameter values not match any of the corresponding prohibited values; they must also match at least one of the corresponding permitted values.

- Separate the list of *permitted* values from the list of *prohibited* values with a semicolon, but keep them all inside the single quotes. Even if you have no list of prohibited values, you still need the semicolon; otherwise what you intend to permit will be prohibited. For example, if you want to allow only the value NAME as a parameter value for the script, enter the following command:

  ```
  newres SUDO scriptname data(‘cmd;;NAME’)
  ```

- Just as in the other list,

  - If a script parameter has more than one permitted value, use the space character as a separator.

  - If more than one script parameter has permitted values, use the pipe character (|) as a separator between sets of permitted values.

  For example, if you have two parameters, and the first must be numeric but must not be a Windows user name, and the second must be alphabetic but must not be a Windows group name, enter the following command:

  ```
  newres SUDO scriptname data(‘cmd; $u | $g ; $N | $A’)
  ```

  If the script has more parameters than you list, then your last set of permitted parameters applies to all the remaining parameters.

Thus, the overall format for the data property is this: first the script; then the prohibited values, parameter by parameter; then the permitted values, parameter by parameter:

```
data('cmd;
param1_prohib1 param1_prohib2 ... param1_prohibN | \
param2_prohib1 param2_prohib2 ... param2_prohibN | \
 ...
paramN_prohib1 paramN_prohib2 ... paramN_prohibN ; \
param1_permit1 param1_permit2 ... param1_permitN | \
param2_permit1 param2_permit2 ... param2_permitN |
 ...
 paramN_permit1 paramN_permit2 ... paramN_permitN')
```

See Also

The authorize, rmres, and showres commands in this chapter.

Examples

- User Bob, who is the owner of the SHARE record shar22, wants to delete the comment field of the SHARE shar22 and ensure that the maximum number of users that can connect to shar22 at one time is 12.

Known	Command
The user Bob is an eTrust AC user and is the owner of the SHARE record shar22.	chres SHARE shar22 comment– maxusers(12)

- User *admin1,* who has the ADMIN attribute, wants to change the owner and default access for the NTFS file d:\tmp\a.exe. The file d:\tmp\a.exe is defined in the Windows database.

Known	Command
User *admin1* has the ADMIN attribute. The file d:\tmp\a.exe is defined in the Windows database.	editres file d:\tmp\a.exe owner(admin1) defaccess(read)

- User *admin1, who has the* ADMIN attribute, wants to add a new REGVAL resource type called Software\Mineval and give it the registry value of 4. This creates a new value that is defined in the registry key HKEY_LOCAL_MACHINE by default.

Known	Command
User *admin1* has the ADMIN attribute.	newres REGVAL HKEY_LOCAL_MACHINE\ Software\Mineval dword(4)

chusr / editusr / newusr

Purpose

The chusr command changes the properties of a user record. eTrust AC changes the user record immediately upon execution of the chusr command, even if the user is currently logged in to the system. The editusr command can define a new user and change the properties of an existing user. The newusr command defines a new user to eTrust AC and to the Windows database.

Authorization

The level of authority required to execute the chusr and editusr command depends on which parameters you want to specify. The following rules apply:

- If you have the ADMIN attribute, you can specify all parameters except audit.
- To specify the audit parameter, you must have the AUDITOR attribute assigned in your user record.
- When updating an existing record, the owner of the user record can specify all parameters except admin, auditor, server, operator, and pwmanager. To assign a security category to the user record, the security category must appear in the owner's user record. To assign a security label to the user record, the security label must be assigned in the owner's user record. The owner of the user record can assign any security level that is less than or equal to the security level assigned in the owner's user record.
- If the user record is within the scope of a group in which you have the GROUP-ADMIN attribute, you have the same authority as the owner of the record.
- If the user record is within the scope of a group in which you have the GROUP-AUDITOR attribute, you can specify the audit parameter.

- If you have the MODIFY (for chusr) or CREATE (for editusr) authority assigned in the access control list of the USER record in the ADMIN class, you have the same authority as the owner of the user record.

For more information on the scope of administration authority that applies to the chusr and editusr commands, see the *Administrator Guide*.

Syntax

```
{chusr   | cu} user-name | (user-names ...)
or
{editusr | eu} user-name | (user-names ...)
or
{newusr | nu} user-name | {user-names ….}

[admin | admin-]
[audit(none | all | success | failure | loginsuccess | loginfail | trace) |
audit-]
[auditor | auditor-]
[auth_type(authentication-method)]
[auth_type+(authentication-method)]
[auth_type-(authentication-method)]
[category(category-names...) | category-(category-names...)]
[comment('installation defined data') | comment- ]
[country(...)]
[enable]
[expire | expire(mm/dd/yy[yy][@hh:mm]) | expire-]
[fullname('full-name')]
[gen_prop(property-name) [ {gen_flag | gen_op}(flag)] gen_val(property-values
...)]
[gowner(group-name)]
[grace(number-of-grace-logins) | grace-]
[ign_hol | ign_hol-]
[inactive(num-inactive-days) | inactive-]
[interval(maximum-password-change-interval) | interval-]
[label(label-name)| label-]
[level(seclevel-num) | level-]
[location(...)]
[maxlogins(maximum-number-of-logins) | maxlogins-]
[min_life(minimum-password-change-interval) | min_life-]
[notify(notify-address) | notify-]
[operator | operator-]
[organization(name)]
[org_unit(name)]
[owner(user-name or group-name)]
[password(user's temporary password)]
[phone(...)]
[pmdb(PolicyModel-name) | pmdb-]
[record(group-name) | record-]
[pwmanager | pwmanager-]
[regular]
[restrictions(days( day-data ) time(hhmm:hhmm | anytime) ) | restrictions-]
day-data: {[mon] [tue] [wed] [thu] [fri] [sat] [sun]} | anyday | weekdays
[resume | resume(mm/dd/yy[yy][@hh:mm]) | resume-]
[server | server-]
[suspend | suspend(mm/dd/yy[yy][@hh:mm]) | suspend-]
[nt| nt( nt-user-attributes  )]
nt-user-attributes :
[admin | admin-]
[comment('installation defined data') | comment- ]
[country(any-string)]
[expire | expire(mm/dd/yy[@hh:mm]) | expire-]
```

```
[flags(account-flags) | -(account-flags)]
[homedir(any-string)]
[homedrive(home-drive)]
[location(any-string)]
[logonserver(server-name)]
[name(full-name)]
[organization(name)]
[org_unit(name)]
[password(user's temporary password)]
[pgroup(primary-group)]
[phone(any-string)]
[privileges(privilege-list)]
[restrictions(days( day-data ) time(hhmm:hhmm | anytime) )]
day-data: {[mon] [tue] [wed] [thu] [fri] [sat] [sun]} | anyday | weekdays
[script(logon-script-path)]
[terminals(terminal-list) | terminals-(terminal-list)]
[workstation(workstation-list)]
```

Arguments

admin

Assigns the ADMIN attribute to the user. A user with the ADMIN attribute is allowed to issue all eTrust AC commands with all parameters except audit. You must have the ADMIN attribute to issue the admin parameter.

admin-

The admin- parameter removes the ADMIN attribute from the user. You must have the ADMIN attribute to use the admin- parameter. Use this parameter only with the chusr or editusr command. (You cannot remove the ADMIN attribute – from a user if the user is the only user in the database with it. There must always be at least one user with the ADMIN attribute in the database.)

audit

Specifies which user activities are logged to the audit log. If more than one event type is specified, separate the event type names with a space or a comma. These are the audit attributes:

- **all**—All user activities on resources protected by eTrust AC are logged. The monitored activities are: failure, loginfail, loginsuccess, and success.
- **failure**—eTrust AC logs failed access attempts.
- **loginfail**—eTrust AC logs failed login attempts.
- **loginsuccess**—eTrust AC logs successful logins.
- **none**—eTrust AC logs no user activities.
- **success**—eTrust AC logs successful accesses.

auditor

Assigns the AUDITOR attribute to the user. A user with the AUDITOR attribute can audit the use of system resources and is able to control the logging of detected accesses to any eTrust AC-protected resource during eTrust AC authorization checking and accesses to the database. For more information on the authorities granted to a user with the AUDITOR attribute, see the *Administrator Guide*. To specify the auditor parameter, you must have the ADMIN attribute.

auditor- Removes the AUDITOR attribute from the user record. To specify the auditor- parameter, you must have the ADMIN attribute. Only use this parameter with the chusr or editusr command.

calendar(*calendarName*) Specifies Unicenter TNG calendar objects, which represent time restrictions in Unicenter TNG. eTrust AC maintains a list of these objects for management purposes only, but doesn't protect them.

calendarName is the name of one or more Unicenter TNG calendar records defined in the CALENDAR class. When assigning more than one calendar, separate the calendar names with a space or a comma.

calendar- Removes one or more Unicenter TNG calendar records from the user record. Only use this parameter with the chusr or editusr command.

category(*categoryName*)

Assigns to the user one or more security category records that are defined in the CATEGORY class. When assigning more than one security category, separate the security category names with a space or a comma. See the *Administrator Guide* for more information about security category checking.

category-(*categoryName*)

Removes one or more security categories from the user record. When deleting more than one security category, separate the security category names with a space or a comma. Use this parameter only with the chusr or editusr command.

comment(*string*) Assigns a comment string to the user record. Enter an alphanumeric string of up to 255 characters. If the string contains any blanks, enclose the entire string in single quotation marks.

comment- Deletes the comment string from the user record. Use this parameter only with the chusr or editusr command.

country(*string*) Specifies the country where the user is located. Enter an alphanumeric string of up to 19 characters. If the string contains any blanks, enclose the entire string in single quotation marks. This string is not used during the authorization process.

enable Enables the login of a user that has for any reason been disabled. This is a chusr and editusr parameter.

expire(*date*) Sets the date when the user account expires. If a date is not specified, the account expires immediately, provided the user is not currently logged in. If the user is logged in, the account expires when the user logs out.

If the user record has a value for this parameter, that value overrides the value in the GROUP record.

Specify the expiration date, and optional time, in the following format: *mm/dd/yy [yy][@HH:MM]*. Year can be either 2 or 4 digits.

Note: You cannot enable expired user records by specifying the resume parameter with a resume date. Use the expire- parameter to enable expired user records.

expire-

For the newusr command, defines a user account that does not have an expiration date. For the chusr and editusr commands, removes an expiration date from a user account.

flags (*flags* | *–flags*)

Specifies particular attributes of a user's account. See the appendix "Windows Values" for a list of valid flag values.

To remove flags from the user record, precede the flag value with a minus (–). You can specify –flags only with the chusr or editusr command.

fullname (*fullName*)

Specifies the full name of the user associated with the user record. In the eTrust database, the string can contain up to 48 alphanumeric characters. If it contains any blanks, enclose it in single quotation marks.

gen_prop(*property*)

Specifies an Active Directory property.

gen_val(*value*)

Specifies the value associated with an Active Directory property.

gowner(*groupName*)

Assigns an eTrust AC group as the owner of the user record. The group owner of the user record has unrestricted access to it, provided the group owner's security level, security label, and security category authorities are sufficient to allow access to the user record. The group owner of the user record is always permitted to update and delete the user record. See the *Administrator Guide* for more information.

grace(*nLogins*)

Sets the number of grace logins the user is allowed. Enter a positive integer between 0 and 255.

After the number of grace logins is reached, the user is cannot access the system and must contact the system administrator to select a new password. If grace is set to zero, the user cannot log in.

If the user record has a value for this parameter, that value overrides the value in the GROUP record.

If this parameter is not specified and the user has a profile group that contains a value for this parameter, the value in the GROUP record is used. If neither the USER nor GROUP record contains a value, the eTrust AC global grace login setting is used.

grace-

Deletes the user's grace login setting. The eTrust AC global grace login setting is used instead. Use this parameter only with the chusr or editusr command.

homedir(*path*)

Specifies the full path of the user's home directory. When you end path with a slash, eTrust AC concatenates userName to the specified path.

homedrive(*drive*)

Specifies the drive of the user's home directory. Users log in automatically to their own home drives and home directories.

ign_hol

Assigns the IGN_HOL attribute to the user. A user with the IGN_HOL attribute can log in during any period defined in a holiday record.

ign_hol-

Removes IGN_HOL attribute from the user, so that the user can no longer necessarily log in during all holidays.

inactive(*nDays*)

Specifies the number of days that must pass before the system changes the user to inactive. When the number of days is reached, the user cannot log in.

Enter a positive integer or zero. If inactive is set to zero, the effect is the same as using the inactive- parameter.

Note: In the user record, inactive users are not marked. To identify inactive users, you must compare the Last Accessed Time value with the Inactive Days value.

inactive-

Changes the user's status from inactive to active. Use this parameter only with the chusr or editusr command.

interval(*nDays*)

Sets the number of days that must pass after the password was set or changed before the system prompts the user for a new password. Enter a positive integer or zero. An interval of zero disables password interval checking for the group so that the password does not expire. The default set by the setoptions command is not used. Set an interval of zero only for users with low security requirements.

When the specified number of days is reached, eTrust AC informs the user that the current password has expired. The user can immediately renew the password or continue using the old password until the number of grace logins is reached. After the number of grace logins is reached, the user is denied access to the system and must contact the system administrator to select a new password.

interval-

Cancels a user's password interval setting. If the user has a profile group with a value for this parameter, that value is used. Otherwise, the default set by the setoptions command is used. Use this parameter only with the chusr or editusr command.

label(*labelName*)
Assigns to the user record a security label record that is defined in the SECLABEL class. A security label represents an association between a particular security level and zero or more security categories. For a complete discussion on how to implement security label checking, see the *Administrator Guide*.

label-
Deletes the security label from the user record. Use this parameter only with the chusr or editusr command.

level(*number*)
Assigns a security level to the user record. Enter a positive integer between 1 and 255. For a complete discussion on how to implement security level checking, see the *Administrator Guide*.

level-
Deletes the security level from the user record, so that the user no longer has access to any resource that requires the accessor to have a security level. Use this parameter only with the chusr or editusr command.

location(*string*)
Specifies the user's location. Enter an alphanumeric string of up to 47 characters. If the string contains any blanks, enclose the entire string in single quotation marks. This string is not used during the authorization process.

logonserver(*serverName*)
Specifies the server that verifies the login information for the user. When the user logs in to the domain workstation, eTrust AC transfers the login information to the server, which gives the workstation permission for the user to work.

maxlogins(*nLogins*)
Sets the maximum number of terminals the user can log in to at the same time. A value of 0 (zero) means that the user can log in from any number of terminals concurrently. If this parameter is not specified, the global maximum logins setting is used.

Note: If maxlogins is set to 1, you cannot run selang. You must shut down eTrust AC, change the maxlogins setting to greater than one, and start eTrust AC again.

maxlogins-
Deletes the user's maximum login setting. The global setting is used instead. Use this parameter only with the chusr or editusr command.

min_life(*nDays*)
The minimum number of days that must pass before the user is allowed to change the password again. Enter a positive integer.

min_life-
Deletes the user's min_life setting. If the user has a profile group with a value for this parameter, that value is used. Otherwise, the default set by the setoptions command is used. Use this parameter only with the chusr or editusr command.

name(*string*)
Specifies the full name of the user that is associated with the user record. Enter an alphanumeric string of up to 48 characters. If the string contains any blanks, enclose the entire string in single quotation marks.

notify(*mailAddress*)

Notifies the user every time the user logs in. Enter a user name, an email address of a user, or the email address of a mail group if an alias is specified. The recipient of the notify messages should log in frequently to respond to the unauthorized access attempts described in each message.

Each time a notification message is sent, an audit record is written in the audit log. For information on filtering and viewing audit records, see the *Administrator Guide*.

notify-

Specifies that no one is notified when the user logs in. Use this parameter only with the chusr or editusr command.

nt

For the chusr and editusr commands, this parameter changes the user definition in the local Windows system. For the newusr command, this parameter adds the user to the local Windows system. If you specify more than one argument, separate the arguments with a space.

For more information on how to operate on the local Windows system from within eTrust AC, see the environment command in this chapter, and the chapter "selang Commands in the Windows Environment."

operator

Assigns the OPERATOR attribute to the user. A user with the OPERATOR attribute can list all resource records in the database, and has read authority for all eTrust AC defined files. For more information, see the *Administrator Guide*.

A user with this attribute can also use all the options of the secons command. For more information on the secons utility, see the chapter "Utilities" in this guide.

operator-

Removes the OPERATOR attribute from a user record. Only use this parameter with the chusr or editusr command.

organization(*string*)

Specifies the organization in which the user works. Enter an alphanumeric string of up to 19 characters. If the string contains any blanks, enclose the entire string in single quotation marks. This information is not used during the authorization process.

org_unit(*string*)

Specifies the organizational unit in which the user works. Enter an alphanumeric string of up to 19 characters. If the string contains any blanks, enclose it in single quotation marks. This information is not used during the authorization process.

owner(*userName*|*groupName*)

Assigns an eTrust AC user (*userName*) or group (*groupName*) as the owner of the user record. For more information, see the *Administrator Guide*.

password(*string*)

Assigns a password of up to 14 characters to a user. Specify any character except a space or a comma. If password checking is enabled, the password is valid for one login only. When the user next logs in to the system, a new password must be set.

You cannot change your own password, even if you have the ADMIN or PWMANAGER attribute or are a member of the eTrust AC Admins group.

pgroup(*groupName*)

Sets the user's primary group ID. A primary group is one of the groups in which a user is defined and must be a Global group.

In eTrust AC, the primary group has no special significance.

phone(*string*)

Specifies the user's phone number. Enter an alphanumeric string of up to 19 characters. If the string contains any blanks, enclose the entire string in single quotation marks. This information is not used during the authorization process.

pmdb(*pmdbName*)

Specifies that when a user changes a password with the utility sepass, eTrust AC will propagate the new password to the specified Policy Model (*pmdbName*). The password is not sent to the Policy Model defined by the parent_pmd or passwd_pmd values in the registry subkey:
HKEY_LOCAL_MACHINE\SOFTWARE\
ComputerAssociates\eTrustAccessControl\eTrustAccessControl

pmdb-

Removes the pmdb attribute from the user record. Only use this parameter with the chusr or editusr command.

privileges

Adds specific rights to the Windows user record or, when privList is preceded by a minus sign (–), removes the specified rights. You can specify this parameter only with the chusr or editusr command, and only when you are changing an existing user record. You cannot use it to assign privileges when you are creating a new user record.

profile(*groupName*)

Assigns a user to a profile group. eTrust AC assigns properties from the profile group to the user if the properties were not explicitly assigned to the user in the user record.

The following values can be taken from the profile group:

- audit
- auth_type
- expire
- grace
- inactive
- interval
- maxlogins
- min_life
- nt
- password rules

- pmdb
- pwd_autogen
- pwd_policy
- pwd_sync
- restrictions (days, time)
- resume
- suspend

profile-

Removes a user from the profile group. Only use this parameter with the chusr or editusr command.

pwmanager

Assigns the PWMANAGER attribute to the user. A user with this attribute can change the passwords of users in the database. For more information, see the *Administrator Guide*.

pwmanager-

Removes the PWMANAGER attribute from the user record. Only use this parameter with the chusr or editusr command.

restrictions([days] [time])

Specifies the days of the week and the hours in the day when users may access the file.

If you omit the days argument and specify the time argument, the time restriction applies to any day-of-week restriction already indicated in the record. If you omit time and specify days, the day restriction applies to any time restriction already indicated in the record. If you specify both days and time, the users may access the system only during the specified time period on the specified days.

- [Days] specifies the days on which users may access the file. The days argument takes the following sub-arguments:
  - **anyday**—Allow users access to the file on any day.
  - **weekdays**—Allow users access to the resource only on weekdays—Monday through Friday.
  - **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, **Sun**—Allow users access to the resource only on the specified days. You can specify the days in any order. If you specify more than one day, separate the days with a space or a comma.
- [Time] specifies the period during which users may access the resource. The time argument takes the following sub-arguments:
  - **anytime**—Allow users access to the resource at any time of the day.

- **startTime:endTime**—Allow access to the resource only during the specified period. The format of both startTime and endTime is *hhmm*, where *hh* is the hour in 24-hour notation (00 through 23) and *mm* is the minutes (00 through 59). Note that 2400 is not a valid time value. startTime must be less than endTime, and both times must occur on the same day. If the terminal is in a different time zone from the processor, adjust the time values by translating the start and end times for the terminal to the equivalent local times for the processor. For example, if the processor is in New York and the terminal is in Los Angeles, to allow access to the terminal from 8:00 a.m. to 5:00 p.m. in Los Angeles, specify time (1100:2000).

restrictions-([days] [time])

Deletes any restrictions that limit the users' ability to access the file.

resume(*date*)

Enables a user record that was disabled by specifying the suspend parameter. If you specify both the suspend parameter and the resume parameter, the resume date must fall after the suspend date. If you omit *date*, the user record is resumed immediately upon execution of the chusr command. See the *Administrator Guide* for more information.

Enter a date, and optional time, in the following format: *mm/dd/yy[@HH:MM].*

resume-

Erases the resume date, and time if used, from the user record. Consequently, the status of the user is changed from active (enabled) to suspended. Use this parameter only with the chusr or editusr command.

scriptpath

Specifies the location of a file that runs automatically when the user logs in. This login script configures the working environment. This parameter is optional, since the profile parameter also sets up the user's working environment.

server

Sets the SERVER attribute on. This attribute allows a process running on behalf of the current user to ask for authorization for other users. For more information, see the *Administrator Guide*.

server-

Sets the SERVER attribute off. Only use this parameter with the chusr or editusr command.

suspend(*date*)

Disables a user record, but leaves it defined in the database. A user cannot use a suspended user account to log in to the system. If *date* is specified, the user record is suspended on the specified date. If *date* is omitted, the user record is suspended immediately upon execution of the chusr command.

Enter a date, and optional time, in the following format: *mm/dd/yy[@HH:MM].*

suspend-

Erases the suspend date from the user record, changing the status of the user from disabled to active (enabled). Use this parameter only with the chusr or editusr command.

userName

The name of the user record. When using the newusr command, this name identifies the user to eTrust AC. Each user name must be unique, must not currently exist in the database as a user or group name, and, if the user is already defined to UNIX, must be the same as the UNIX username.

Though typically an eTrust AC username should be identical to a login name recognized by Windows, for some purposes you may want an eTrust AC username that is not a Windows login name. (Then the login command could not put that user to work, but another command such as sesu could.)

When defining or changing more than one user record, enclose the list of user names in parentheses and separate the user names with spaces or commas.

workstations

Specifies up to eight workstations from which the user can log in. Surround the list with quotation marks, and separate the names with commas. For example: “workstation1,workstation2”

See Also

The rmusr and showusr commands in this chapter.

Examples

- The user Bob wants to add the FINANCIAL category to Jim’s record, change Jim’s security level to 155, and restrict Jim’s access to the system to weekdays between 8:00 a.m. and 8:00 p.m.

Known	Command
The user Bob has the ADMIN attribute.	chusr Jim \
The user Jim is defined to eTrust AC.	category(FINANCIAL) \
The FINANCIAL category is defined to eTrust AC.	level(155) \
	restrictions \
	(days(weekdays)time(0800:2000))

- The user “admin” wants to suspend the user Joel, who will be on vacation for three weeks, starting on August 5, 1995.

Known	Command
The user admin has the ADMIN attribute. The user Joel is defined to eTrust AC. Today’s date is August 3, 1994.	chusr Joel \\ suspend(8/5/95) \\ resume(8/26/95)

- The user Security2 wants to remove the AUDITOR attribute from the user Bill and wants to audit all activity by Bill.

Known	Command
The user Security2 has the ADMIN and AUDITOR attributes. The user Bill is defined to eTrust AC.	chusr Bill \\ auditor- \\ audit(all)

- The user Rob wants to change the comment stored in the record of the user Mary.

Known	Command
The user Rob is the owner of Mary’s user record.	chusr Mary \\ comment \\ (‘Administrator of the SALES group’)

- The admin user Sally wants to remove the country name and the location properties stored in the record of the user Jared.

Known	Command
The user Sally is the owner of Jared’s user record.	chusr Jared \\ country() \\ location()

To remove any record property, if the property is defined by a string, type the property with either the “-” sign or empty parenthesis “()”.

- The user Bob wants to define the users Peter and Joe to eTrust AC.

Known	Command	Defaults

The user Bob has the ADMIN attribute.
The users Peter and Joe are not defined to eTrust AC.
	newusr (Peter Joe)	owner(Bob)
		audit(failure, loginfailure)

- The user Bob wants to define the user Jane to eTrust AC and assign "payroll" as the owning group.

Known	Command	Defaults
The user Bob has the ADMIN attribute. The user Jane is not defined to eTrust AC. The full name of the user Jane is JG Harris.	newusr Jane \ owner(payroll) \ name('J.G. Harris')	audit(failure, loginfailure)

- The user Bob wants to define the user *JohnD* to eTrust AC with the security category NewEmployee and a security level of three. JohnD is to be allowed to use the system only on weekdays between the hours of 8:00 a.m. and 6:00 p.m.

Known	Command	Defaults

The user Bob has the ADMIN attribute.
The NewEmployee category is defined to eTrust AC.
The new user's full name is John Doe.
	newusr JohnD \
	name('John Doe') \
	category(NewEmployee) \
	level(3) \
	restrictions(days(weekdays) \
	time(0800:1800))
		owner(Bob)
		audit(failure)

environment

Purpose

The environment command sets the security environment. eTrust AC supports the eTrust AC, Windows, and UNIX security environments. When you invoke the selang command shell, the eTrust environment is the default.

Syntax

```
{environment | env} {eTrust | native | nt | pmd | unix}
```

Arguments

eTrust

Indicates the eTrust security environment. The selang commands affect the eTrust AC database. Some commands support simultaneous updates to the native OS security settings of the host you are connected to. In the eTrust environment, the selang prompt is: eTrust>.

native

Indicates the native OS security environment (either Windows or UNIX) of the host you are connected to, whether local or remote. The selang commands affect the native OS database. In the native environment, the selang prompt is: eTrust(native)>.

nt

Indicates the Windows security environment. The selang commands affect the Windows database. Some commands support simultaneous updates to the eTrust AC security settings. In the Windows environment, the selang prompt is: eTrust(nt)>.

pmd

Indicates the remote management environment. The selang commands affect the PMDB of the selected host. In the pmd environment, the selang prompt is: eTrust(pmd)>.

unix

When connected to a remote UNIX host, indicates that commands you enter affect the UNIX database. In the UNIX environment, the selang prompt is: eTrust(unix)>.

find

Purpose

The find command has several functions:

- If you do not specify a class, the output is the names of all the classes defined to eTrust AC.
- If you only specify a class, the output is the names of all the objects in the specified class.
- If you specify both a class and an object mask, the output is the names of all the objects in the specified class that match the specified object mask.

Notes

- If you have the ADMIN, AUDITOR, or OPERATOR attribute, you can use the find command with all parameters.
- If you have READ authority in the access control list of a record in the ADMIN class, you can specify the class parameter for the class represented by the record.

Syntax

```
{find | f} [{className | class(className)} | className(memberName) | objMask ]
```

class(*className*) The name of any valid class in the eTrust environment except SEOS.

objmask Lists all objects in the specified class that match the specified object mask. Indicate an object mask by using wildcards.

className(*memberName*) The name of a member of a class. Enclose multiple entries in parentheses and separate them with a space or comma.

Example

User Sue, who has the ADMIN attribute, wants to list all the resource types supported by eTrust AC. The output resembles the following:

```
NT:
===
USER
GROUP
FILE
PRINTER
SHARE
DISK
COM
SEOS
REGVAL
REGKEY
DOMAIN
PROCESS
```

help

Purpose

The help command displays selang syntax.

- Used without parameters, it displays a list of the selang commands, with a brief explanation of each:

```
authorize (auth) - set user/group’s permissions to a resource.
authorize- (auth-) - remove user/group’s permissions to a resource.
.
.
.
```

- Used with a selang command name, it displays the syntax of the given command. (See Example in this section.)

- Used with the access parameter, it displays a list of values for the access parameter of the authorize command and the defaccess parameter of the new*, ch*, and edit* commands:

  ```
  For all classes access values NONE and ALL are valid.
  FILE :
  READ, WRITE, EXECUTE, UPDATE, CHOWN, CHMOD,
  RENAME, DELETE, UTIME, SEC, CREATE
  PROGRAM, SUDO:
  EXECUTE
  ADMIN:
  READ, MODIFY, CREATE, DELETE, JOIN, PASSWORD
  Other resources:
  READ
  ```

  For more information on access authorities, see the *Administrator Guide*.

- Used with the lineedit parameter, it displays a list of special characters for selang command line manipulations:

  ```
  # or * in the beginning of a line - a comment
  ! in the beginning of a line - a shell command
  UP-ARROW to get previous commands.
   If the command-line is not empty only commands that match current
   command-line will be searched.

   DOWN-ARROW to get next command.

   ^ in the beginning of a line - invoke commands from history.
   type help history for more information.

   \ in the last character of a line - there will be a\
   continuation line

   | (pipe) at the end of the line.
   pipes the command output to pipe (only one pipe is allowed)

   [TAB] to use word completion.

   [CTRL-D] to get a list of all possible completions.

   press ESC twice to get help text for current command -
   if for example you type “authorize FILE /tmp/foo [ESC ESC] you will
   get help text for authorize command, and the command line will remain
   untouched.
  ```

Syntax

```
{help | h | ?} [command-name | access | lineedit ]
```

Arguments

commandName Requests the syntax for the specified command.

access	Requests a class-by-class list of the access types that the access and defaccess parameters can specify.
lineedit	Requests a list of special characters for selang command line manipulations.

Example

This example displays the syntax of the showusr command.

```
eTrust> help showusr
>> {showusr | su} user-name
                  [nt]
```

history

Purpose

The history command lists all the commands entered during the current selang command shell session. The commands are ordered chronologically. The number of the command precedes each command. For example, the number three precedes the third command entered.

The history command does not display a password even if one was entered as part of a chusr, newusr, or editusr command. The history command displays a series of asterisks (***) instead of the clear text password.

The selang command language supports the following shortcuts that make use of commands in the history list:

Specify...	To execute...
^^ [*string*]	The previous command. If you specify *string*, it is appended to the original command.
^*n* [*string*]	The command preceded by the number *n* in the history list, where *n* is a positive integer. If you specify *string*, it is appended to the original command.
^-*n* [*string*]	The *n*th command from the end of the list, where *n* is a positive integer. If you specify *string*, it is appended to the original command.
^match [*string*]	The most recently issued command that begins with the characters *match*, where *match* is a text string. If you specify *string*, it is appended to the original command. *Match* and *string* are separated by a space.

Syntax

```
history
```

hosts

Purpose

You can connect to a remote eTrust AC machine with a different name, so you can remotely manage the machine while local eTrust AC services are not running.

The hosts command specifies the hosts or Policy Models that receive the selang commands. The hosts command must be executed before executing the commands that are directed to the hosts. If you do not specify hosts, the local host is the default; that is, all commands are directed to the database on the local host.

To list all the hosts and PMDBs currently available, specify the hosts command without any parameters.

Notes

- To administer (update) a remote host database from the local host, the user must meet one of the following criteria:
  - Be explicitly authorized to update the remote host database from the local database
  - Be a member of a group that is allowed to update the remote host database from the local database
  - Be the owner of the local host as defined in the remote host
- To give a user authorization to update the remote host database from the local database, on the remote host enter the command:

  ```
  authorize TERMINAL local_host uid user_name access(write)
  ```

- In order to give a group authorization to update the remote host database from the local database, on the remote host enter the command:

  ```
      authorize TERMINAL local_host gid(group_name) access(write)
  ```

- If you specify hosts *policy@*, all commands that you enter update the PMDB on the local host.
- eTrust AC protects hosts through their canonical host names and not through aliases. In order to avoid the confusion caused by alias names, eTrust AC issues a warning when a HOST rule is defined for an alias name.

- Similarly, eTrust AC gives a warning if you attempt to define a HOST with less than a fully qualified name, because eTrust AC uses fully qualified names (such mymachine.yourcompany.com) for hosts.

Syntax

```
hosts [{systemIds | policyModel@hostname}]
```

Arguments

systemIds The system IDs of the hosts on which the selang commands will execute. When specifying more than one host, enclose the list of systems IDs in parentheses and separate the system IDs with a space or a comma.

policyModel@hostname The addresses of the Policy Models on which the selang commands will execute. When specifying more than one Policy Model, enclose the list of Policy Model addresses in parentheses and separate the Policy Model addresses with a space or a comma.

The advantage of using a Policy Model over explicitly specifying the hosts is that the system where the Policy Model resides keeps on trying to update all the systems defined to the Policy Model, even if they are currently unavailable. For more information on Policy Models, see the *Administrator Guide*.

Examples

- To apply all subsequent commands to the Policy Model on the station h1, type the command:

  ```
  hosts Policy@h1
  ```

  If the connection to *Policy@h1* is successful, the following message appears.

  ```
  >> Successfully connected to h1
  ```

  All commands entered from now on are directed to Policy@h1 and not to the local host. The selang prompt changes to the following:

  ```
  Remote eTrust>
  ```

- To apply all future commands to the station athena, type the command:

  ```
  hosts athena
  ```

  If successful connections are made to athena, the following messages appear on the screen.

  ```
  >> (athena)
  >> Successfully connected
  >> INFO: Target version is 2.50
  ```

  Any command you enter is applied to athena and is not sent to the local host. If you add a new user, the user is only added to athena, as shown in this example:

```
Remote eTrust>newusr steve
(athena) >> USER steve successfully added.
```

join

Purpose

The join command adds users to one or more groups, or changes their set of properties with respect to the groups. The specified users and groups must already exist in eTrust AC.

The set of properties from the join command *completely replaces* any previous set of properties for the specified users in the specified groups. If any such properties were defined earlier, they are not retained unless the new join command specifies them again.

Note: Both the MODIFY and JOIN properties are required if an ADMIN is to have the authority to modify eTrust AC GROUP records and Windows groups.

Syntax

```
{join | j} user-name | (user-names ...)
   group(group-names)
   [admin | admin-]
   [auditor | auditor-]
   [gowner(group-name)]
   [operator | operator-]
   [owner(user-name or group-name)]
   [pwmanager | pwmanager-]
   [regular]
   [nt]
```

Arguments

admin

Assigns the GROUP-ADMIN attribute to the user specified by *userName*. See the *Administrator Guide* for more information.

admin-

Removes the GROUP-ADMIN attribute from the user.

auditor

Assigns the GROUP-AUDIT attribute to the user specified by *userName*. See the *Administrator Guide* for more information.

auditor-

Removes the GROUP-AUDITOR attribute from the user.

group(*groupName*)

Specifies that the user is being added to the group *groupName*. When specifying more than one group, enclose the group names in parentheses and separate the names with a space or a comma.

nt — Connects *userName* to a group in the Windows database.

operator — Assigns the GROUP-OPERATOR attribute to the user specified by *userName*. See the *Administrator Guide* for more information.

operator- — Removes the GROUP-OPERATOR attribute from the user.

owner(*userName* |*groupName*) — Specifies an eTrust AC user or group as the owner of the join record. If you are creating a connection and you do not specify an owner, you are assigned ownership of the connection.

pwmanager — Assigns the GROUP-PWMANAGER attribute to *userName*. pwmanager- removes the attribute when the user is reconnected to the group. For more information, see the *Administrator Guide*.

userName — The user name of the user who is connecting (or reconnecting with a new set of properties) to the group or groups specified by the group parameter. When specifying more than one user, enclose the user names in parentheses and separate the user names with a space or a comma. *userName* is required and must appear as the first parameter.

See Also

The showusr and showgrp commands in this chapter.

Examples

- The user Rory wants to join the user Bob to the group staff.

Known	Command	Defaults
Rory has the ADMIN attribute.	join Bob group(staff)	admin- auditor- owner(Rory) pwmanager-

- The user Rory wants to change the definition of Sue in the group staff. She currently is a GROUP-AUDITOR; Rory wants to add the GROUP-PWMANAGER attribute.

Known	Command	Defaults
Rory has the ADMIN attribute.	join Sue group(staff) auditor \ pwmanager	admin- owner(Rory)

When eTrust AC executes this command, it deletes the previous record. No record is kept of Sue's previous attributes. Therefore, Rory must specify the two attributes Sue should have now.

- The user Bill wants to remove the users sales25 and sales43 from the group PAYROLL.

Known	Command
The user Bill has the ADMIN attribute.	join- (sales25 sales43) group(PAYROLL)

list

Purpose

Lists the classes in the environment.

Syntax

```
list
```

rename

Purpose

Renames an object in the database. All the rules of the old object apply to the renamed object. The object is known by its new name only.

Note: You cannot rename the SEOS, UACC, and ADMIN classes.

Note: The maximum length of an object name is 255 characters. eTrust AC does not allow managing resources with names exceeding 255 characters. This statement is relevant for the native environment as well.

Authorization

To use the rename command, you must have adequate authority for a resource. eTrust AC makes the following checks until **one** of the following conditions is met:

- You have the ADMIN attribute.
- The resource record is within the scope of a group in which you have the GROUP-ADMIN attribute.
- You are the owner of the record.
- You are assigned MODIFY (for chres) or CREATE (for editres) access authority in the eTrust AC list of the resource class's record in the ADMIN class.

Syntax

```
rename className oldresourceName newresourceName
```

Arguments

className

The class in which the object is defined.

oldresourceName

The old names of the object.

newresourceName

The new name of the object. All the rules of the old object name apply to the renamed object.

Example

A user named ADMIN 1 wants to rename a record in the HOST class from spree3 to spree4. The specified user has the ADMIN attribute. The user can then use the following command:

```
rename host spree3 spree4
```

rmfile

Purpose

The rmfile command deletes files from the database. Files are resource records belonging to the FILE class.

Syntax

```
{rmfile | rf} file-name | (file-names ...)
```

Arguments

fileName

The name of the file you are removing. When removing more than one file, enclose the list of file names in parentheses and separate the file names with a space or a comma.

eTrust AC processes each file record independently. If an error occurs while processing a file, eTrust AC issues a message and continues processing with the next file in the list.

See Also

The checklogin, editfile/newfile and showfile commands in this chapter.

Example

The security administrator wants to remove eTrust AC protection for the file C:\temp\passwords.txt.

Known	Command
The security administrator has the ADMIN attribute.	rmfile C:\temp\passwords.txt

rmgrp

Purpose

The rmgrp command removes one or more groups from eTrust AC and the Windows database.

There are places in the eTrust AC database where the group ID may appear that are not updated by the rmgrp command, because processing of the rmgrp command does not delete every occurrence of the group ID. For example, the group ID could occur in resource access control lists; in this case, the group would be considered unknown.

In Windows, each SID (security identifier) is unique; if you remove a group, the unique identifier for the group account no longer exists. A new group created with the same name will have a different identifier and will, therefore, be unable to access anything the previous group was able to access unless the new group is given the same permissions and other necessary properties.

Use the authorize command to remove the group ID from access control lists that may contain it.

Syntax

```
{rmgrp | rg}  group-name | (group-names ...)
   [nt]
```

Arguments

groupName

Specifies the name of the eTrust AC group record to be deleted. To delete more than one group, enclose the list of group names in parentheses and separate the group names with a space or a comma.

If you are still using the version 4.1 designation for Global groups, precede the name with a tilde (~).

GlobalGroup(*globalGroupName*)

Specifies a Global group record to be deleted. This parameter was introduced in version 5.1 to replace the tilde (which is still supported for backward compatibility.)

nt

Specifies a Windows group to be deleted.

See Also

The chgrp/editgrp/newgrp, showgrp, and join commands in this chapter.

Example

The user Joe wants to delete the groups DEPT1 and DEPT2 from the eTrust AC database.

Known	Command
The user Joe has GROUP-ADMIN authority to the SALES group. The SALES group owns the groups DEPT1 and DEPT2.	rmgrp (DEPT1 DEPT2)

rmres

Purpose

The rmres command removes resources from the database. Records belonging to the following classes can be deleted using the rmres command: ADMIN, CATEGORY, CONNECT, FILE, GHOST, GSUDO, GTERMINAL, HOST, HOSTNET, HOSTNP, SECFILE, SECLABEL, SUDO, SURROGATE, TERMINAL, PROGRAM, PROCESS, TCP, UACC, and any user defined class.

Syntax

```
{rmres | rr} class-name record-name | (record-names ...)
```

Arguments

class-name

The name of the class to which the resource belongs. To list the resource classes defined to eTrust AC, use the find command. For more information, see the find command in this chapter.

record-name

The name of the resource record you are deleting. When removing more than one resource, enclose the list of resource names in parentheses and separate the resource names with a space or a comma.

eTrust AC processes each resource record independently. If an error occurs while processing a resource, eTrust AC issues a message and continues processing with the next resource in the list.

See Also

The chres/editres/newres and showres commands in this chapter.

Example

The user Admin1 wants to remove the record TERMS from the TERMINAL class in the database.

Known	Command
The user Admin1 has the ADMIN attribute.	rmres TERMINAL TERMS

rmusr

Purpose

The rmusr command removes a user from eTrust AC and Windows by removing the user's record from the database and removing all references to the user's record that exist in group records. The rmusr command optionally removes the user from the Windows database as well.

There may be places in the eTrust AC database where the user's user ID appears that the rmusr command does not delete. For instance, the user could be the owner of a group, the owner of other records, or in an access control list for a resource. Use the chgrp, chusr, chres, and authorize commands, as required, to manually change ownership and remove access authorities relating to the user record you want to delete.

In Windows, each SID is unique; if you remove a user, the unique identifier for the user account no longer exists. A new account created with the same name will have a different identifier and will, therefore, be unable to access anything the previous account was able to access unless the new account is given the same permissions and other necessary properties.

Syntax

```
{rmusr | ru} user-name | (user-names ...)
        [nt]
```

Arguments

user-name
The name of the user record. When removing more than one user record, enclose the list of user names in parentheses and separate the user names with a space or a comma.

nt
Deletes the user from the Windows environment, in addition to deleting the user from eTrust AC.

See Also

The chusr/editusr/newusr and showusr commands in this chapter.

Example

The user admin wants to delete the user TerryS from eTrust AC.

Known	Command
The user TerryS is defined to eTrust AC.	rmusr TerryS

ruler

Purpose

The ruler command determines which properties eTrust AC displays whenever the showusr, showgrp, showres, or showfile command is executed. By default, eTrust AC displays all the properties of a class except for electronic signatures. By using this command, you can choose to display only properties that interest you.

The ruler command only applies to the hosts of the current session and displays the rulers of all the hosts of the current session. The properties of each host are displayed in a separate list. If you change hosts, the ruler command does not change the display of properties in the new hosts.

If you do not enter at least one property name when executing this command, eTrust AC displays the names of the properties that are in the current ruler.

Authorization

Only the following users can issue this command:

- Users with the ADMIN, AUDITOR, or OPERATOR attribute.
- Users who have access read in class ADMIN for the class whose ruler they are trying to set. For example, if you have access read in class ADMIN for the record representing class TERMINAL, you can set the ruler for class TERMINAL.

Syntax

```
ruler class-name [props(all | list-of-property-names)]
```

Arguments

class-name

The name of the class whose display you want to change

props()

Specifies the properties to be displayed:

- **all**—Specifies that all the properties of the class are to be displayed.
- **list-of-property-names**—Specifies the names of the one or more eTrust AC properties to be displayed. When specifying more than one property, enclose the property names in parentheses and separate the names with a space or a comma.

See Also

The showfile, showgrp, showres, and showusr commands in this chapter.

Examples

- The user admin wants eTrust AC to display only two properties for each user: the owner and the user who is notified about changes.

Known	Command
The class USER is defined to eTrust AC.	ruler USER props(NOTIFY OWNER)

- The user admin wants to display the properties in the current ruler for class USER.

Known	Command
The class USER is defined to eTrust AC.	ruler USER

- The user admin wants eTrust AC to revert to the default ruler—to display all the properties in the class USER.

Known	Command
The class USER is defined to eTrust AC.	ruler USER props(all)

search

See the find command in this chapter.

setoptions

Purpose

The setoptions command dynamically sets system-wide eTrust AC options related to resource protection. Specifically, use setoptions to enable or disable security checking on a class-by-class basis or for all classes system-wide; to set the password policies; and to list the current settings of the eTrust AC options.

To issue the setoptions command with most parameters, you must have the ADMIN attribute. A user with only the AUDITOR or OPERATOR attribute can, however, execute the setoptions command with the list parameter.

Syntax

```
{setoptions | so}
 [{class+|class-}(class-name...)]
        class-name can be SECLEVEL, PASSWORD or any valid resource
        class in the database.
        Use 'list' command to list all classes in the database
 [accgrr | accgrr-]
 [accpacl | accpacl-]
 [inactive(num-inactive-days) | inactive-]
 [maxlogins(maximum-number-of-logins) | maxlogins-]
 [password(
        [history(number-stored-passwords) | history-]
        [interval(maximum-password-change-interval) | interval-]
        [min_life(minimum-password-change-interval) | min_life-]
        [rules(
                [alpha(minimum-alpha-characters)]
                [alphanum(minimum-alphanumeric-characters)]
                [grace(number-of-grace-logins)]
                [min_len(minimum-password-length)]
                [max_len(maximum-password-length)]
                [lowercase(minimum-lowercase-characters)]
                [max_rep(max-repetitive-characters)]
                [namechk | namechk-]
                [numeric(minimum-numeric-characters)]
                [oldpwchk | oldpwchk-]
                [special(minimum-special-characters)]
                [uppercase(minimum-uppercase-characters)]
                [use_dbdict | use_dbdict-]
                [bidirectional | bidirectional-]
                [prohibited(prohibited-characters)]
        )]
        [rules-]
)]
or:
setoptions list | tngclslist
```

Arguments

accgrr

Specifies that the authority of a user belonging to more than one group is equal to the sum of all the authorities of the groups to which the user belongs. However, if any of the access types is NONE, then NONE always takes precedence over the access types from other groups. When you install eTrust AC, the value of this property is set to yes.

accgrr-

Specifies that eTrust AC does **not** accumulate the group rights of a user when checking access authorizations, but instead assigns the access type of the first group checked to the user. However, if any of the access types is NONE, then NONE always takes precedence over the access types from the other groups.

accpacl

Specifies the accessors and programs that eTrust AC will permit to run a particular resource along with the access type associated with each program.

If explicit access is provided for a user through an ACL, then that access is the allowed access. If explicit access has not been specified through ACL, or access is not specified as NONE, then access rules are a combination of PACL and ACL specifications.

accpacl-

Disables ACCPACL. When ACCPACL is not active, if explicit access is provided for a user through an ACL, then that access is the allowed access. If no explicit access is provided through an ACL, then the allowed access follows the PACL access.

class+(*className*)

Enables one or more eTrust AC classes. A class must be enabled in order for eTrust AC to protect resources of that class. Specify any classes except GROUP, SECFILE, SEOS, UACC, and USER; these protected classes cannot be disabled. A class should be activated only after you have defined the necessary records to allow access to the resources that belong to the class. See the *Administrator Guide* for more information on the resource classes supplied with eTrust AC.

Use one of the following values, and specify the *className* argument in all upper case letters:

- The name of an eTrust AC class.

- SECLEVEL (enables security level checking).
- PASSWORD (activates password quality checking).

class-(*className*)

Disables one or more eTrust AC classes. Resources that belong to a disabled class are not protected by eTrust AC. Use one of the following values, and specify the *className* argument in all upper case letters:

- The name of an eTrust AC class
- SECLEVEL (disables security level checking)
- PASSWORD (disables password quality checking)

The *className* argument **must be written** in all upper case letters.

cng_adminpwd

Enables users with the PWMANAGER attribute to change the ADMIN user's password.

cng_adminpwd-

Disables users with the PWMANAGER attribute from changing the ADMIN user's password. This is the default setting.

cng_ownpwd

Enables users to change their own passwords.

cng_ownpwd-

Disables users from changing their own passwords. This is the default setting.

inactive(*nDays*)

Specifies the number of inactive days after which a user's login is suspended. An inactive day is a day when the user does not log in. Enter a positive integer. If inactive is set to zero, the effect is the same as using the inactive- parameter.

inactive-

Disables the inactive login check.

list

Displays the current values of the password policy.

maxlogins(*nLogins*)

The default maximum number of terminals the user can log in from concurrently. A value of 0 (zero) indicates no maximum and the user can log in from any number of terminals concurrently.

Note: if maxlogins is set to 1, you cannot run selang. You must bring down eTrust AC, change the maxlogins setting to greater than one, and start up eTrust AC again.

This value can be overridden by assigning a value in the user's user record.

maxlogins-

Disables the global maximum logins check. The number of terminals a user can log in from is unlimited, unless the user's login is restricted in the user record of the user.

password

Sets the password options.

history(*NStoredPasswords*)

Specifies the number of previous passwords that are stored in the database. When supplying a new password, the user cannot specify any of the passwords stored in the history list. *NStoredPasswords* is an integer between 1 and 24. If you specify zero, no passwords are saved.

history-

Disables password history checking.

interval(*nDays*)

Sets the number of days that must pass after passwords are set or changed before the system prompts users for a new password.

The value of *nDays* must be a positive integer or zero. An interval of zero disables password interval checking for users. Set the interval to zero if you do not want passwords to expire.

interval-

Cancels the password interval setting.

min_life(*NDays*)

Sets the minimum number of days between password changes. *NDays* must be a positive integer.

min_life-

Disables checking the number of days between password changes.

rules

Sets one or more password rules that eTrust AC uses to check the quality of new passwords. The rules are:

- **alpha(*nCharacters*)**—Sets the minimum number of alphabetic characters the new password must contain. Enter an integer.
- **alphanum(*nCharacters*)**—Sets the minimum number of alphanumeric characters the new password must contain. Enter an integer.
- **grace(*nLogins*)**—Sets the maximum number of grace logins that are permitted before the user is suspended. The number of grace logins must be between 0 and 255.
- **min_len(*nCharacters*)**—Sets the minimum password length. Enter the minimum total number of characters that the new password must contain.
- **max_len(*nCharacters*)**—Sets the maximum password length. Enter the maximum total number of characters that the new password must contain.
- **lowercase(*nCharacters*)**—Sets the minimum number of lowercase characters the new password must contain. Enter an integer.
- **max_rep(*nCharacters*)**—Sets the maximum number of repetitive characters the new password must contain. Enter an integer.
- **namechk**—Checks whether the password contains or is contained by the user’s name. By default, eTrust AC performs this check.
- **namechk**—Turns off this check.

- **numeric(*nCharacters*)**—Sets the minimum number of numeric characters the new password must contain. Enter an integer.
- **oldpwchk**—Checks whether the new password contains or is contained by the password being replaced. By default, eTrust AC performs this check.
- **oldpwchk-** —Turns off this check.
- **special(*nCharacters*)**—Sets the minimum number of special characters the new password must contain. Enter an integer.
- **uppercase(*nCharacters*)**—Sets the minimum number of uppercase characters the new password must contain. Enter an integer.

rules-

Disables password quality checking. None of the rules specified by the rules argument are used for password quality checking.

Examples

The user Mike wants to set a password policy that forces users to supply passwords of length at least 6 characters. Mike also wants to activate password policy enforcement.

Known	Command
The user Mike has the ADMIN attribute.	setoptions password(rules(length(6)))

showfile

Purpose

The showfile command displays the properties of files.

Authorization

In addition to the standard authorization requirements, you can execute a showfile command if at least one of the following conditions is true:

- You have either the AUDITOR or OPERATOR attribute.
- You have the GROUP-AUDITOR attribute in the group that owns the file or that is a parent of the group that owns the file.
- You are assigned read authority in the access control list of the object representing the FILE class record in the ADMIN class.

Notes

- The showfile command lists all the properties of a file record.
- eTrust AC processes each record independently and displays information only for those resources for which you have sufficient authority.

Syntax

```
{showfile | sf} fileName \
    [addprops(propName)] \
    [next] \
    [props(all | propName)] \
    [useprops(propName)] \
    [nt]
```

Arguments

addprops(*propName*)

List of property names. Sets the properties (ruler) to be displayed. The list of properties is added to the current ruler. The ruler is set for this query only, and reverts to the previously set ruler.

fileName

The name of the file record whose properties are to be listed. When listing the properties of more than one file, enclose the list of file names in parentheses and separate the file names with a space or a comma.

You can specify a name pattern to list the properties of all files that match the specified pattern.

eTrust AC processes each file record independently. If an error occurs while processing a file, eTrust AC issues a message and continues processing with the next file in the list.

next(*propName*)

Displays parts of the requested data. This option is useful when the query data is larger than the set query size.

The maximum query size is determined by the query_size token in the lang section of the seos.ini file. The query size default is set at 100.

nt

Displays the Windows file attributes as well as the eTrust AC properties.

props(all|*propName*)

Sets the properties (ruler) to be displayed.

The ruler remains set for future queries.

useprops(*propName*)

Sets the properties (ruler) to be displayed. The current ruler is ignored. The ruler is set for this query only.

See Also

The checklogin, newfile, and rmfile commands in this chapter.

Examples

- User Lyn, who has the ADMIN attribute, wants to list the properties of the file record d:\winnt35\win.ini.

Known	Command
User Lyn has the ADMIN attribute.	showfile D:\winnt35\win.ini

showgrp

Purpose

The showgrp command displays the settings of all the eTrust AC properties of a group record. Optionally, the Windows properties are also shown.

Authorization

In addition to the standard authorization requirements, you can execute a showgroup command if at least one of the following conditions is true:

- You have either the AUDITOR or OPERATOR attribute.
- You have the GROUP-AUDITOR attribute in each group to be listed, or each group to be listed is within the scope of a group in which you have the GROUP-ADMIN attribute.
- You are assigned read authority in the access control list of the object representing the GROUP class record in the ADMIN class.

Syntax

```
{showgrp | sg} groupName \
    [addprops(propName)] \
    [next] \
    [props(all | propName)] \
    [useprops(propName)] \
    [nt]
```

Arguments

addprops(*propName*)
List of property names Sets the properties (ruler) to be displayed. The list of properties is added to the current ruler. The ruler is set for this query only, and reverts to the previously set ruler.

groupName
The name of the group whose properties you want to list. To list the properties of more than one group, enclose the list of group names in parentheses and separate the group names with a space or a comma. You can specify a mask that identifies several groups that have a common name pattern. To list the information contained in all the eTrust AC group records, specify an asterisk (*).

In order to display the properties of a single group whose name contains a special character or space, type a backslash (\) before the special character or space.

next
Display parts of the requested data. This option is useful when the query data is larger than the set query size.

The maximum query size is determined by the query_size token in the lang section of the seos.ini file. The query size default is set at 100.

nt
Shows the group's details from the local Windows system in addition to the properties in the database.

props(all|*propName*)
Sets the properties (ruler) to be displayed. The ruler remains set for future queries.

useprops(*propName*)
Sets the properties (ruler) to be displayed. The current ruler is ignored. The ruler is set for this query only.

See Also

The chgrp/editgrp/newgrp and rmgrp commands in this chapter.

Examples

- The user root wants to display the properties of the security group.

Known	Command
The user root has the GROUP-ADMIN attribute in the security group.	showgrp security

- The user admin wants to display the properties of all eTrust AC groups.

Known	Command
The user admin has the ADMIN and AUDITOR attributes.	showgrp *

showres

Purpose

The showres command displays the properties of resources belonging to classes in the database.

The following classes can be listed using the showres command: ADMIN, CATEGORY, CONNECT, FILE, GHOST, GSUDO, GTERMINAL, HOST, HOSTNET, HOSTNP, SECFILE, SECLABEL, SUDO, SURROGATE, TERMINAL, PROGRAM, PROCESS, TCP, UACC, and any user defined class.

Authorization

In addition to the standard authorization requirements, you can execute a showgroup command if at least one of the following conditions is true:

- You have either the AUDITOR or OPERATOR attribute.
- You have the GROUP-AUDITOR attribute in the group that owns the resource or that is a parent of the group that owns the resource.
- You are assigned read authority in the access control list of the object representing the resource class record in the ADMIN class.

Notes

- The showres command lists all the properties of an existing resource or resource group record. For a list of all the properties of the eTrust AC classes, see the chapter “eTrust Environment Classes and Properties” in this guide.

  For a list of all properties of the Windows resource types, see the chapter “Windows Environment Classes and Properties” in this guide.
- eTrust AC processes each resource independently and displays information only for those resources for which you have sufficient authority.

Syntax

```
{showres | sr} className resourceName \
    [addprops(propName)] \
    [next] \
    [props(all | propName)] \
    [useprops(propName)]
```

Arguments

addprops(*propName*) Sets the properties (ruler) to be displayed. The list of properties is added to the current ruler. The ruler is set for this query only, and reverts to the previously set ruler.

className The name of the class to which the resource belongs. To list the resource classes defined to eTrust AC, use the find command. For more information, see the find command in this chapter.

next Display parts of the requested data. This option is useful when the query data is larger than the set query size.

The maximum query size is determined by the query_size token in the lang section of the seos.ini file. The query size default is set at 100.

props(all|*propName*) Sets the properties (ruler) to be displayed. The ruler remains set for future queries.

resourceName The name of the resource record whose properties are to be listed. When listing the properties of more than one resource, enclose the list of resource names in parentheses and separate the resource names with a space or a comma.

You can specify a name pattern to list the properties of all resources that match the specified pattern. To display the properties of all the resources defined to the specified class, specify an asterisk (*). In order to display the properties of a single resource whose name contains a special character or space, type a backslash (\) before the special character or space.

eTrust AC processes each resource record independently. If an error occurs while processing a resource, eTrust AC issues a message and continues processing with the next resource in the list.

useprops(*propName*) Sets the properties (ruler) to be displayed. The current ruler is ignored. The ruler is set for this query only.

See Also

The chres/editres/newres and rmres commands in this chapter.

Examples

The user Admin1 wants to list the properties of the records whose names match the mask ath* in the TERMINAL class.

Known	Command
User Admin1 has the ADMIN and AUDITOR attributes.	showres TERMINAL ath*

showusr

Purpose

The showusr command lists the values of all the properties contained in an eTrust AC user record. If you enter the showusr command without specifying *userName* or *mask*, eTrust AC lists the information from your own user record.

Authorization

In addition to the standard authorization requirements, you can execute a showgroup command if at least one of the following conditions is true:

- You have either the AUDITOR or OPERATOR attribute.
- You have the GROUP-AUDITOR attribute in the group that owns the user record or that is a parent of the group that owns the user record.
- You are assigned read authority in the access control list of the object representing the USER class record in the ADMIN class.

Syntax

```
{showusr | su} userName \
    [addprops(propName)] \
    [next] \
    [props(all | propName)] \
    [useprops(propName)] \
    [nt]
```

Arguments

addprops(*propName*) Sets the properties (ruler) to be displayed. The list of properties is added to the current ruler. The ruler is set for this query only, and reverts to the previously set ruler.

userName	The name of the user record. When listing the properties of more than one user record, enclose the list of user names in parentheses and separate the user names with a space or a comma. In order to display the properties of a single user whose name contains a special character or space, type a backslash (\) before the special character or space. You can specify a name pattern to identify a group of users with similar record names. For example, to list all users whose names begin with A, specify A*.
nt	Shows the user details from the local Windows system in addition to the properties in the database.
props(all | *propName*)	Sets the properties (ruler) to be displayed. The ruler remains set for future queries.
userName	The name of the user record. When listing the properties of more than one user record, enclose the list of user names in parentheses and separate the user names with a space or a comma. In order to display the properties of a single user whose name contains a special character or space, type a backslash (\) before the special character or space. You can specify a name pattern to identify a group of users with similar record names. For example, to list all users whose names begin with A, specify A*.
useprops(*propName*)	Sets the properties (ruler) to be displayed. The current ruler is ignored. The ruler is set for this query only.

Examples

- The user root wants to list the properties of Robin's user record.

Known	Command	Defaults
The user Robin is defined to eTrust AC.	showusr Robin	UserName=root (*the user name of the person executing the showusr command*.)

- The user root wants to list the user properties of the users Robin and Leslie.

Known	Command
The root has the ADMIN and AUDITOR attributes.	showusr (Leslie, Robin)

See Also

The chusr/editusr/newusr and rmusr commands in this chapter.

source

Purpose

The source command allows you to execute one or more selang commands that have been placed in a file. eTrust AC reads the specified file, executes the commands, and returns an selang prompt. Any user defined in the eTrust AC database can use this command.

This command is like the source command in csh and tcsh in UNIX.

Syntax

`source` *fileName*

Arguments

fileName The name of the file that contains the selang commands.

Example

The user admin wants to execute the commands in the file called initf1. The user enters the following command:

```
source initf1
```

Chapter 3 selang Commands in the Windows Environment

This chapter contains a complete reference to all the selang commands available in the Windows (Native) environment of the selang command shell, arranged alphabetically. When working in the Windows environment, you use the selang commands to add, delete, modify, and list the users and groups in the local Windows host. You can also modify and list the Windows file permission (NTFS file systems only) and ownership settings. See the chapter "The selang Command Language" for general information about the different selang environments, getting help, command syntax, and overall organization of the commands.

authorize

Purpose

The authorize command maintains the lists of users and groups authorized to access a particular resource. Using authorize, you can change a list to:

- Permit access to a resource for specific eTrust AC users or groups.
- Block access to a resource for specific eTrust AC users or groups.
- Change the level of access authority to a resource for specific users or groups.

The authorize- command removes the access authority to a resource by deleting the accessors from the standard access control list. This leaves the default access to determine accessors' ability to access a particular resource.

The following Windows environment classes support ACLs, and can be controlled by the authorize command.

- COM
- DISK
- FILE
- PRINTER

- REGKEY
- SHARE

Classes that do not appear in the list have no access control lists and cannot be controlled by the authorize command.

Syntax

```
{authorize | auth} className resourceName     \
    access(accessValue)                       \
    [gid(groupName, ...) ]                    \
    [uid(userName, ...)]


authorize | auth} className resourceName \
    [deniedaccess(accessvalue)]

{authorize- | auth-} className resourceName   \
    [gid(groupName, ...) ]                    \
    [uid(userName, ...)]
```

Arguments

access(*accessValue*)

Specifies the access authority you want the accessors you identify in the uid or gid parameters to have to the resource.

Valid values for *accessValue* depend on the resource type, as follows:

- **COM** and **DISK**—all, change, changepermissions, delete, none, read, takeownership, and write
- **FILE**—all, change, chmod, chown, control, delete, execute, none, read, sec, write, and update

  Note: For FILE resources, it is only possible to define access authorities for NTFS files; FAT files cannot have access authorities.
- **PRINTER**—all, none, manage, and print
- **REGKEY**—all, append, chown, create, delete, enum, link, manage, none, notify, query, read, readcontrol, sec, set, subkey, and write
- **SHARE—**all, change, read, and none

className

Specifies the name of the class to which *resourceName* belongs.

deniedaccess(*accessvalue*)

Specifies the negative access authority that you want accessors, who you identify in the uid or gid parameters, to have to the resource.

The denied *accessvalue* can be: all, create, delete, join, modify, none, password, or read.

Note: You can only use *accessValue* with the authorize command, not with authorize-.

gid(*groupName*)
: Specifies the Windows group or groups whose access authority to the resource you are setting. The value *groupName* represents the name of one or more Windows groups. When specifying more than one group, separate the group names with a space or a comma.

resourceName
: The name of the resource record to modify or add. When changing or adding more than one resource, enclose the list of resource names in parentheses and separate the resource names with a space or a comma. At least one resource name must be specified.

eTrust AC processes each resource record independently in accordance with the specified parameters. If an error occurs while processing a resource, eTrust AC issues a message and continues processing with the next resource in the list.

uid(*userName*)
: Specifies the Windows users whose access authority to the resource you are setting. *userName* is the user name of one or more Windows users. When specifying more than one user, separate the user names with a space or a comma. To specify all users who are defined in Windows, specify an asterisk (*) for *userName*.

chfile / editfile

Purpose

The chfile and editfile commands are identical. They modify one or more records in the FILE class.

Syntax

For NTFS file systems:

```
{chfile | cf | editfile | ef} fileName | (fileNames...)  \
    [attrib(attributeValue)]            \
    [attrib(-attributeValue)]
    [defaccess(accessValue)]            \
    [owner(userName or groupName)]
```

For FAT file systems:

```
{chfile | cf | editfile | ef} fileName | (fileNames...)  \
    [attrib(attributeValue)]             \
    [attrib(-attributeValue)]
```

Arguments

attrib(*attributeValue*)

Specifies a set of attributes that determine the character of the file. When a minus sign (–) precedes the argument *value*, this parameter removes the attribute. See the appendix "Windows Values" for a list of Windows file attributes.

defaccess(*accessValue*)

Specifies the access authority for the Native security built-in group Everyone. All the system users are members of the Everyone group. Providing access to the Everyone group covers all the potential anonymous users in addition to all authenticated users.

Note: Defaccess for an object defined in the eTrust AC environment has a different meaning; the default access authority is the authority granted to any accessor who is not in the resource's eTrust AC list who requests access to the resource. The default access also applies to users not defined in eTrust AC.

The defaccess parameter applies only to NTFS file systems.

owner(*userName*|*groupName*)

Assigns a user or group as the owner of the file record. The owner of the file record has unrestricted access to the file. The owner of the file may always update or delete the file record.

Generic File Protection

Generic file protection enables you to apply a particular access rule to all the files that fit a specified file name pattern (regular expression). The generic access rule protects any file resource with a name matching that wildcard pattern. Should a resource match more than one generic access rule, eTrust AC uses the closest of the matches for that resource.

With generic file protection, you do not need to define more than a handful of security rules in order to protect most of the files that need protection in a Windows system.

eTrust AC, however, does *not* accept the following patterns:

- *
- \tmp*
- \etc*

Note: If more than one file name is specified, eTrust AC processes each file record independently in accordance with the specified parameters. If an error occurs while processing a file, eTrust AC issues a message and continues processing with the next file in the list.

See also

The showfile command in this chapter.

chgrp / editgrp / newgrp

Purpose

The newgrp command defines a new Windows group by adding a record for the new group to the Windows database.

The chgrp command changes the definition of a Windows group. If the group is also defined to eTrust AC, the chgrp command can be used to change the group's eTrust AC definition. You can change the definition of more than one group with a single chgrp command.

The editgrp command either adds a new group to the database like the newgrp command or changes the definition of an existing Windows group like the chgrp command.

When defining more than one group or changing the properties of more than one group, enclose the list of group names in parentheses and separate the group names with a space or a comma.

Note: To add or remove members from a group use the join or join- command.

Syntax

```
{chgrp | cg | editgrp | eg | newgrp | ng} (groupName) | (groupNames...) | \
(~groupName) | ( ~groupNames) \
[global] \
[comment(string) | comment- ] \
[privileges(privList)]   \
[privileges(-privList)]   \
[rename_group]
```

Arguments

comment(*string*)

Adds an alphanumeric comment string of up to 255 characters to the group record. If you previously added a comment string to the group record, the new string specified here replaces the existing string. If the string contains any blanks, enclose the entire string in single quotation marks.

Standard Windows groups have a descriptive comment added on system installation. If you create a new group in both the Windows and eTrust environments, eTrust AC inserts the comment “eTrust Group.”

global

Indicates a global group. Each group name must be unique and cannot currently exist in the Windows database. Windows does not allow groups and users to share the same name.

Note: Use ~*groupName* when you create global groups and use the services of eTrust AC version 4.1. Version 4.1 and above support this format for backward compatibility.

groupName

For the command newgrp, specifies the name of the group record added to the database. Each group name must be unique and must not currently exist in the Windows database. Unlike the eTrust database, Windows does not allow groups and users to share the same name.

For the command chgrp, specifies the name of the group whose properties you are changing.

When defining more than one group or changing the properties of more than one group, enclose the list of group names in parentheses and separate the group names with a space or a comma.

privileges(*privList* | –*privList*)

Adds specific rights to the Windows group record or, when privList is preceded by a minus sign (–), removes the specified rights. Valid values are any of the privileges available in native Windows.

You can specify this parameter only with the chgrp or editgrp command, and only when you are changing an existing group record. You cannot use it to assign privileges when you are creating a new group record. See the appendix “Windows Values” for a list of Windows privileges.

rename_group

Renames the group account in the Windows database. All the properties of the old group name apply to the renamed group account. Each group name must be unique and must exist in the Windows database. Unlike the eTrust AC database, Windows does not allow groups and users to share the same name.

Note: When eTrust AC is installed on Windows 2000 with Active Directory, eTrust AC renames the pre-Windows 2000 group name.

See Also

The rmgrp, showgrp and join commands in this chapter.

chres / editres / newres

Purpose

The newres command defines a new resource to an eTrust AC class. The chres command modifies one or more resource records that belong to an eTrust AC class. The editres command either defines a new resource or modifies an existing resource.

Syntax

```
{chres | cr | editres | er | newres | nr}         \
    className resourceName | (resourceNames...)    \
    [comment(string) | comment-]            \
    [defaccess(accessValue)]                \
    [dword(integer)|string(string)|binary(hexastring)|multistring(string)]     \
    [location(string) | location()] \
    [maxusers(integer)]                    \
    [owner(userName | groupName)]
    [share_name(string) | sharename-]     \

{chres | cr | editres | er | newres | nr}     \
    DOMAIN resourceName | (resourceNames...)    \
    [computer(workstationName) | computer-(workstationName)]\
[domainpwd(connectPassword)]                \
    [trusted(domainName) | trusted-(domainName)]
```

Arguments

binary(*hexastring*)

Specifies the value of a registry key when it is a hexadecimal.

className

Specifies the name of the class to which *resourceName* belongs.

For the newres command, valid values are: REGKEY, REGVAL, OU, and SHARE. For the chres and editres commands, valid values are: COM, DISK, DOMAIN, FILE, PRINTER, REGKEY, REGVAL, SERVICE, DEVICE, SESSION, OU, and SHARE.

comment(*string*)
Adds a comment string to the resource record. If you previously added a comment string to the resource record, the new string specified here replaces the existing string. This parameter is valid for SHARE and PRINTER resources only.

computer(*workstationName*)|computer-(*workstationName*)
Specifies the name of the workstation you are adding to the domain, or, when a minus sign precedes the argument, the name of the workstation you are removing from the domain. This parameter can only be used with DOMAIN resources. You can specify this parameter only with the chres or editres command.

defaccess(*accessValue*)
Specifies the access authority for the Native security built-in group Everyone. All the system users are members of the Everyone group. Providing access to the Everyone group covers all the potential anonymous users in addition to all authenticated users.

Note: Defaccess for an object defined in the eTrust AC environment has a different meaning; the default access authority is the authority granted to any accessor who is not in the resource's eTrust AC list who requests access to the resource. The default access also applies to users not defined in eTrust AC.

The defaccess parameter applies only to NTFS file systems.

domainpwd(*connectPassword*)
Specifies the password an administrator must enter when changing trust relationships.

This parameter can only be used with DOMAIN resources. You can specify this parameter only with the chres or editres command.

dword(*integer*)
Specifies the value of a registry key when it is an integer.

gen_prop(*propertyName*)
Specifies the property for the OU class.

This parameter is valid for the OU class only.

gen_value(*valueName*)
Specifies the property value for the OU class.

This parameter is valid for the OU class only.

location(*string*)
Indicates the location of a printer. Use ( ) with blanks to remove this property.

This parameter is valid for PRINTER resources only.

maxusers(*integer*)
Specifies the maximum number (*integer*) of users that can connect to a shared directory at one time.

This parameter is valid for SHARE resources only.

multistring(*string*)
Specifies the value of a registry key when it is a multistring.

owner(*userName*|*groupName*)
Assigns a user or group as the owner of the resource record. The owner of the resource record has unrestricted access to the resource. The owner of the resource is always permitted to update and delete the resource record. For more information, see the *Administrator Guide*.

For FILE or SHARE records on a FAT file system, you may not specify the owner parameter. This parameter is also not valid for DEVICE, DOMAIN, OU, PROCESS, REGVAL, SERVICE, and SESSION resources.

resourceName
The name of the resource record to modify or add. When changing or adding more than one resource, enclose the list of resource names in parentheses and separate the resource names with a space or a comma. At least one resource name must be specified.

eTrust AC processes each resource record independently in accordance with the specified parameters. If an error occurs while processing a resource, eTrust AC issues a message and continues processing with the next resource in the list.

share_name(*shareName*) | share_name-
Identifies the share point for a printer.

This parameter is valid for PRINTER resources only.

string(*string*)
Specifies the value of a registry key when it is a string.

trusted(*domainName*)|trusted-(*domainName*)
Specifies the name of the domain you are adding to trusted domains, or, when a minus sign precedes the argument, the name of the domain you are untrusting. This parameter can only be used with DOMAIN resources. You can specify this parameter only with the chres or editres command.

chusr / editusr / newusr

Purpose

The newusr command defines one or more new users to the Windows system. The chusr command modifies the definition of one or more users in the Windows system. The editusr command can define a new user or change the properties of an existing user.

Syntax

```
{{chusr | cu | editusr | eu | newusr | nu} userName    \
    [comment(string) | comment- ]   \
    [country(string)]   \
    [expire | expire(mm/dd/yy[@hh:mm]) | expire-]  \
    [flags(accountFlags) | -(accountFlags)]  \
    [fullname(fullName)]    \
    [homedir(homeDir)]   \
    [homedrive(homeDrive)]    \
    [location(string)]    \
    [logonserver(serverName)]    \
    [organization(name)]    \
    [org_unit(name)]    \
    [password(password)]    \
    [pgroup(primaryGroup)]    \
    [phone(string)]    \
    [privileges(privList)]    \
    [profile(path)]    \
    [restrictions(days( day-data ) time(hh:hh | anytime) )]\
      day-data: {[mon] [tue] [wed] [thu] [fri] [sat] [sun]} | anyday | weekdays \
    [rename_user]
    [restrictions-]    \
    [resume[(date)] | resume-} \
    [script(logonScriptPath)]    \
    [suspend[(date)] | suspend-] \
    [terminals(terminalList) | terminals-(terminalList)]   \
    [workstations(workstationList)|workstations-(workstationList)|workstations-]
```

Arguments

comment(*string*) | comment-

Assigns a comment string to the user record.

The argument is an alphanumeric string of up to 255 characters. If the string contains any blanks, enclose the entire string in single quotation marks.

country(*string*)

Specifies the country where the user is located. This string is not used during the authorization process.

The argument is an alphanumeric string of up to 19 characters. If the string contains any blanks, enclose the entire string in single quotation marks.

expire | expire(*mm/dd/yy[@hh:mm*) | expire-

Sets the date on which the user's account expires. If a date is not specified, the user account expires immediately, provided the user is not currently logged in. If the user is logged in, the account expires when the user logs out.

expire- with the newusr command defines a user account that does not have an expiration date. For the chusr and editusr commands, it removes an expiration date from the specified user account.

The date argument takes the format: *mm*/*dd*/*yy* [@*hh*:*mm*].

flags(*accountFlags* | – *accountFlags*)

Specifies particular attributes of a user's account. See the appendix "Windows Values" for a list of valid flag values.

To remove flags from the user record, precede *accountFlags* with a minus (–).

fullname(*fullName*) Specifies the full name of the user associated with the user record.

The argument is an alphanumeric string of up to 48 characters. If the string contains any blanks, enclose the entire string in single quotation marks.

homedir(*homeDir*) Specifies the user's home directory. Users log in automatically to their own home drives and home directories.

homedrive(*homeDrive*) Specifies the drive of the user's home directory. Users log in automatically to their own home drives and home directories.

location(*string*) Specifies the user's location. This string is not used during the authorization process.

The argument is an alphanumeric string of up to 19 characters. If the string contains any blanks, enclose the entire string in single quotation marks.

logonserver(*serverName*)

Specifies the server that verifies the login information for the user. When the user logs in to the domain workstation, eTrust AC transfers the login information to the server, which gives the workstation permission for the user to work.

organization(*name*) Specifies the organization in which the user works. This information is not used during the authorization process.

The argument is an alphanumeric string of up to 19 characters. If the string contains any blanks, enclose the entire string in single quotation marks.

org_unit(*name*) Specifies the organizational unit in which the user works. This information is not used during the authorization process.

The argument is an alphanumeric string of up to 19 characters. If the string contains any blanks, enclose the entire string in single quotation marks.

password(*password*)

Assigns a password to a user. If password checking is enabled, the password is valid for one login only. When the user next logs in to the system, a new password must be set.

The argument is a string of up to 14 characters, and cannot include either a space or a comma. If password checking is enabled, the password is valid for one login only. When the user next logs in to the system, the user must set a new password, unless you set the flag for “Password Never Expires”. You cannot change your own password using the chusr or editusr command, even if you have the ADMIN attribute or are a member of the eTrust AC Admins group.

If you are setting passwords for users on Windows NT systems, the following message may appear:

```
The password is shorter than required.
```

This error means that the password does not meet the policy requirements. This is caused by any of the following:

- The password is shorter or longer than the required length.
- The password has been used recently and exists in the Windows NT Change History field.
- The password does not have enough unique characters.
- The password does not meet other password policy requirements (such as those set with eTrust AC password policies).

To avoid this error, make sure you set a password which meets all applicable requirements.

pgroup(*primaryGroup*)

Sets the user’s primary group ID. A primary group is one of the groups in which a user is defined and must be a Global group.

The argument is a string of up to 14 characters, and cannot include either a space or a comma.

phone(*string*)

Specifies the user’s phone number. This information is not used during the authorization process.

privileges(*privList*)

Adds specific rights to the Windows user record or, when *privList* is preceded by a minus sign (–), removes the specified rights. You can specify this parameter only with the chusr or editusr command, and only when you are changing an existing user record. You cannot use it to assign privileges when you are creating a new user record.

See the appendix “Windows Values” for a list of Windows privileges.

profile(*path*)

Specifies the full path location of the file that contains a user's profile for the Desktop environment (program groups, network connections). Every time the user logs in to any workstation, the same environment appears on the screen.

rename_user

Renames the user account in the Windows database. All the properties of the old user name apply to the renamed user account. Each user name must be unique and must exist in the Windows database. Unlike the eTrust AC database, Windows does not allow groups and users to share the same name.

Note: When eTrust AC is installed on Windows 2000 with Active Directory, eTrust AC renames the user logon name (the pre-Windows 2000 user name). However, eTrust AC does not rename the full name as Windows does.

Note: The maximum length of an object name is 255 characters. eTrust AC and Windows do not manage resources with names exceeding 255 characters.

restrictions([*days*] [*time*])|restrictions-([*days*] [*time*])

Specifies the days of the week and the hours in the day when users may access the file.

If you omit the days argument and specify the time argument, the time restriction applies to any day-of-week restriction already indicated in the record. If you omit time and specify days, the day restriction applies to any time restriction already indicated in the record. If you specify both days and time, the users may access the system only during the specified time period on the specified days.

- [Days] specifies the days on which users may access the file. The days argument takes the following sub-arguments:
  - **anyday**—Allow users access to the file on any day.
  - **weekdays**—Allow users access to the resource only on weekdays—Monday through Friday.
  - **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, **Sun**—Allow users access to the resource only on the specified days. You can specify the days in any order. If you specify more than one day, separate the days with a space or a comma.
- [Time] specifies the period during which users may access the resource. The time argument takes the following sub-arguments:
  - **anytime**—Allow users access to the resource at any time of the day.

- **startTime:endTime**—Allow access to the resource only during the specified period. The format of both startTime and endTime is *hhmm*, where *hh* is the hour in 24-hour notation (00 through 23) and *mm* is the minutes (00 through 59). Note that 2400 is not a valid time value. startTime must be less than endTime, and both times must occur on the same day. If the terminal is in a different time zone from the processor, adjust the time values by translating the start and end times for the terminal to the equivalent local times for the processor. For example, if the processor is in New York and the terminal is in Los Angeles, to allow access to the terminal from 8:00 a.m. to 5:00 p.m. in Los Angeles, specify time (1100:2000).

resume(*date*) | resume-

The date, and optionally time, on which Windows will reinstate the user account.

Enter a date, and optional time, in the following format: *mm /dd/yy[@HH:MM]*.

Use resume- parameter to change the status of the user account from active (enabled) to suspended. Use this parameter with the chusr or editusr commands only.

script(*loginScriptPath)*

Specifies the location of a file that runs automatically when the user logs in. This login script configures the working environment. This parameter is optional, since the profile parameter also sets up the user's working environment.

suspend(*date*) | suspend-

Disables a user account. A user cannot use a suspended user account to log in to the system. If you specify date, Windows suspends the user account on the specified date. If you omit a date, Windows suspends the user account immediately upon execution of the chusr command.

Enter a date, and optional time, in the following format: *mm /dd/yy[@HH:MM]*.

Use the suspend- parameter to change the status of the user account from disabled to active (enabled). Use this parameter with the chusr or editusr commands only.

terminals(*terminalList*) | terminals-(*terminalList*)

Specifies up to eight terminals from which the user can log in. Surround the list with quotation marks, and separate the names with commas. For example:

```
“terminal1,terminal2”
```

workstations(*workstationList*) | workstations-(*workstationList*) | workstations-

Specifies up to eight workstations from which the user can log in. Surround the list with quotation marks, and separate the names with commas. For example:

```
“workstation1,workstation2”
```

See Also

The rmusr, showusr and join commands in this chapter.

environment

Purpose

The environment command sets the security environment. eTrust AC supports the eTrust AC, Windows, and UNIX security environments. When the selang command shell is invoked, the eTrust environment is selected by default.

Syntax

```
{environment | env} {etrust | native | nt |pmd | seos | unix}
```

Arguments

eTrust

Specifies the eTrust security environment. The selang commands affect the eTrust database. Some commands support simultaneous updates to the native OS security settings of the host you are connected to. In the eTrust environment, the selang prompt is: `eTrust>`

native

Specifies that the commands you enter affect the database in the native environment (either Windows or UNIX) of the host you are connected to, whether local or remote. In the native environment, the selang prompt is: `eTrust(native)>`

nt

Specifies the Windows security environment. The selang commands affect the Windows database. Some commands support simultaneous updates to the eTrust security settings. In the Windows environment, the selang prompt is: `eTrust(nt)>`

pmd

Specifies the selang commands in the remote management environment. When the selang command shell is set to the pmd environment, the selang commands operate on the PMDB of the selected host. In the pmd environment, the selang prompt is: `eTrust(pmd)>`

seos

Specifies the eTrust security environment. This parameter is maintained for compatibility with older versions. The selang prompt is: eTrust>

unix

When connected to a remote UNIX host, specifies that commands you enter affect the UNIX database. In the UNIX environment, the selang prompt is: eTrust(unix)>

find

Purpose

The find command lists the classes in the environment. Used with the parameter *className*, it lists the names of all records in a specified Windows environment class. Used with the parameter "file," the command lists all the files that match the mask, which is a string.

Note: This usage of the file parameter is different than in the eTrust environment.

The find command cannot be used with the SEOS class.

Syntax

```
{find | f} [{className | class(className)} | className(memberName) | objMask ]  \
            file \[directory][\mask]
```

Arguments

class(*className*) The name of any valid class in the Windows environment except SEOS.

className(*memberName*) The name of a member of a class. Enclose multiple entries in parentheses and separate them with a space or comma.

objmask Lists all objects in the specified class that match the specified object mask. Indicate an object mask by using wildcards.

file \directory\ List all the files in the directory *directory*.

\directory\mask List all the files in the directory *directory* that match the *mask* variable. The *mask* should include wildcard characters.

Wildcard Matching

selang supports the following wildcard characters:

Character	Matches
* (asterisk)	Any sequence of zero or more characters.
? (question mark)	Any single character.

To make a single character a “do not care” character that matches any other single character, use a question mark (?), as in the following examples:

Specify this...	To do this...
mmc?	mmc3, mmcx, mmc5
mmc?.t	mmc1.t, mmc2.t
mmc04.?	mmc04.a, mmc04.1

To match any string of zero or more characters, use an asterisk (*), as in the following examples:

Specify this...	To do this...
i.c	main.c, list.c
st*.h	stdio.h, stdlib.h, string.h
*	All records of the specified class

help

Purpose

Displays help for selang commands in the Windows environment.

Syntax

```
{help | h | ?} [command-name | access | privileges ]
```

Arguments

command-name

Displays the syntax for the specified command.

access

Displays a class-by-class list of the access types that the access and defaccess parameters can specify.

privileges

Displays a list Windows privileges that can be used with the chgrp, editgrp, chusr, and editusr commands.

history

Purpose

Lists the previously entered commands. See the description in the chapter “The selang Command Language” in this guide.

Syntax

```
history
```

join

Purpose

The join command adds users to a group. The join- command removes users from a group. The specified users and group must already be defined to Windows.

Authorization

In addition to the standard authorization requirements (see Authorization in the chapter “The selang Command Language”), note that **both** the MODIFY and JOIN properties are required if an administrator is to have the authority to modify eTrust AC GROUP records and Windows groups.

Syntax

```
{join | j} userName group(groupName)
{join- | j-} userName group(groupName)
```

Arguments

group(*groupName*)

Specifies the group to which the users are being joined, or from which they are being removed. The argument *groupName* must be the name of an existing Windows group.

userName

The user name of the Windows user who is being connected to, or removed from, the group specified by the group parameter. When specifying more than one user, enclose the user names in parentheses and separate the user names with a space or a comma.

See Also

The chgrp, rmgrp and showgrp commands in this chapter.

list

Purpose

Lists the classes in the environment. With the parameter *className*, lists the names of all records in a specified Windows environment class. With the parameter “file,” Lists the files in a directory that match a mask. This command is the same as the find command. For detailed description, see the find command in this chapter.

Syntax

```
list {[className] | file \[directory][\mask]}
```

See Also

The find command in this chapter.

rmgrp

Purpose

The rmgrp command deletes one or more groups from the Windows system database.

Syntax

```
{rmgrp | rg} groupName
```

Argument

groupName The name of the group to be deleted. The group name must be an existing Windows group name. Specify one or more group names. When removing more than one group, enclose the list of group names in parentheses and separate the group names with a space or a comma.

See Also

The chgrp, newgrp, and showgrp commands in this chapter.

rmres

Purpose

The rmres command removes one or more resources from the Windows system database.

Syntax

```
{rmres | rr} className resourceName
```

Arguments

className

The name of the class the resource belongs to.

resourceName

The name of an existing Windows resource of class *className*. When removing more than one resource, enclose the list of user names in parentheses and separate the names with a space or a comma.

See Also

The chres, newres, and showres commands in this chapter.

rmusr

Purpose

The rmusr command removes one or more users from the Windows system database.

Syntax

```
{rmusr | ru} userName
```

Argument

userName The user name of an existing Windows user. When removing more than one user, enclose the list of user names in parentheses and separate the user names with a space or a comma.

See Also

The chusr, newusr, and showusr commands in this chapter.

search

Purpose

This command is the same as the find command. For detailed description, see the find command in this chapter.

Syntax

```
search {[className] | file \[directory][\mask]}
```

See Also

The find command in this chapter.

showfile

Purpose

The showfile command lists the details of one or more files. You may display details for multiple files by listing their names separately, or by using wildcards.

Syntax

```
{showfile | sf} fileName
```

Argument

fileName The full path and name of the file whose details are to be listed. Enter one or more Windows file names. When specifying more than one file, enclose the list of file names in parentheses and separate the individual names with a space or a comma.

See Also

The chfile command in this chapter.

showgrp

Purpose

The showgrp command displays the details of one or more Windows groups.

Syntax

```
{showgrp | sg} groupName
```

Argument

groupName The name of the group whose details are to be displayed. The group name must be an existing Windows group name. Specify one or more group names. When listing more than one group, enclose the list of group names in parentheses and separate the group names with a space or a comma.

See Also

The chgrp, newgrp, rmgrp commands in this chapter.

showres

Purpose

Displays the properties of Windows resources.

Syntax

```
{showres | sr } className resourceName
```

Arguments

className The name of the class the resource belongs to.

resourceName The name of an existing Windows resource of class *className*.

showusr

Purpose

The showusr command displays the properties of one or more Windows users.

Syntax

```
{showusr | su} userName
```

Argument

userName The name of the user whose Windows properties are to be displayed. Specify an existing Windows user name. When listing the properties of more than one user, enclose the list of user names in parentheses and separate the names with a space or a comma.

See Also

The chusr, newusr, and rmusr commands in this chapter.

xaudit

Purpose

The xaudit command adds entries in the system access control list (SACL). Each entry in this list causes an audit message to be logged when a specified user or group attempts to gain access to the resource. The xaudit- command removes entries from the SACL, and is valid for resource types FILE, PRINTER, REGKEY, DISK, COM, or SHARE.

Syntax

```
xaudit className, resourceName \
[failure(auditMode)]    \
[gid(groupName)] \
[success(auditMode)] \
[uid(userName)]
```

```
xaudit- className, resourceName \
     [gid(groupName)] \
     [uid(userName)]
```

Argument

className

The name of the resource type to which the resource belongs.

failure(*auditMode*)

Logs unauthorized access attempts to the resource.

Valid values for *auditmode* depend on the resource type to which it belongs:

Note: Only NTFS files can have audit modes

- DISK and COM: changePermissions, delete, modify, query, read, synchronize, takeOwnership.
- FILE: changePermissions, delete, execute, read, takeOwnership, and write.
- PRINTER: changePermissions, delete, print, and takeOwnership.
- REGKEY: delete, enumerate, link, notify, queryValue, readControl, setValue, subkey, and write.

For all resource types: **none** and **all**.

gid(*groupName*)

Specifies the groups or groups whose access to the resource is being audited. When specifying more than one group, separate the names with spaces or commas.

resourceName

Specifies the name of the resource record whose system access control list (SACL) is being modified.

success(*auditMode*)

Logs authorized accesses to the resource.

Valid values for *auditmode* depend on the resource type to which it belongs:

Note: Only NTFS files can have audit modes

- DISK and COM: changepermissions, delete, modify, query, read, synchronize, takeownership.
- FILE: changePermissions, delete, execute, read, takeOwnership, and write.
- PRINTER: changePermissions, delete, print, and takeOwnership.
- REGKEY: delete, enumerate, link, notify, queryValue, readControl, setValue, subkey, and write.

For all resource types: **none** and **all**.

uid(*userName*)

Specifies the user whose access to the resource is being audited. When specifying more than one user, separate the user names with spaces or commas. To specify all users who are defined in the Windows NT database, specify an asterisk (*) for *userName*.

Chapter
4

selang Commands in the Policy Model Environment

This chapter provides a detailed reference to all the commands available in the pmd environment of the selang command shell. Remote management of Policy Models lets you administer subscribers, truncate the update file, and manage the Policy Model error file. See the chapter “The selang Command Language” for general information about the different selang environments, getting help, command syntax, and overall organization of the commands.

findpmd

Purpose

The findpmd command lists the PMDBs in the host to which you are connected.

Syntax

```
findpmd
```

listpmd

The listpmd command lists information about the PMDB and its subscribers, update file, and error log. If no options are used, the command lists all subscribers of the Policy Model *pmdName.*

```
listpmd pmdName   \
[cmd(offset)]   \
[errors|all_errors[next(N)]]   \
[info]   \
[subscriber(subNames)]
[log]
```

Arguments

cmd**(***offset)*

Displays all commands in the update file and their offsets.

The offset indicates the location of the update inside the file. If an offset is specified, the list starts from offset. If no offset is specified, the display begins from the beginning of the update file.

errors|all_errors [next(*N*)]

Displays the Policy Model error log. The errors parameter displays all types of errors except non-connection failure errors. all_errors displays all errors.

If next is specified, eTrust AC displays the next *N* number of errors, where *N* is the value of query_size in the registry subkey: HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrustAccessControl\lang.

info

Displays general information about the Policy Model pmdName, including whether the Policy Model has a parent.

subscriber(*subNames*)

Lists the subscribers of the Policy Model and their status, including number of errors, availability, offset, and the next command to be propagated. The subNames parameter lets you select a subset of subscribers.

The listpmd command lists information about the PMDB and its subscribers, update file, and error log.

log

Displays the policy model general log file.

Comments

The update file contains updates that must be, or have been, propagated by the Policy Model. The offset indicates the location of the next update that must be sent to a subscriber. The update file’s initial and latest offsets are displayed.

pmd

Purpose

The pmd command clears the Policy Model error log, updates the subscriber list, starts and stops the Policy Model service, and truncates the update file.

```
pmd pmdName  {                   \
     backup                      \
     operation                   \
    [{clrerr|clrerror}]          \
    [killog]                     \
    [release(subName)]           \
    [reloadini]                  \
    [startlog]                   \
    [start]                      \
    [stop]                       \
        [{trunc|truncate}(offset)] }
```

Arguments

backup

Moves the Policy Model to backup status.

clrerror|clrerr

Clears the Policy Model error log.

killlog

Disables the Policy Model general log file.

Warning: Do not use the kill command to shut down the PMDB service.

operation

Moves the Policy Model from backup to operational status.

release(*subName*)

Removes the subscriber specified by *subName* from the list of unavailable subscribers. This means that the subscriber can receive updates immediately. *subName* specifies the subscriber that is to become available for update.

reloadini

Rereads the Policy Model pmd.ini file and the seos.ini file, enabling values of certain tokens to change without having to reload the Policy Model service.

startlog

Enables the Policy Model general log file for writing.

start

Starts the eTrust AC Policy Model service. Use this option when there are no other commands to execute.

stop

Stops the eTrust AC Policy Model daemon/service.

truncate|trunc[*offset*]

Truncates the update file. If an offset is not specified, the file is truncated at the highest possible offset. The highest possible offset is the location of last command that successfully updated the subscriber. If *offset* is specified, all the entries up to the specified offset are deleted.

subs

Purpose

The subs command adds a subscriber to a parent PMDB or subscribes a database to a parent PMDB.

Syntax

```
subs pmdName {                         \
    [newsubs(subsName)]                \
    [parentpmd(pmdName2@host)]         \
    [subs(subName)]                    \
    [host_type(Mainframehosttype)      \
       sysid(systemId)                 \
       mf_admin(Mainframeadministrator)    \
       port(Remoteport)]               \
     {offset(offset)} }
```

Arguments

host_type(*Mainframehosttype*)
The mainframe host type of the subscriber.

mf_admin(*Mainframeadministrator*)
The mainframe administrator of the subscriber.

newsubs(*subsName*)
Subscribes *subName* to policy model *pmdName*, and sends the new subscriber the contents of the whole PMDB, password, and group files.

parentpmd(*pmdName2@host*)
Makes the PMDB specified by the argument *pmdName2@host* the parent Policy Model of *pmdName*.

port(*Remoteport*)
The port number of the subscriber.

subs(*subsName*)
Assigns a subscriber to the PMDB.

sysid(*systemId*)
The system ID of the subscriber.

When you subscribe a host to a PMDB:

- The host must be up
- eTrust AC must be running on that host

- The PMDB must be the parent PMDB of the subscribed host. This relationship is set by the token parent_pmd in the subscriber's seos.ini file, which must contain the name of the PMDB to which the host is being subscribed.

When you subscribe a PMDB to another PMDB:

- the token parent_pmd in the pmd.ini file of the subscribed PMDB must contain the name of the PMDB to which it is subscribing (its parent PMDB)
- eTrust AC must be running on the host in which the subscribed PMDB resides.

A PMDB should have only one parent. If you decide to establish a PMDB with more than one parent give the parent_pmd token the name of a file containing a list of the parent PMDBs.

However, establishing more than one parent is not recommended because you risk inundating your database with unreliable instructions from multiple sources.

subspmd

Purpose

The subspmd command changes the parent of the eTrust AC database in the host to which you are connected. The new parent PMDB is specified by *pmdName@host*.

Syntax

```
subspmd parentpmd(pmdName@host)
```

unsubs

Purpose

The unsubs command removes the subscriber *subName* from the subscriber list of the Policy Model specified by *pmdName*.

Syntax

```
unsubs pmdName subs(subName)
```

Chapter 5 Utilities

This chapter describes the utility programs and services that are included with eTrust AC. The utilities are found in the *eTrustACDir*\bin directory (where *eTrustACDir* is the directory where you installed eTrust AC). Use them in a DOS window as you would DOS commands. The switches, options, and parameters that apply to each utility are described in the following sections.

Utilities by Category

This section lists the eTrust AC utilities category, as an aid to finding the detailed description.

User Utilities

Utility Name	Description
defclass	Defines basic Unicenter TNG asset types in each database and every new PMDB that is defined.
ExportTngDb	Migrates the current Unicenter Security data into a local eTrust AC database or PMDB.
MigOpts	The eTrust AC program run at installation that translates the current Unicenter Security environment into the global settings of either a local eTrust AC database or PMDB.
sesudo	Executes commands that require Administrator authority on behalf of a regular user.

General Administration Utilities

Utility Name	Description
seaudit	Provides a facility for viewing the eTrust AC audit logs.
sechkey	Changes the encryption key for various eTrust AC programs.
secons	Provides a console for controlling the eTrust AC engine.
selang	The eTrust AC command line language.
seretrust	Retrusts untrusted programs.

Database Administration Utilities

Utility Name	Description
eACSyncLockout	Synchronizes an account's lockout with the eTrust AC database.
dbmgr	Manages the eTrust AC database. This new utility replaces several database utilities in previous versions.
ntimport	Copies information for Windows system users and groups to eTrust AC database.
seclassadm	Adds new classes to the local eTrust AC database.
sepmd	Administers PMDBs.

Support Utilities

Utility Name	Description
dbmgr	Maintains and reports on the records in the eTrust AC database.
semsgtool	Maintains the eTrust AC message file.
sepropadm	Administers properties of a local eTrust AC database.

Utilities in Detail

In this section, eTrust AC utilities are listed in alphabetical order. A detailed description of each is given.

Utilities can be modified to perform certain tasks. These command modifiers are represented in the syntax by the term *switch*. Switches are arguments that control operation. Some of the switches have *parameters* that customize the operation of the selected switch. The parameters may take on different *values*.

Syntax

The syntax used with utilities is the same as for selang. See the chapter “The selang Command Language” for details.

To invoke a Help menu when working with utilities, execute the utility without switches if the switches are not mandatory. With certain utilities you must specify the –h switch to invoke the Help screen.

dbmgr

The dbmgr utility manages eTrust AC databases. It replaces the dbutil, dbdump, rdbdump, secredb, sedb2scr, and sepropadm utilities of previous eTrust AC versions.

Warning! *This utility should be used only with the guidance of technical support personnel during problem resolution. With some options, it assumes eTrust AC is not currently running and should be invoked from the directory where the eTrust AC database resides.*

To execute the dbmgr utility, you must have the ADMIN, AUDITOR, or SERVER attribute.

Syntax

The general syntax for the dbmgr utility is:

```
dbmgr option switch [parameter][filename]
```

The following sections, organized by function, describe specific syntax, options and switches.

Database Creation

This option replaces the secredb utility.

Syntax

```
dbmgr [-h] | -c –c[q] [-v |-d] [-u(username)]   \
[-t(terminalname1[,terminalname2]…) [-o | -w]
```

Options

-create | -c -c[q]
: Creates a new database. When used with the -cq switch, does not prompt for verification.

Switches

-d
: Creates a database layout document.

-h
: Displays help. You can type dbmgr –h to get help for all options, or dbmgr –c (**without –h**) to get help for the option.

-o
: Adds Unicenter TNG classes to an existing database.

-t *terminalName*
: Specifies the terminals from which the administrator can manage the local database. To specific more than one terminal, separate the names with a comma.

-u *userName*
: Gives the user *userName* the ADMIN attribute for the database. If not specified, the default user is the Administrator.

-v
: Disables the verbose progress mode. The switches -d and -v cannot be used together.

-w
: Creates a new database that includes Unicenter TNG classes.

Notes

The -create option generates a new empty eTrust AC database. This command should be used only at installation time or when creating a new database or Policy Model database. The database is created in the current directory.

For example, if at the system prompt c:\temp> you enter:

```
c:\Program Files\CA\eTrustAccessControl\bin\dbmgr -c -c -u userName \
-t terminalName
```

The utility creates a new database in the c:\temp directory. It creates the user *userName* in the database, who has the ADMIN attribute and can administer the database from the terminal *terminalName*.

No special files are used.

Database Dump

This option replaces the dbdump and rdbdump utilities.

Syntax

```
dbmgr [–h ] |{–d |-dump} [-r]          \
   [c] | [d class [property | @filename]] |      \
   [o class record [property | @filename]]|      \
   [e class record [property]] |  [f] | [fc] |    \
   [p(class)] | [fp(class)] | [g(user)] |[l(class)]      \
```

Options

-d|-dump -r

Displays the information in the database. When used with the -r switch, dumps the database currently in use.

Switches

c

Lists the names of all classes defined in the database.

d *class* [*property*|*@filename*])

Displays the values of selected properties for all records of a class. The variable *class* specifies the class. The list of properties whose values are to be displayed is specified by *property*. To specify more than one property, separate the property names with a space. To read the property list from a file, replace *property* with an "at" sign (@) followed directly (with no intervening space) by the name of the file. Each property must appear on a separate line in the file. If *property* is not specified, the values of all the properties are listed.

e *class record* [*property*| *@filename*]

Displays the values of selected properties for all records of a class except a single specified record. The variable *class* specifies the class. The name of the record that is to be omitted from the list is specified by *record*. The list of properties whose values are to be displayed is specified by *property*. To specify more than one property, separate the property names with a space. To read the property list from a file, replace *property* with an "at" sign (@) followed directly (with no intervening space) by the name of the file. Each property must appear on a separate line in the file. If *property* is not specified, the values of all the properties are listed.

f
Writes the data to a specified file.

fc
Lists all database class information for all classes in the database.

fp *class*
Lists all database property information for properties of the specified class.

g *userName*
Lists the groups the specified user is a member of.

-h
Displays help. You can type dbmgr –h to get help for all options, or dbmgr –d (with or without –h) to get help for the option.

l *class*
Lists all the records in the specified class.

o *class record* [*property*|*@filename*]
Displays the values of selected properties for a single record of a class. The variable *class* specifies the class. The record is specified by *record*. The variable *property* specifies the list of properties whose values are to be displayed. To specify more than one property, separate the property names with a space. To read the property list from a file, replace *property* with an "at" sign (@) followed directly (with no intervening space) by the name of the file. Each property must appear on a separate line. If *property* is not specified, the values of all the properties are listed.

p *class*
Lists the names of the properties of the specified class.

Notes

The -dump option without the -r switch displays information from the local database located in current directory. It assumes eTrust AC is not currently running and must be invoked from the directory where the local database resides. With the -r switch, it reports on the records in the local database currently being used by the authorization engine but does not have to be executed from the directory containing the local databases. The utility performs the following functions:

- Dumps information for records of a specified class
- Dumps information for a single record of a specified class
- Dumps information for all records of a class except a specified one
- Generates lists of classes and property definitions
- Generates a list of groups of which a user is a member
- Generates a list of records of a particular class

Only one switch is allowed with the -dump or -dump -r option.

Database Export

This option replaces the sedb2scr utility.

Syntax

```
dbmgr [-h ] | {-e |-export} \
    [-l | -r]  [-c(classes)]  [ -f(filename)]
```

Options

-e|-export

Creates a script that contains the selang commands required to duplicate a local database.

Switches

-c *classes*

Exports data for specified classes only. Separate names with a space. Use this switch with either the -l or -r switches.

-f *fileName*

Writes the data to a specified file. Use this switch with either the -l or -r switches.

-h

Displays help. You can type dbmgr –h to get help for all options, or dbmgr –e (with or without –h) to get help for the option.

-l

Exports the database found in the current directory.

-r

Exports the database currently being used by seosd. Only users with the ADMIN or SERVER attribute can use this option, and the eTrust AC engine must be running.

Notes

The -export option generates a script consisting of the selang commands required to define an existing database and writes them to standard output. This script can be used to replicate a database on other stations.

Do **not** use this option with the -l switch when eTrust AC is running. If you invoke the –l switch when eTrust AC is running, the utility issues an error message.

Use the -f switch to write the generated commands to a file. A new database can then be created from the file, by instructing selang to read the commands from the file.

Database Maintenance

This option replaces the dbutil utility.

Syntax

```
Dbmgr [-h] | {-u | -util}
       -all   <filename> \
 -build <filename> \
 -close \
 -dump  <filename> \
 -dup   <filename> <destfile>  \
 -f     <outfile>  \
 -free  <filename>  \
 -index <filename>   \
 -key   <filename>    \
 -load  <filename> <ASCIIfile>   \
 -scan  <filename>  \
 -scana <filename>   \
 -stat  <filename>    \

 -stat  \
 -index \
 -free   \
 -dump \
 -scan  \
 -scana \
 -dup    \
 -load   \
 -build  \
 -key    \
 -all     \
 -close\
```

Options

-u |-util

Maintains the existing database.

Switches

-all

Performs all index checks. This is the same as specifying the index and free switches.

-build

Builds indexes of a DBIO based on data records.

-close

Closes the database files.

-dump

Dumps the data file as ASCII on the standard output device.

-dup*filename destinationFile*

Duplicates the DBIO file based on the file header. You must specify both a source and a destination file.

-f Writes the data to a specified file. This switch may be used with any other switch.

-free Checks for a free index.

-h Displays help. You can type dbmgr –h to get help for all options, or dbmgr –u (with or without –h) to get help for the option.

-index Checks the consistency of the index.

-key Scans the index file sequentially.

-load*filename ASCIIfilename*

Loads an ASCII file and converts it into a DBIO file.

-scan Scans the database sequentially.

-scana Scans the database sequentially, including deleted records.

-stat Lists the header information of the database file.

Notes

The -util option is used to manage and manipulate the local database specified by the parameter file name. Database files have the extension .dat and must be DBIO files. Database index files (files with the extension .001) may not be used with the -util option.

Database Backup

The dbmgr -backup function creates an online backup of the eTrust AC database in the specified directory.

This function is available whether the eTrust AC services are running or not.

The backup directory cannot be located on a remote machine; if the directory does not exist, this dbmgr -backup option creates it.

Syntax

```
dbmgr -backup | -b backup_directory
```

See Also

- The secons utility in this chapter.

Copying Data to a Flat File

The dbmgr -migrate function copies data from user records in an existing database to a flat file. It can also copy the data from the flat file into a new database. The database from which the data is imported must be version 1.21 or later.

When you copy a flat file into a new database, it is important to use the same version of this function that you used to create the flat file. If you have more than one version, it is strongly recommended that you use the most recent version.

Syntax

```
dbmgr migrate | -m switch [option]
```

Switches

-r *filename*

Read the database in the current directory and copy certain data into the flat file specified in the command line.

-w *filename*

Read the flat specified in the command line and copy the data into the database in the current directory.

Options

-f *filename*

Directs output to the specified file, instead of the standard output device. You must include this option when working from the WINDOWS GUI.

-s

Read the information from the database using the eTrust AC server, rather than reading the database directly. This option is valid only with the -r switch. To run the command with the -s option, you must have administrator privileges and R (read) and W (write) access to the terminal.

Imported Data Description

The imported USER data includes the following:

- OLD_PASSWD - The old passwords of the user; that is, the user's password history.
- PASSWRD_L_C - The date and time the user password was last changed.
- LAST_ACC_TERM - The terminal from which the user last logged in.
- LAST_ACC_TIME - The date and time the user record last logged in.

Notes

The -migrate function always reads from or writes to the database in the current directory unless you include the -s option.

Always create a backup of the database before using this function.

For better security, delete the old database, the script used to build the new database, and the flat file created by this function after copying the data from the old database into the new database

The flat file is written in binary format.

Examples

The following steps illustrate how to copy data from an existing database into a new database. The old database is assumed to be in the directory C:\Tmp\old_db. The new database is assumed to be in the directory eTrustACdir/seosdb (where eTrustACdir is the directory in which you installed eTrust AC).

1. If the eTrust AC services are running, shut them down with the following command:

   ```
   > secons -s
   ```

2. Create a backup of the old database by copying it to a different location or to a backup medium.

3. Copy the database into C:\Tmp\old_db, then create a script that duplicates the old database by running the dbmgr utility on the old database:

   ```
   > cd C:\Tmp\old_db
   > dbmgr -export -l > lang_script
   ```

4. Create a new database:

   ```
   > cd .\Program Files\CA\eTrustAccessControl\data\seosdb
   > dbmgr -c -c -u <Administrator name> -t <terminal name>
   ```

5. Execute the script generated in the previous step and create the new database:

   ```
   > cd .\Program Files\CA\eTrustAccessControl\data\seosdb
   > selang -l C:\Tmp\old_db\lang_script
   ```

6. Execute the dbmgr utility to create a flat file containing data from the old database:

   ```
   > cd C:\Tmp\old_db
   > dbmgr -migrate -r flat_file
   ```

7. Load the data from the flat file into the new database:

```
> cd .\Program Files\CA\eTrustAccessControl\data\seosdb
> dbmgr -migrate -w C:\Tmp\old_db\flat_file
```

Registry Settings

The -migrate function uses the database files in the current directory; it does not use the registry settings.

See Also

- The dbmgr -export function in this section.
- Secons utility in this chapter.

defclass

Defines basic Unicenter TNG asset types in each database and every new PMDB that is defined

Syntax

```
defclass.bat
```

Description

eTrust AC now defines basic Unicenter TNG asset types in each eTrust AC database and every new PDMB that is defined. This script defines user-defined security asset types as eTrust AC classes in the eTrust AC database.

The installation program automatically executes this script when Unicenter Integration is selected.

eACSyncLockout

Synchronizes an account's lockout with the eTrust AC database. (That is, upon account lockout, the corresponding user's record in the eTrust AC database becomes suspended. This utility is effective only when password synchronization is on **and** the user running the utility has the ADMIN property.

Syntax

```
eACSyncLockout  \
    -start | -stop | –remove \
    –p (password)  \
    –u (user)  \
```

Arguments

-p (*password*)
Causes the service to be installed and started in the current user's context, with the password given as input.

-remove
Causes the service to be stopped and uninstalled. (In the next boot of the machine, the service does not appear in the "Service Control Manager.")

-start
Causes the service to be installed and started in the current user's context, assuming the user has no password.

-stop
Stops the service.

-u (*user*)
Causes the service to be installed and started in the argument user's context, assuming the user has no password.

Note: If you enter -u(*user*) -p(*password*), the service is installed in the argument user's context, with the password given as input.

ExportTngDb

Migrates the current Unicenter Security data into a local eTrust AC database or PMDB.

Syntax

```
ExportTngDb.exe
```

Options

/A
Migrates asset types into the local database.

/I:casecdb
Required with the /A option, specifies where to import data from.

/O:selang
Required with the /A option, specifies how to output the data.

/N:*nodeName*
Targets a satellite node (machine) using eTrust AC push technology. The default is the local node.

/S — Migrates data in silent mode (unattended).

/L:*fileName* — Sends all output to a log file.

Description

The ExportTngDB.exe program migrates the current Unicenter Security data into a local eTrust AC database or PMDB.

The installation program automatically executes this program when Unicenter Integration is selected.

MigOpts

Translates current Unicenter Security environment into the global settings of either a local eTrust AC database or PMDB.

Syntax

```
MigOpts.exe
```

Options

-d *pmdName* — Issues an eTrust AC **hosts** command before running any selang commands to update the imported PMDB (rather than the local eTrust AC database, which is the default).

-f *fileName* — Generates any **selang –c** commands into an executable script file.

-l *logfileName* — Writes log messages to the fully specified file name.

Description

The MigOpts.exe program is responsible for translating the current Unicenter Security environment into the global settings of either a local eTrust AC database or PMDB.

The installation program automatically executes this program when Unicenter Integration is selected.

The migopts program can, and should, be executed manually whenever a new PMDB is created.

ntimport

The ntimport utility extracts Windows users and groups from the Windows operating system database for import into a local database.

Syntax

```
ntimport <switches> <options>
Switches:
 -u
 -g
 -c
 -a
 -d
 -U
Options:
 -o <owner>
 -f <filename>
 -p <pmdb>
 -pn <pmdb>
 -pa <pmdb>
 -r <remote host>
 -D
 -v
```

Options

-f *filename*

Redirects the output to the specified file.

-o *owner*

Sets ownership rules for each imported record. Use this flag, to prevent *Administrator* from automatically becoming the owner of all the records. *Owner* is the name of the user or group to be assigned ownership of all records defined by ntimport.

-v

Provides the user with progress information. Use this flag to verify the program's progress when there are many users or groups.

Switches

-a

Performs all actions of the –c, -g, and -u switches.

-c

Generates the selang commands required to join users to their default groups.

-g Generates selang commands required to import groups from Windows to the local database.

-u Generates the selang commands required to import users from the Windows database to the local database. Names longer than 40 characters are truncated.

Notes

The ntimport utility creates the Windows commands necessary to add users and groups to the local eTrust AC database.

The ntimport utility is typically used as part of the installation procedure.

The generated commands are displayed to the standard output. Use the option -f *filename* if you want to create a file to be used as input to the selang utility.

seaudit

The seaudit utility is used to display the eTrust AC audit log.

Authorization

To execute the seaudit utility, you must have the AUDITOR attribute.

Files

The seaudit utility uses the following values in the Windows registry subkey HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrustAccessControl\:

Subkey	Values
logmgr	audit_back error_size
message	filename

For more information, see the appendix “Registry Keys.”

By default, the audit file is located at *eTrustACDir*\log\seos.audit (where eTrustACDir is the directory where you installed eTrust AC, by default Program Files\CA\eTrustAccessControl).

Syntax

```
seaudit -h |{-a |-all} |    \
   {-i |-inet} host service |   \
   {-l |-login} user terminal |   \
   -nt | m         \
   {-r |-resource}(class)(resource)(user)|\
   {-s |-start} |      \
   {-t |-table} |       \
   {-u |-update}command class record user | \
   {-w |-watchdog        \
   [-c ]          \
   [-delim(delimiter) ]       \
   [-detail ]          \
   [-ed(date) ]          \
   [-et(time) ]          \
   [-f |-failure]        \
   [-fn |-filename] filename    \
   [-g |-grant] | [-gn |-grantnotify] \
   [-logout ]         \
   [-millenium ]       \
   [-n |-netaddr]       \
   [-notify ]          \
   [-o |-origin] host        \
   [-pwa ]          \
   [-sd(date) ]          \
   [-st(time) ]        \
   [-v |-servnum ]       \
   [-warn ]
```

Switches

-a

Lists all records except those sent to the audit log.

-h

Displays examples and help.

-i(*host service*)

Lists the INET audit records of TCP requests received from *host* for *service*. The variables *host* and *service* are masks that specify the set of hosts and services that are searched for.

-l(*user terminal*)

Lists LOGIN records logged for *user* on *terminal*. Both *user* and *terminal* are masks.

-nt

Show only Windows environment records.

-r(*class resource user*)

Lists general resources audit for *class* on resource *resource* for *user*. *class* is a mask that identifies the class to which the accessed resource belongs. *resource* is a mask that identifies the names of the resources that were accessed. *user* is a mask that identifies the names of the users who accessed the resources.

-s

Lists the start-up and shutdown messages from the eTrust AC engine.

-t

Displays the table of log codes.

-u(*command class record user*)

Displays database update audit records. *command* is a mask identifying the set of selang commands to search for. *class* is a mask identifying the classes to be searched. *record* is a mask identifying the records to search for. *user* is a mask identifying the users who executed the commands.

Options

-c
Show TCP connected INET records.

-delim(*delimiter*)
Use *delimiter* as a delimiter between fields.

-detail
Show elaborate information about each field.

-ed(*date*)
Specifies the end date (*dd-mmm-yyyy*). Records logged after the end date are not displayed in the list. You can use the string *today* to set the end date to the current date. You can use the string today-*n* to specify the end date as *n* days before the current date.

-et(*time*)
Specifies the end time (*hh:mm*) in 24-hour format. Records logged after the end time are not displayed in the list. You can use the string *now* to set the end time to the current time. You can use the string now-*n* to specify the end time as *n* minutes before the current time.

-f
Specifies that failures should not be displayed.

-fn(*fileName*)
Specifies the name of the audit log to be searched.

-g
Specifies that successful (granted) accesses should not be displayed.

-gn
Specifies that successful (granted) accesses should not be displayed unless a notify record was created.

-logout
Specifies that logout records should not be displayed.

- millennium
Specifies that years should be displayed with four digits instead of two.

-n
Specifies that internet addresses, not host names, should be displayed for TCP/IP services.

-notify
Specifies that notify audit records should not be displayed.

-o(*host*)
Specifies that records originating only from the specified *host* should be displayed. This option applies only when browsing records from a consolidated audit file created by the **selogrcd** log-routing collection engine.

-pwa
Specifies that password attempt records should not be displayed.

-sd(*date*) Specifies the start date (*dd-mmm-yyyy*). Records logged prior to the start date are not displayed in the list. You can use the string *today* to set the start date to the current date. You can use the string today-*n* to specify the start date as *n* days before the current date.

-st(*time*) Specifies the start time (*hh*:*mm*) in 24-hour format. Records logged prior to the start time are not displayed in the list. You can use the string *now* to set the start time to the current time. You can use the string now-*n* to specify the start time as *n* minutes before the current time.

-v Displays port numbers rather than service names.

-w Lists the watchdog audit records.

-warn Specifies that warning records should not be displayed.

Notes

Log records are submitted by the eTrust AC authorization engine seosd when an access to a resource requires auditing (as specified in the resource's audit mode property) or when the accessing user's audit mode property specifies auditing of the access operation. This command-line utility is used to generate a report from the eTrust AC audit log.

When displaying audit records that include passwords, seaudit protects password identity by substituting a series of asterisks (*) in place of the password text.

Output

Each record that seaudit displays contains data arranged in columns. The data in the first three columns has the same meaning for all types of records. The remaining data displayed is dependent on the type of record. The following table describes the format of the output for the most common types of records, by column.

Column	Contents	Description
1	Date	The date the access or attempted access occurred.
2	Time	The time the access or attempted access occurred.

Column	Contents	Description
3	Return code	The eTrust AC return code that indicates what happened. Valid values are: D eTrust AC denied access to a resource or did not permit an update to the local database because the accessor did not have sufficient authorization. F An attempt to update the local database failed. M eTrust AC was started or shut down. O A user logged out. P eTrust AC permitted access to a resource or permitted a login. S The local database was successfully updated. U A trusted PROGRAM or SECFILE was changed, so it is now untrusted. W An accessor's authority was insufficient to access the specified resource; however, eTrust AC allowed the access because warning mode is set in the resource.
4	Event type/ Class	The type of event being audited or the class on which the action was performed.
5	Accessor/ Class	If the previous column contains a class name, this column contains the name of the accessor who executed the command. If the previous column contains UPDATE, this column contains the class in which the action was performed. Otherwise, this column contains the name of the accessor who executed the command or any other relevant information about the class.
6	Access type/ Accessor	If the previous column contains the accessor name, this column contains the access type, if relevant. If the previous column contains the class name, this column contains the name of the accessor who executed the command. Otherwise, this column contains the access type, if relevant, or any other relevant information according to the class.
7	Stage code	A number (up to three digits) that indicates at which stage eTrust AC decided what action to take and why.

Column	Contents	Description
8	Audit record code	A number that represents the reason that eTrust AC wrote an audit record.
9	Resource	This column contains the name of the resource being accessed or updated.
10	Terminal/ Program	If column 4 contains UPDATE, this column contains the name of the terminal from which the update was made. Otherwise, this column contains the name of the program that accessed the resource.
11	Command	If column 4 contains UPDATE, this column contains a complete copy of the command entered by the accessor. If the command is a password update, the password itself is replaced by a series of asterisks.

The output generated by **seaudit** typically looks like this:

```
07 Mar 99 17:42 P FILE         Dennis     Read 59  2
               \device\harddisk0\partition1\file.txt
07 Mar 99 17:59 O LOGOUT       Bill                49  2
07 Mar 99 18:05 M START                                  seosd
07 Mar 99 18:07 M SHUTDOWN     John                  452 seosd
Following is a line-by-line explanation of this output:
07 Mar 99 17:42 P FILE         Dennis     Read 59  2
               \device\harddisk0\partition1\file.txt
```

On 7 March 1999 at 17:42, eTrust AC permitted (P) user Dennis to read the file \device\harddisk0\partition1\file.txt. The eTrust AC stage code is 59 (resource UACC check). The event is logged in the audit log because code 10 (User audit mode) in the user's audit record requires auditing of all types of accesses.

```
07 Mar 99 17:59 O LOGOUT       Bill                49  2
```

User Bill logged off the system. eTrust AC knows about most process terminations in the system, and considers Bill logged off when all processes associated with his credentials have terminated. The LOGOUT class entry and the O in the return column identify Logout records. Code 49 indicates a LOGOUT audit record. Code 2 indicates the event was logged due to the user's audit mode. eTrust AC reports logouts only if logins are also reported for the user.

```
07 Mar 99 18:05 M START                                  seosd
07 Mar 99 18:07 M SHUTDOWN     John                  452 seosd
```

These audit records indicate the start-up and shutdown of the eTrust AC engine seosd. seosd started at 18:05 and John brought it down at 18:07. John was allowed to take seosd down because he has the ADMIN attribute—reason code 452. Return code M indicates start-up or shutdown of seosd.

Examples

Situation	Command
List all audit records since January 3, 1998.	seaudit -a -sd 03-Jan-1998
List all accesses by user John to every resource of class FILE.	seaudit -r FILE * John
List all audit records that were logged between 17:00 yesterday and 08:00 today.	seaudit -a -st 17:00 -et 08:00
List all audit records that were logged today between 08:00 and 17:00.	seaudit -a -st 08:00 -et 17:00
List all the audit records from yesterday.	seaudit -a -sd today-1 -ed today-1

sechkey

The sechkey utility changes the encryption key for various eTrust AC programs.

Syntax

```
sechkey [-d]| [-h] |[-s <registry path>]
```

Parameters

-d Restores the original encryption key supplied with eTrust AC.

-h Display help. This is one of the utilities where you must type the –h switch to get help.

-s Define registry root specified by <registry path>

Notes

When you type sechkey with no parameter, the sechkey utility prompts you for a new encryption key.

Note: Before running the sechkey utility, stop eTrust AC by executing the secons -s command in a DOS window. eTrust AC begins using the new key after eTrust AC is restarted. Restart eTrust AC by executing the seosd -start command. You may also use the SeStart and SeStop utilities from the Start button on the Windows taskbar.

The sechkey utility can work on two types of programs:

- The following group of eTrust AC programs for which an encryption key is always used in order to protect your communications: SeOSAgent, selang, seosd, sepass, and sepmdd, located in *eTrustACDir*\bin.
- Programs you create using an eTrust AC API that communicates with an eTrust AC service. These programs' communications are encrypted with the default eTrust AC encryption key.

To ensure successful communication, you should use the same encryption key for all these programs. In Windows, when you change the encryption key, sechkey changes the key in all programs in the eTrust AC database at once. (In UNIX, you can choose to change the key in one program without changing the key in another program. However, if you change the key in one program without changing it in another, the two programs cannot communicate successfully.)

You should change the key in all the hosts in Windows and UNIX that communicate with each other to avoid creating a situation in which the encryption keys are not identical and the hosts cannot communicate successfully.

Comments

- In previous versions of eTrust AC, a user could connect to both Windows and UNIX machines only by using the default encryption key. If the encryption key was changed using sechkey, the user could not "talk" with UNIX machines. The reason for this was that key encryption on UNIX and Windows machines was done in a different way according to different rules. As a result, Windows and UNIX machines could not "understand" each other.

  Beginning with Patch 4 for eTrust AC Version 4.1, the same form of key encryption is used for both UNIX and Windows. Thus, the sechkey utility may be used to change encryption, even when connecting a Windows to a UNIX machine, without affecting communication.

  If your network includes older versions of eTrust AC for Windows, you should upgrade the sechkey utility by using the *eTrustACDir*\bin\sechkey.exe file from the latest version to overwrite the file in the same directory of the older version.
- The maximum length of the encryption key is 55 characters.

seclassadm

The seclassadm adds new classes (User Defined Classes) to the local database.

Files

The seclassadm utility uses the local database files if these files are located in the current directory.

Syntax

```
seclassadm [-h] | {-add |-del} classname         \
    [-a modes] -d access] |[-f] |[-g] |[-n] |[-o] |[-p]
```

Commands

-add(*className*)

Adds a new resource class to an existing local database. *className* is the name of the new class. eTrust AC reserves class names that are in all uppercase characters. When you add a class, you should use at least one lowercase character in the class name. Class names can be up to 15 characters long.

After adding a new class, you must enable the class by using the setoptions command under selang. For more information, see setoptions in the chapter “selang Commands in the eTrust Environment.”

-del(*className*)

Deletes the specified resource class from the database.

Switches

-a(*modes*)

Sets the access modes for the class. The string *modes* represents the allowed accesses. Each access mode is represented by a single character code listed in any order. The string must not contain any blank or other non-alphabetic characters. Valid access modes are:

Abbreviation	Description
C	control
D	delete
E	create
F	filescan
M	chmod
O	chown
R	read
S	security
T	utime

Abbreviation	Description
U	update
V	rename
W	write
X	execute

-d(*access*) Sets the class's default access—the access that is assigned to a user when the authorize command is executed without specifying an access authority. This is the implicit access used by the authorize command and is not to be confused with the default access assigned to a resource. The valid access types are those listed under -a modes. When specifying access, the order of the access characters does not matter, but the string cannot contain blanks or other non-alphabetic characters.

-f Forces eTrust AC to accept a new class name even though the name contains all uppercase characters.

-g Specifies that the new class is a resource that groups members of an existing class. The relationship between the existing class and the new group class is like the relationship between class TERMINAL and class GTERMINAL in the local database.

A resource that groups members of an existing class must begin with the uppercase character G. By convention the remainder of the class name is the same as the existing class.

-n Writes output to a specified file name.

-o Creates a _default object for the class with the specified default access.

-p Full path location of the localhost database.

-r Specifies that this class has a resource description object (for eTrust™ Web Access Control classes).

-t Specifies that this class is a Unicenter TNG class.

Notes

- The seclassadm utility must be invoked from the directory in which the local database resides.
- Do not use this program while the eTrust AC services are running.
- Specify one command only.

- The switches are optional, and you may specify more than one switch.
- If you must add a user-defined class to a new database, run the seclassadm utility after you have created the new database with secredb. This process must be repeated every time you create a new database.

Examples

Situation	Command
Add a resource class named dbfield.	seclassadm -add dbfield
Add a resource class named report with only read access.	seclassadm -add report -d R -a R
Add a resource class named batch_jobs with read, write, and modify permissions and read access as the default when not specified.	seclassadm -add batch_jobs -d R -a RWM
Add a resource class that groups records in the CLASS class with execute access and default execute access.	seclassadm -add GCLASS -d X -a X -f -g

secons

The secons command-line utility provides a control console to the eTrust AC engine. secons performs various operations, such as:

- Control tracing of the eTrust AC authorization engine
- Control concurrent logins
- Display run-time statistics
- Shut down the eTrust AC engine and all other eTrust AC services on the local station or on one or more remote stations

Authorization

The secons utility is available to both security administrators and other users. However, only the option -m is available for users who do not have the ADMIN attribute.

Only users defined as ADMIN or OPERATOR can shut down eTrust AC. To shut down eTrust AC on remote stations, you must be defined as ADMIN or OPERATOR on those remote stations.

Files

The secons utility uses the following values in the Windows registry subkey HKEY_LOCAL_MACHINE\Software\ComputerAssociates\ eTrustAccessControl:

Subkey	Values
SeOSD	trace_file trace_file_type trace_space_saver trace_to

For more information on these tokens, see the appendix “Registry Keys.”

By default, the trace file is located at *eTrustACDir*\log\seosd.trace (where eTrustACDir is the directory where you installed eTrust AC, by default Program Files\CA\eTrustAccessControl).

Syntax

```
secons <options>
Where <options> is one or more of:
  -t+
  -t-
  -tt
  -ts
  -tc
  -tv [<KBytes>]
  -file <FName>

  -d+
  -d-
  -ds

  -u+ <UName>
  -u- <UName>
  -us <UName>

  -l+
  -l-
  -ls

  -i
  -m <Message>
  -s [term/gterm list]
```

Options

-h

Displays help. This is one of the utilities where you must type the –h switch to get help.

-i

Gets run-time statistics and displays formatted text with various information as described in the section Output.

-m(*message*)

Sends a message to the console, adding text to the trace file produced by the eTrust AC authorization engine.

-s [*host*] [*ghost*]

Shuts down the eTrust AC engine. Before shutting down, the eTrust AC engine brings down the other eTrust AC services. *host* and *ghost* can be a single host or host group, or a list of hosts and host groups. Separate members of a list with spaces or commas. If *host* or *ghost* is not specified, the eTrust AC services are shut down on the local station only.

-t+

Enables tracing, which causes the eTrust AC engine seosd to dump messages that specify its operations and actions to the trace file. This option is only available to users with the ADMIN or OPERATOR attribute.

-t-

Disables tracing, which stops the eTrust AC engine seosd from dumping messages to the trace file. This option is only available to users with the ADMIN or OPERATOR attribute.

-tc

Clears trace file, removing all records from it. This option is only available to users with the ADMIN or OPERATOR attribute.

-ts

Displays the current tracing status. This option is only available to users with the ADMIN or OPERATOR attribute.

-tt

Toggles the tracing status between enabled and disabled. This option is only available to users with the ADMIN or OPERATOR attribute.

-tv [-file(*fileName)* | *(size)*]

Starts a browse and provides an online trace view. This option is only available to users with the ADMIN attribute.

-file starts a browse on the specified file instead of \Program Files\CA\eTrustAccessControl\log\seosd.trace. This option can be used whether or not seosd is running.

*size s*tarts a browse on the trace file and provides an online trace view, operating in a manner similar to the UNIX tail-f utility. Supply a *size* in KB to limit the output to only the last *size*. The default value is 2. Specifying 0 shows the entire trace file.

To stop this operation, use Ctrl+C.

Output

The screen output generated by the -i option resembles the following:

```
# \Program Files\CA\eTrustAccessControl\bin\secons -i
secons  eTrust Console Utility

Run-Time Statistics:
--------------------
INet Statistics:
      Requests Denied                                             : 0
      Requests Granted               : 17
      Errors found                                                : 0
Queues Size:
      Audit Log: 0
      Error Log: 0
Cached Tables Info:
      ACEE Handles       :     11
      Protected clients :       0
      Trusted Programs                                        :     77
      Untrusted Programs         :      0
Database info  :( record count & First Free Id)
      Classes       :     18 ( CID    0x0012 )
      Properties    :    223 ( PID    0x00df )
      Objects       :    152 ( OID 0x00000a8 )
      PropVals      :    972 ( N/A )
#
```

Following is an explanation of this output:

```
INet Statistics:
      Requests Denied    : 0
      Requests Granted   : 17
      Errors found       : 0
```

This section provides statistics on the number of authorization requests for incoming connection activity received by eTrust AC while class HOST is active. These lines summarize the number of requests denied and granted, and the number of errors that occurred during the request authorization.

```
Queues Size:
      Audit Log: 0
      Error Log: 0
```

Since eTrust AC creates logging with file locking, it is possible that certain events are held in memory and written to log files after a while. If these values exceed 10, then an error could be interfering with the eTrust AC logging facility.

```
Cached Tables Info:
      ACEE Handles       :     11
      Protected clients  :      0
      Trusted Programs   :     77
      Untrusted Programs :      0
```

- An ACEE (Accessor Entry Element) is a table containing logged-in processes.
- Protected clients lists the number of cached clients. Usually, this value is 0.
- Trusted Programs lists the number of entries in class PROGRAM that are cached in memory. Normally, all programs should be cached as trusted.

- Untrusted Programs displays the number of programs that were found to be untrusted.

```
Access Control Database: Record Count & First Free Id
      Classes       :     18 ( CID    0x0012 )
      Properties    :    223 ( PID    0x00df )
      Objects       :    152 ( OID 0x00000a8 )
      PropVals      :    972 ( N/A )
```

This section provides general information regarding the size of the local database and the number of records in each part of the database.

Examples

Situation	Command
Shut down eTrust AC.	secons -s
Shut down eTrust AC on remote stations remoteStat1 and remoteStat2.	secons -s remoteStat1 remoteStat2 eTrust AC notifies you that the station shutdown was successful. Even if eTrust AC does not shut down remoteStat1 successfully, it still shuts down remoteStat2.
Place the string “Start Event” in the eTrust AC trace file.	secons -m ‘Start Event’
Display the run-time statistics.	secons -i

selang

The selang utility invokes a command shell that provides access to the eTrust AC database and the Windows environment. The database is updated dynamically by issuing selang commands from within the command shell. selang commands are described in the chapter “selang Commands in the eTrust Environment” in this guide.

The result of the command’s execution is sent to the standard output unless the -o option is used.

Files

The selang utility uses the following files:

- *.selangrc

  The *.selangrc file is the default file for the -r option. It is a file of selang commands that are to be executed automatically each time you invoke selang.

  Note: It is your responsibility to write this file if you want it.

- An index file and a shell file. Do not edit these files.
  - lang.idx
  - lang.shl

Syntax

```
selang [-h ] | [-c(command) ]    \
    [-f ] | [-r ] (filename) ]   \
    [-d(dbdirectory)] | [-l ] | [-p(policymodelname)] \
    [-o(filename)]               \
    [-s ] [-v]
```

Options

-c(*command*)
Executes *command* and exits. If *command* contains any spaces, enclose the entire string in single quotation marks. For example, enter — selang -c 'showusr rosa'

-d(*dbdirectory*)
Updates the database in the specified directory. This option is only valid when seosd is not running.

-f(*fileName*)
Reads the commands from the specified file rather than from the terminal's standard input. As the commands in the input file are executed, the number of the line currently being executed is displayed on the screen. The selang prompt is not displayed on the screen. After selang executes the commands in *fileName*, it exits.

-h
Displays help.

-l
Updates the local database. This option replaces sedlang. (The shell script sedlang invokes this command.) It is only valid when seosd is not running, and can be executed only by a user who has the ADMIN attribute in the database.

-o(*fileName*)
Writes the output in the specified file. Each time selang is invoked, it creates a new, empty file. If you specify the name of an existing file, selang writes over the information currently in the file.

-p(*policyModelName*) Updates the PMDB specified in the command. The PMDB must be in the local station. This option is not valid if seosd is running on the specified PMDB. To update a PMDB when seosd is running, use the hosts command. For more information, see the description of the hosts command in the chapter “selang Commands in the eTrust Environment.”

-r(*fileName*) Reads the commands from the specified file. The file should consist of commands in normal selang syntax, separated by semicolons or line breaks. After the commands in *fileName* are executed, selang prompts the user for input. If *fileName* is not specified, selang uses the *.selangrc file in the user’s home directory.

-s Does not display the copyright message.

-v Writes command line to output.

Usage

Screen prompt—Once you enter the selang environment, you see a special selang prompt on your screen. The exact form of the prompt depends on your working environment. It looks similar to this:

```
eTrust>
```

If you want to work in a Windows environment, issue an env(nt) command. You then see:

```
eTrust(nt)>
```

If you want to work in a pmdb environment, issue an env(pmd) command. You then see:

```
eTrust(pmd)>
```

Other environment options are: native and UNIX.

- **Standard smart features—**Many of the command line entry features available in tcsh and other smart shells are supported.
- **Special characters—**The following special characters are supported:

Character	Meaning
*	At the beginning of a line, indicates that the line is a comment line. The line is not executed. Comment lines are useful when inputting the selang commands from a file.
!	At the beginning of the line, indicates that the rest of the line is a shell command. The command is sent to the operating system shell program for execution; eTrust AC does not execute the line.

Character	**Meaning**
Up-arrow or Down-arrow or ^	Retrieves a command from the history list, as documented in the following section.
\	As the last character of a line, indicates the command continues on the following line.
	Terminates a command and introduces a new command on the same line.
| *pipe*	Pipes the command output to the specified *pipe*.
Tab	Serves for word completion, as discussed under Ctrl+D.
Ctrl+D	With the cursor positioned at the end of the line, displays a list of words that match the word completion string in the command line. With the cursor positioned anywhere other than at the end of the line, deletes the character to the right of the cursor.
Esc Esc	Displays the help text for the command in the command line. All the text in the command line is preserved, so that you can continue typing the command from where you left off.

- **Longer lines—**Type one selang command per line. To continue a command on the following line, type a backslash (\) at the end of the line.
- **History—**Executed commands are stored in a *history list*. Use the up and down arrow keys to display commands in the command line from the history list. To see only the commands that start in a particular way, type the beginning of the command before using the up and down arrows. When Enter is pressed, the text currently displayed in the command line is executed.

  The selang command shell supports the following shortcuts that use the commands stored in the history list:

Specify ...	**To execute ...**
^^ [*string*]	The previous command. If *string* is specified, *string* is appended to the original command.
^n [*string*]	The command that is numbered *n* in the history list, where *n* is a positive integer. If *string* is specified, *string* is appended to the original command.
^-n [*string*]	The *n*-th command from the end of the list, where *n* is a positive integer. If *string* is specified, *string* is appended to the original command.

Specify ...	To execute ...
^mask [*string*]	The most recently issued command that begins with the characters *mask*, where *mask* is a text string. If *string* is specified, *string* is appended to the original command.

- **Command line editing—**The text in the command line can be edited. Use the arrow keys to move around within the line. You may insert characters by typing them directly into place and delete characters with the standard Backspace and Delete keys, or by pressing Ctrl+D.
- **Shortcuts in typing—**You can use various additional techniques to save keystrokes in the selang command shell:
  - **Command recognition—**The selang command shell recognizes which command you wish to execute as soon as you have typed in enough characters to distinguish it from all the other available commands. For example, the only command beginning with the letters "ho" is the hosts command. As soon as you type ho, the command shell can recognize which command is intended. On the other hand, several commands begin with the string new. You must add enough characters to distinguish between newusr, newgrp, newfile, and newres.
  - **Abbreviations—**Each command is also associated with a one to four letter abbreviation. For example, because several commands begin with the string new, you may also use the abbreviation nu for the command newusr. These abbreviations are documented as part of the command syntax for each command in the chapter "selang Commands in the eTrust Environment" in this guide. Commands may be entered in either upper or lower case. Record and class names, however, are case-sensitive.
  - **Word completion—**Press Tab in the middle of a word to complete the word. Word completion is context sensitive. If more than one word matches the supplied string, the shortest word or word fragment that matches the string is used. For example, if you type the letter n, selang supplies ew, giving the word new.

    If this is not the required word, type one or more characters and press Tab again to complete the word. Type Ctrl+D to see all the possible options. This is useful if you are not sure which command to use. Using the example in the previous paragraph, if you add the letter u to the word new and press Tab, selang supplies sr, giving you the command newusr.

    Words that are not part of the selang commands are stored in memory for use by the word completion feature later on in the same session. For example, if you type newusr Mercedes and later on type showusr Me followed by Tab, the Me is expanded to Mercedes, as follows:

    ```
    showusr Mercedes
    ```

This assumes that no other username was previously typed in that begins with “Me.”

selogrcd

Emitter daemon for the eTrust Access Control log routing system. Selogrcd must be running to enable eTrust Single Sign-On auditing.

Syntax

```
Selogrcd options
```

Options

-audit *audit-file-name* The utilty uses the file name provided instead of the file as default for the input audit file.

-config *config-file-name* The utility uses the file name provided instead of the default file for the configuration file.

-d Specifies debug mode.

-data *data-file-name* The utility uses the file name provided instead of the default file to store routing progress information.

-h Shows the usage screen.

-l *lock-file-name* Enables multiple instances of selogrcd to run concurrently. *Lock-file-name* is the name of the lock file to be used for each instance that selogrcd runs. Use this option if your system does not support file locking or if you want to execute more than one instance of selogrcd on the system. Each lockfile must have a distinct name.

-pmdb *policy-model* Instructs selogrcd where to route audit data from a policy model database (PMDB). The command tells selogrcd to send audit data from the audit file specified in the audit_log token in the PolicyServer.ini file of the Policy Server.

By default, selogrcd uses the data file and lock file that consist of the policy model name. If you specify the data file or lock file or both on the command line, the files that you specified override the default values. The lock file and data file names should be different from those of the selogrcd that route the audit data of the station. Selogrcd can only support policy model names of 12 characters.

The audit data that is sent from a PMDB appears in the collected audit file as if it comes from a station with the name policy-model-name@station-name.

semsgtool

The semsgtool utility semsgtool can perform the following functions:

- Show a single message from the eTrust AC message file.
- List an entire section of messages.
- Dump the entire file into ASCII files, one ASCII file for each section.
- Build a new message file.

You can only specify one command each time you execute semsgtool.

The default location of the message file is *eTrustACDir*\data\seos.msg (where *eTrustACDir* is the directory where you installed eTrust AC).

Syntax

```
semsgtool [-h] | [-b |-build] asciiSourcefile outputMessagefile |        \
    [-d |-dump] [messagefile ] |                 \
    [-l |-list] [messagefile(section) ] |        \
    [-s | -show] messagefile {(hexerrorcode) | (section#msg#)} | \
```

```
    [-number | -n] [message-file] <sub-str>
```

Lists messages, including sub-str

```
    [-change | -c] [message-file] [0x<error-code> | <section# msg#>] <new-
    message>
```

Changes message to a new one. Creates new message file as [message-file].new

Options

-b(*asciiSourceFile outputMessageFile*)

Creates a new eTrust AC message file from an ASCII source file.

-c *(message-file hexerrorcode, section# msg#, new-message)*

Given a specific message code or section number and a new message (set of characters limited between inverted commas), semsgtool replaces the message associated with 'hexerrorcode' with the new message. This action creates new message file with extension ".new". Old message file is not changed. If the parameter messageFile is not supplied, semsgtool uses the message file as specified in the file name value in the registry subkey: HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\message. The message code can be a hex number or two parameters specifying section code and message code. The section or message code in turn can also be decimal or hex numbers. Hex numbers must be preceded by 0x.

-d(*messageFile*) Dumps the message file into several files, one file for each section of the message file. This creates ASCII source files that later can be used to create new eTrust AC message files.

-l(*messageFile* (*section*)) Lists all the messages in a given section in the file *messageFile*. If the parameter *messageFile* is not supplied, semsgtool uses the message file as specified in the file name value in the registry subkey: HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\message. The section number can be a hex number or a decimal number. Hex numbers must be preceded with 0x (zero x).

-s (*messageFile, hexerrorcode, section*#*msg*#)

Given a specific message code or section number, semsgtool shows the message associated with it. If the parameter messageFile is not supplied, semsgtool uses the message file as specified in the file name value in the registry subkey: HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\message. The message code can be a hex number or two parameters specifying section code and message code. The section or message code in turn can also be decimal or hex numbers. Hex numbers must be preceded by 0x.

Notes

The eTrust AC message file is composed of sections and message numbers. Each section holds messages for different eTrust AC modules or sub-modules.

Examples

- To list the message associated with the error code 0x0205, type:

```
semsgtool -s 0x205
```

- To create a modified eTrust AC message file, do the following:

1. Create a temporary directory

```
md \tmp\msg_build
```

2. Change to the new directory

```
cd \tmp\msg_build
```

3. Dump the messages to ASCII files

```
semsgtool -dump *:\Program Files\CA\eTrustAccessControl\data\seos.msg
```

Now you should have a file for each section in the messages file.

4. Create a single file from all the sections as follows.

   For each file created in the last stage concatenate to the new file:

   – SECTION <filename> <new line>

   – The contents of the file.

5. Rebuild the eTrust AC message file:

   ```
   semsgtool -b ascii_file seos.msg
   ```

6. Install the new message file:

   ```
   copy seos.msg \Program Files\CA\eTrustAccessControl\data\seos.msg
   ```

sepmd

The sepmd utility administers the PMDBs. It supports multiple PMDBs on a single host.

- Manage the list of subscriber databases
- Display and clear the Policy Model error log
- Clear the file containing PMDB updates

Important! *Do not use the Windows Task Manager application to shut down the Policy Model engine.*

Authorization

- You can run sepmd if you have the ADMIN attribute and have been given write permissions to the PMDB directory and files.
- To shut down a PMDB, you must be an administrator of the Policy Model—have the ADMIN attribute in the PMDB—or have the OPERATOR attribute on the station on which the Policy Model resides.

Files

sepmd uses the following files:

- updates.dat
- error_log
- The Windows registry

Syntax

```
sepmd [-h ] | [-k ] | [-S ] |   \
      [-c ] | [-C   ] | [-cl ] |       \
      [-dl ] | [-e ] |   \
      [-l ] | [-L ] | [-p ] |   \
      [-kl ] | [-ri ] | [-n ]   \
      [-sl] pmd         \
      [-t pmd {auto | offset } ] |   \
      [-r ] | [-u ] pmd subscriber |   \
      [-s ] pmd subscriber [offset] |    \
      [-sm] pmd mfsubscriber mftype mfsysid mfadmin [offset]]
```

Switches

-c
Clears the Policy Model error log.

-C
Displays the commands in the update file of the specified PMDB.

-cl
Clears the Policy Model log file.

-dl
Displays the Policy Model log file.

-e
Displays the Policy Model error log.

-k
Deactivates (“kills”) the Policy Model service. In Windows (unlike UNIX), this option does not stop the Policy Model service.

-kl
Stops logging in the Policy Model log file.

-l
Lists the subscribers of the Policy Model.

-L
Lists the subscribers of the Policy Model and their offsets in the update file. The update file contains updates that must be or have been propagated by the Policy Model. The offset indicates the location of the first update that must be sent to a subscriber.

-n
Creates a new subscriber and updates it retroactively to the Policy Model. For general rules that apply for updating a subscriber, see the description for the -s option. This option sends the contents of the entire PMDB to the new subscriber.

A subscriber added with -n is marked as **sync**, indicating that it is now in synchronization mode and receives all of the PMDB rules. When the subscriber has received all the rules, it is released from synchronization mode and becomes a regular subscriber. The -n option may take some time to process. If there are multiple or contradictory updates, the last one is used.

-p
Lists the Policy Models resident on the host and their status.

-r	Removes the subscriber from the list of unavailable subscribers maintained by the Policy Model service sepmdd, making the subscriber available for immediate updates. Normally, if a subscriber is down and cannot receive updates from the Policy Model, sepmdd tries to send updates to that subscriber only after a certain period of time. However if this parameter is used, sepmdd skips the waiting period and tries to send updates to the subscriber immediately.
-ri	Reloads Policy Model information from the registry to the hosts. Use this switch if you changed data and want to be sure it is sent to the host PMDBs.
-s	Subscribes another database or PMDB to the Policy Model. When subscribing to a Policy Model, the value of the entry parent_pmd in the Windows registry sub-key of the subscribed PMDB must contain the name of its parent PMDB.
-S	Activates ("starts") the Policy Model.
-sl	Starts logging in the Policy Model log file. -sm Subscribes a mainframe computer to the Policy Model.
-t [offset]	Deletes entries from the update file, updates.dat, truncating the file. When you specify -t, sepmd calculates the offset of the first unpropagated entry and deletes all the entries before it. When you have previously run sepmd -L and know the offset (distance from the beginning of the file to the position of a particular subscriber) at which you want to truncate the file, specify this *offset*. Sepmd truncates the update file at the given offset, which was rounded to match an existing record in the update file. If a subscriber misses an update before the specified offset, sepmd displays an error message and does not truncate the file. To force truncation of the file in any case: 1. Unsubscribe the station that was not updated. 2. Truncate the file. 3. Resubscribe the station to the Policy Model. When you do this, the subscriber misses one or more updates from the Policy Model. Any changes made to the Policy Model while the subscriber is unsubscribed do not get propagated after resubscribing.
-t auto	Truncates the update file at the highest possible offset, deleting transactions that have been propagated to all subscribers.
-u	Removes ('unsubscribes') a subscriber from the Policy Model subscription list.

Parameters

PolicyModel The name of the Policy Model.

Subscriber The full name or IP address of the subscriber station or the host of the subscriber PMDB.

Notes

- You must run the sepmd utility on the host where the Policy Model resides.
- When subscribing a host to a Policy Model, the Policy Model must be the parent PMDB of the subscriber station; that is, the parent_pmd value for the HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\eTrustAccessControl subkey in the Windows registry must be set to the name of the Policy Model.
- When subscribing one Policy Model to another, the following must be true:
  - The subscribed Policy Model has been defined and initialized.
  - The Policy Model must be the parent PMDB of the subscriber PMDB; that is, the parent_pmd value in the Windows registry subkey: HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\eTrustAccessControl must be set to the name of the parent PMDB.

sepropadm

Administers eTrust AC database properties.

Important: *This utility is used by eTrust AC technical support personnel only.*

Description

The sepropadm utility adds, updates, and deletes properties in the database. You must invoke this utility from the directory in which the database resides, and while the eTrust AC daemons are **not** running. The sepropadm utility can add only one property at a time.

WARNING! *Do* ***not*** *use sepropadm with a description file that was* ***not*** *certified by eTrust AC technical support personnel.*

Syntax

```
sepropadm file
```

Parameters

file

A description file supplied by eTrust AC support personnel. The description file uses the following format:

Lines that begin with a semicolon (;) are comments and are not processed.

There must be one line that begins with the hash symbol (#). This line must precede the description lines.

The description line to add a new property, which must conform to the following format:

```
CLASS=%s PROPERTY=%s TYPE=%d SIZE=%d FLAGS=%x
```

The description line to update a new property, which must conform to the following format:

```
CLASS=%s OBJECT=%s PROPERTY=%s VALUE=%s
```

The description line to delete a new property which must conform to the following format:

```
CLASS=%s PROPERTY=%s
```

Files

The eTrust AC database files are used.

Example

The following is a sample description file.

```
 ; Sample Patch File for the eTrust Access Control database
 ; Copyright 2003 Computer Associates International, Inc.
 ; ---------------------------------------------
 ; DO NOT USE THIS FILE UNLESS YOU KNOW HOW TO!
 # seclassadm database add property patch utility
 ; Format is :
 CLASS=PROGRAM PROPERTY=SNEFRU TYPE=29 SIZE=32 FLAGS=0
```

See Also

The dbmgr, seclassadm, and lang.ini utilities in this chapter.

seretrust

Generates the selang commands required to retrust programs and secured files.

Syntax

```
seretrust switches path
```

Switches

-a
Generates retrust commands for all records, no matter their database properties.

Base_path
Processes records defined in the specified directory only. If you use this parameter without the - prefix, the path is considered to be the current one. If you do not specify a Base_path, then an empty directory is presumed. (That is, all records are processed.)

-h
Displays help for this utility.

-l
Extracts information about the programs and files from the database in the current directory. (This switch is not applicable when the services are running). Omitting this switch means the database processed in this session is the same database that the seos Engine services uses.

-p
Processes records in the PROGRAM class only.

-s
Processes records in the SECFILE class only.

Parameters

path
Specifies the path of the programs to be retrusted. The specified directory and all subdirectories are processed.

Description

The eTrust AC database contains two classes, SECFILE and PROGRAM, which give eTrust AC the ability to monitor resources (executables and files). Any changes to resources in the SECFILE and PROGRAM classes should be alerted to the eTrust AC administrator.

The Watchdog checks the defined resources at defined intervals (configured in the registry) and then makes the decision about the integrity of the resources. If a change is detected, the resource becomes untrusted and an audit record is sent to the audit log.

Because of this, a resource could be defined in the eTrust AC database as trusted although it has changed. This can happen if the resource has changed and the next Watchdog check has not occurred yet.

The seretrust utility reports the status of the SECFILE and PROGRAM resources that are defined as trusted but have changed. seretrust also checks whether programs have been changed but have not yet been caught by the Watchdog. (This means that in the eTrust AC database, these programs are still marked as trusted.) These programs are added to seretrust output with a note that the program content or timestamp has been changed, and the program needs to be retrusted.

Notes:

- The program generates a script that contains the commands required to retrust every trusted program and secured file in the database.
- The output is directed to the standard output device. To direct the output to a file, use the redirection commands.
- If you omit the -l parameter, seretrust obtains the list of programs and files to be retrusted from the eTrust AC service.

seversion

Displays the version information of an eTust Access Control and eTrust Single Sign-On program module. The following data can be displayed:

- The global and minor version numbers.
- The date and timethe module was compiled.
- The station the module was compiled on.
- The file's Snefru digital signature.

Syntax

```
seversion switches module
```

Switches

-a

Displays the requestd information in the form of a table.

-g

Displays only the global version number.

-h

Displays the help screen.

-m Displays only the minor version number. Titles are omitted.

-s Displays only the Snefru number. Titles are omitted.

-l Displays the included libraries.

-5 Displays MD5 signature.

sewhoami

The sewhoami utility displays the user name as it is known to the eTrust Acces control authorization daemon. The sewhoami utility is similar to the whoami utility provided by the Unix system, but it produces different and often more useful information.

- If the user executes an "su" command and then executes the Unix whoami utility, the whoami utility displays the user name according to the user ID aquired after executing the "su" command.
- If the user executes an "su" command and then executes the eTrust Access Control sewhoami utility, the sewhoami utility displays the original login ID of the user. Sewhoami also displays authorization information

Syntax

```
sewhoami switches
```

Switches

-a Displays the user's credentials, which are the contents of the user's ACEE.

-d Displays the ACEE handle associated with the user and the handle'[s name in the eTrust Access Control database.

Services in Detail

In this section, eTrust AC services are listed in alphabetical order. A detailed description of each is given.

sepmdd

sepmdd is the PMDB service. It performs the following functions:

- administers the eTrust AC and Windows databases of the Policy Model
- administers the subscribers' database
- propagates changes from the PMDB to the subscriber databases

SeOSAgent starts the sepmdd service. There is no need to run sepmdd explicitly. Sepmdd runs as the service 'SeOS Policy Model' under Windows. The two possible states for each Policy Model are Started and Stopped.

The PMDBs are stored in a common directory. The registry value _pmd_directory_ in the subkey HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\Pmd specifies the name of the common directory:

Each Policy Model resides in a subdirectory of the common directory. The name of the Policy Model is the name of the subdirectory in which it resides.

When sepmdd starts, it checks whether any subscriber databases need to be updated and, if necessary, updates them. After this startup process, the sepmdd service waits for user requests. User requests are sent by the Policy Model management utility sepmd and by selang using the eTrust AC agent SeOS Agent.

When a request is received, sepmdd applies it to the PMDB and sends the result back to the user. If the request should be propagated, sepmdd propagates the update to its subscriber databases.

The sepmdd service tries to update a subscriber database for 30 seconds. If this elapses and the service does not succeed in updating a subscriber, it skips that particular subscriber and tries to update the remainder of the subscribers on its list. After it completes its first scan of the subscriber list, sepmdd then performs a second scan, in which it tries to update the subscribers that it did not succeed in updating during its first scan. During the second scan, it tries to update a subscriber until the connect system call times out (approximately 90 seconds).

If a subscriber is unavailable during the second scan, sepmdd attempts to send it updates every 30 minutes.

Since the updates must be sent in the order in which they are received, sepmdd does not send subsequent updates to the subscriber database until it becomes available.

Each time sepmdd fails to update a subscriber database, a warning message is written in the Policy Model error log. For more information about the Policy Model error log, see the section, "Managing Policy Models" in the *Administrator Guide.*

eTrust AC tries to fully qualify subscribers as they are added or deleted from the Policy Model.

To remove a subscriber from the list of unavailable subscribers, enter:

```
sepmd -r policyModel subscriber
```

If a subscriber database rejects an update, as can occur if the subscriber database differs from the PMDB, sepmdd writes an error message in the Policy Model error log and continues.

To view the error log, enter the following command on the host where the PMDB resides:

```
sepmd -e policyModel
```

To deactivate the Policy Model service, enter:

```
sepmd -k policyModel
```

Filter Mechanism

You may want your PMDB to update the subscriber stations below it selectively. To define which records to be sent to the subscriber stations, set the registry key string value to a filter file. Updates to the subscriber stations are then limited to the records that pass the filter file. Here is an example:

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\Pmd\
PolicyModelName\Filter
```

A filter file consists of lines with six fields per line. The fields contain this information:

The form of access permitted or prohibited
Valid values are: CREATE, EDIT, MODIFY, DELETE, AUTHORIZE_MODIFY, AUTHORIZE_DELETE, JOIN_MODIFY, JOIN-_DELETE

The environment affected
Valid values are: eTrust, UNIX, Native

The class of the record
Valid values include all classes in eTrust AC, including user-defined classes.

The objects within the class that the rule covers
For example: User1, AuditGroup, or COM2.

The properties that the record grants or cancels
For example, including GROUPS and FULLNAME in the filter line for user records means that any command having those user properties is filtered. You must enter each property exactly as it appears in the chapter “eTrust Environment Classes and Properties.”

Whether such records should be forwarded to the subscriber station
Valid values are: PASS, NOPASS

Note: You can use an asterisk to mean "all possible values" in any field. If more than one line covers the same records, the first applicable line is used.

In each line of the filter file, spaces separate the fields. In fields with more than one value, separate the values with semicolons. Any line beginning with "#" is considered a comment line. Empty lines are not allowed. Here is an example of a line from a filter file:

`CREATE`	`eTrust`	`USER`	`*`	`FULLNAME;OBJ_TYPE`	`NOPASS`
form of access	environment	class	record name (* =all)	properties	treatment

If, for example, the file with this line is named Printer1_Filter.flt and the registry key HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\Pmd\PM-\Filter contains the line "D:\Program Files\CA\eTrustAccessControl\data\Printer1_Filter.flt," then Policy Model PM-1 will not send records that create new eTrust AC users with the FULLNAME and OBJ_TYPE (admin, auditor, and so on). The asterisk means "regardless of name."

The selang commands that are relevant for each access value are:

Access	selang Command
CREATE	newres, newusr, newgrp, newfile
DELETE	rmres, rmusr, rmgrp, rmfile, join- (UNIX)
EDIT	editres, editusr, editgrp, editfile
MODIFY	chres, chusr, chgrp, chfile, join (UNIX)
AUTHORIZE_MODIFY	authorize
AUTHORIZE_DELETE	authorize-
JOIN_MODIFY	join
JOIN_DELETE	join-

Note: eTrust AC does not validate rules; therefore, if you enter an invalid value in a rule, the rule will never match an update transaction.

Registry Subkeys

Each PMDB has its own registry subkey under:
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\
eTrustAccessControl\Pmd

This subkey contains the values that define and determine the activity of the PMDB. The sepmdd utility creates a subkey, if it does not already exist, with the minimum number of entries needed.

The sepmdd utility uses the following registry subkey values on the station on which the Policy Model resides:

Value	Description	Default
Min_Retrys	The minimum number of attempts made to access an unavailable subscriber before sepmdd becomes inactive. The actual number of retries may be larger than the value specified here. Note that if sepmdd stops running without updating the subscriber, it attempts to update the subscriber when it next starts.	4
Active_Policy	The name of the active Policy Model.	*PolicymodelName*
Always_Propagate	Determines whether the Policy Model propagates transactions that it cannot execute itself to subscribers. For example, a transaction may fail under Windows but execute when propagated to UNIX hosts. If this value is set to no, a command that fails to execute is not propagated.	yes
Auto_Truncate	Truncates propagated entries from the update file. If this value is set to ‘no’, you can truncate the update file manually. See sepmd utility, -t switch in this guide.	yes
Filterj	The directory path of the filter file	
Parent_PMD	The directory path of the parent PMD, if there is one.	

Other Files

No other special files are used.

Notes

- When you use selang and choose a Policy Model as your target (using hosts pmd@hostname), queries to sepmdd apply to the PMDB but not to the various subscribers' databases.
- Ensure that a PMDB does not become a subscriber of itself. If a PMDB is subscribed to itself, the Policy Model may block or the network may become overloaded, filling the disk in the process.
- You cannot specify more than one user with the newusr command when you are working in the UNIX environment using selang to update a Policy Model.
- You cannot specify more than one group in the newgrp command when you are working in the UNIX environment using selang to update a Policy Model.
- When updating UNIX file attributes from selang, the Policy Model generates a message stating that the command has been passed to its subscribers.
- When working on a Policy Model, you cannot query the status of Windows file attributes.
- The sepmdd service remains active indefinitely until deactivated with the -k options.

See Also

seagent, sepmd, and sepmdadm in the UNIX *Utilities Guide*.

Chapter

6

eTrust Environment Classes and Properties

This chapter contains a description of each property in every class defined in the eTrust AC database. Arranged alphabetically by class, the chapter provides information on which properties you can modify, which selang parameters you use to update these properties, and which commands contain these parameters.

Note: Some classes, such as USER, GROUP, or FILE are found in both the eTrust and the native environments. In those cases where the same property names are used in both environments, the description indicates whether the properties are identical or separate.

Class and Property Information

For each class, all modifiable and non-modifiable properties are listed. Both types of properties contain the following information:

- **Property Name**—The name of the property in the eTrust AC database.
- **Description**—A description of the function and purpose of the property.

In addition, the modifiable properties include information on the selang commands and parameters used to modify the properties.

Note: The symbol [-] used with a parameter indicates that the parameter may be deleted from the database by typing it with a minus sign. For example, **comment** (with appropriate text) adds a comment to a database record; comment**-** removes the comment from the database. You cannot use parameters with a minus sign when creating a record.

In the descriptive material before the property lists, the **key** of the class record is defined. The key is the record identifier, which you specify when you create a new record. Once created, it becomes a non-modifiable property.

Two types of classes in the database are accessor classes and resource classes. You operate on records in the accessor classes—USER and GROUP—with different selang command sets than you use for the resource classes. (In Policy Manager, you use different workspaces.)

- Use chusr, editusr, and newusr to operate on USER class records.
- Use chgrp, editgrp, and newgrp to operate on GROUP class records.
- Use chres, editres, and newres to operate on records in any of the resource classes. If the resource is a file, you may also use the chfile or editfile commands.
- Use showgrp, showres, showfile, or showusr to list the properties of a record.
- Use authorize and authorize– to add, change, or remove ACLs for resource records.

Note: "edit" is equivalent to "new" and "change". That is, you can use editusr instead of either chusr or newusr.

For more information about the selang commands, see the chapter "selang Commands in the eTrust Environment."

Accessor Classes

This section describes the eTrust AC database accessor classes: USER and GROUP.

USER Class

Each record in the USER class defines a user in the database.

The key of the USER record is the name of the user—the name entered by the user when logging into the system. The following list describes the properties that you can modify in a USER class record.

Modifiable Properties

APPLIST
Used by eTrust™ Single Sign-On and eTrust™ Web Access Control.

APPLIST_TIME
Used by eTrust Single Sign-On and eTrust Web Access Control.

APPLS
The list of applications that the user is explicitly allowed to access. Used by eTrust Single Sign-On and eTrust Web Access Control.

AUDIT_MODE

Identifies the activities that eTrust AC records in the audit log. You can specify any combination of the following activities:

- No logging
- All activities recorded in the trace file (UNIX only)
- Unsuccessful login attempts
- Successful logins
- Failed access attempts to resources protected by eTrust AC
- Successful accesses to resources protected by eTrust AC

A value for the AUDIT_MODE property in a USER record overrides a value in a GROUP record.

Use the audit parameter with the chusr, editusr, or newusr command to modify this property.

In the Audit Mode of the Policy Manager interface, there is an option Trace. The description about that option is not listed here in the description.

AUTHNMTHD

The authentication method or methods to be used with the user, from method 1 to method 32, or none. Used by eTrust Single Sign-On and eTrust Web Access Control.

BADPASSWD

Used by eTrust Single Sign-On and eTrust Web Access Control.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

CATEGORY

One or more security categories assigned to a user. You can specify any security category that is defined in the CATEGORY class. If a resource has one or more security categories assigned to it, a user is granted access to the resource only if the user security category list contains all the security categories assigned to the resource.

Use the category[–] parameter with the chusr, editusr, and newusr commands to modify this property.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization. The information in this property is identical to that in the COMMENT property in the native environment. You cannot change them separately.

Use the comment[–] parameter with the chusr, editusr, and newusr commands to modify this property.

COUNTRY

A string that specifies a country descriptor for a user. This string is part of the X.500 naming scheme. eTrust AC does not use it for authorization.

Use the country parameter with the chusr, editusr, and newusr commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access resources. A value for the DAYTIME property in the USER record overrides a value in the GROUP record. The information in this property is identical to that in the DAYTIME property in the native environment, except that the eTrust AC database can accept times that include minutes.

Use the restrictions (days and time) parameter with the chusr, editusr, and newusr commands to modify this property.

EMAIL

The email address of the user, up to 128 characters.

Use the email parameter with the chusr, editusr, and newusr commands to modify this property.

EXPIRE_DATE

The date on which a USER record expires and becomes invalid. A value for the EXPIRE_DATE property in a USER record overrides a value in a GROUP record. To reinstate the expired record, use the chusr command with the expire– parameter. You cannot resume an expired user. You can resume a suspended user by specifying a resume date.

Use the expire or expire- parameter with the chusr, editusr, or newusr command to modify this property.

FULLNAME

The full name associated with a user, an alphanumeric string of up to 47 characters. eTrust AC uses the full name to identify the user in audit log messages, but not for authorization.

Use the name parameter with the chusr, editusr, or newusr command to modify this property.

GAPPLS

The list of application groups that the user is authorized to access. Used by eTrust Single Sign-On and eTrust Web Access Control.

GRACELOGIN

The number of grace logins a user has after a password expires. When the number of grace logins is exceeded, the user is denied access to the system and must contact the system administrator for a new password.

The number of grace logins must be between 0 and 255. **If this value is 0, the user cannot log in.**

A value for the GRACELOGIN property in a USER record overrides a value for NGRACE in a GROUP record. Both override the PASSWDRULES property in the SEOS class record.

Use the grace[–] parameter with the chusr, editusr, and newusr commands to modify this property.

GROUPS

The list of user groups (GROUP records) a USER record belongs to. This property also contains any group authorities, such as group administration authority (GROUP-ADMIN), assigned to the user for each group the user belongs to.

The group list contained in this property may be different from the one in the native environment GROUPS property.

Use the group parameter with the join[–] command to modify this property.

HOMEDIR

(UNIX only) A string specifying the user's home directory. Users log in to their home directories automatically. Used by eTrust Single Sign-On and eTrust Web Access Control.

Use the homedir parameter with the chusr, editusr, or newusr command to modify this property.

INACTIVE

The number of days of inactivity that must pass before the system changes the status of a user to inactive. When the specified number of days is exceeded, the account is marked as inactive and the user cannot log in.

A value for the INACTIVE property in a USER record overrides a value in a GROUP record. Both override the INACT property in the SEOS class record.

Note: In the user record, inactive users are not marked. To identify inactive users, you must compare the Last Accessed Time value with the Inactive Days value.

Use the inactive parameter with the chusr, editusr, and newusr commands to modify this property.

LOCALAPPS

Used by eTrust Single Sign-On and eTrust Web Access Control.

LOCATION

A string used to store a user location. eTrust AC does not use this information for authorization.

Use the location parameter with the chusr, editusr, and newusr commands to modify this property.

LOGININFO

A section of the record containing information needed to log the user into a specific application and audit data. LOGININFO contains a separate list for each application that the user is authorized to access. Used by eTrust Single Sign-On and eTrust Web Access Control.

LOGSHIFT

Indicates whether to allow login outside of the shift time frame. eTrust AC writes an audit record in the audit log for this event.

MAXLOGINS

The maximum number of concurrent logins (terminal sessions) a user is allowed, after which the user is denied access. A zero value indicates no maximum and the user can log in to any number of terminal sessions concurrently. The value must be either zero or greater than 1 if the user needs to log in and run selang or otherwise administer the database, because eTrust AC considers each task (login, selang, GUI, and so forth) to be a terminal session.

A value for the MAXLOGINS property in a USER record overrides a value in a GROUP record. Both override the MAXLOGINS property in the SEOS class record. The value in the SEOS record is the default value used when there is no explicit value in the accessor record.

Use the maxlogins parameter with the chusr, editusr, and newusr commands to modify this property.

MIN_TIME

The minimum time in days allowed between password changes for the user.

A value for the MIN_TIME property in a USER record overrides a value in a GROUP record. Both override the PASSWDRULES property in the SEOS class record.

Use the min_life[–] parameter with the chusr, editusr, and newusr commands to modify this property.

NOTIFY

The user notified when a resource generates an audit event. eTrust AC creates a special audit record that can be directed to the specified email address using selogrd**.**

Use the notify[–] parameter with the chusr, editusr, and newusr commands to modify this property.

OBJ_TYPE

Specifies the user authority attributes, which may be one or more of the following:

ADMIN—allows the user to perform most administrative functions, similar to root in the UNIX environment.

AUDITOR—allows the user to monitor the system, list information in the database, and set the audit mode for existing records.

IGN_HOL—allows the user to log in during any period of time defined in a HOLIDAY record.

OPERATOR—allows the user to list everything in the database and to use the secons utility.

PWMANAGER—allows the user to modify the password settings of other users and to enable a user account that has been disabled by serevu.

SERVER—allows a process to ask for authorization for users and can issue the SEOSROUTE_VerifyCreate API call.

A user can have more than one attribute assigned.

See the *Administrator Guide* for more information on special attributes that you can assign to a user.

Use the admin[-], auditor[-], ign_hol[-], operator[-], pwmanager[-], or server[-] parameter with the chusr, editusr, and newusr commands to modify this property.

OIDCRDDATA

Used by eTrust Single Sign-On and eTrust Web Access Control.

ORG_UNIT

A string that stores information on the organizational unit in which the user works. This string is part of the X.500 naming scheme. eTrust AC does not use it for authorization.

Use the org-unit parameter with the chusr, editusr, and newusr commands to modify this property.

ORGANIZATION

A string that stores information on the organization in which the user works. This string is part of the X.500 naming scheme. eTrust AC does not use it for authorization.

Use the organization parameter with the chusr, editusr, and newusr commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chusr, editusr, and newusr commands to modify this property.

PASSWD_INT

The maximum time in days between password changes for users.

A value for the PASSWD_INT property in a USER record overrides the value in a GROUP record. Both override the PASSWDRULES property in the SEOS class record.

Use the interval[–] parameter with the chusr, editusr, or newusr command to modify this property.

PHONE

A string that can be used to store a user telephone number. This information is not used for authorization.

Use the phone parameter with the chusr, editusr, and newusr commands to modify this property.

POLICYMODEL

The PMDB that receives new passwords when you change user passwords with the sepass utility. The passwords are **not** sent to the Policy Model defined by the parent_pmd or passwd_pmd Windows registry sub-key entries if a value is entered for this property.

Use the pmdb[–] parameter with the chusr, editusr, and newusr commands to modify this property.

PROFILE

A string that specifies a path to the user's profile. This string can include a local absolute path, or a UNC path.

Use the profile[-] parameter with the chusr, editusr, or newusr command to modify this property.

PWD_AUTOGEN

Indicates whether the user password is automatically generated. Used by eTrust Single Sign-On and eTrust Web Access Control. The default is no.

PWD_SYNC

Indicates whether the user password is automatically kept identical for all user applications. Used by eTrust Single Sign-On and eTrust Web Access Control. The default is no.

RESUME_DATE

The date on which a suspended USER account becomes valid.

See SUSPEND_DATE for an explanation of how RESUME_DATE and SUSPEND_DATE work together.

REVOKE_COUNT

Used by eTrust Single Sign-On and eTrust Web Access Control.

SCRIPT_VARS

Used by eTrust Single Sign-On and eTrust Web Access Control, a variables list with the variable values of the application script that are saved per application.

SECLABEL

The security label of a user. A security label associates a security level with security categories.

When applicable, a security label overrides any specific security level and category assignments in the record. Assigning a security label is equivalent to explicitly assigning the level and categories of the label to the user. The specified security label must be defined as a record in class SECLABEL. When a USER record includes a security label, the user is granted access to a resource only if both of the following are true:

- The user security level specified in the security label is equal to or greater than the resource security level.

- All categories specified in the resource record are included in the security category list of the user security label.

Use the label[–] parameter with the chusr, editusr, and newusr commands to modify this property.

SECLEVEL

The security level of the user. The security level is a positive integer between 0 and 255. A value of 0 means no security level is assigned. If a resource has a security level assigned to it, the user is granted access to the resource only if the security level of the user is equal to or greater than the security level of the resource.

Use the level[–] parameter with the chusr, editusr, and newusr commands to modify this property.

SESSION_GROUP

Used by eTrust Single Sign-On. This property assigns an SSO session group to a user. The SESSION_GROUP property is a string with a maximum length of 16 characters.

In Windows, an administrator can enter a session group new name if the preferred name is not in the drop-down list.

SHIFT

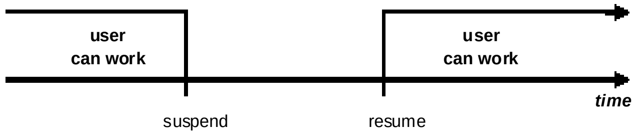
Used by eTrust Single Sign-On and eTrust Web Access Control.

SUSPEND_DATE

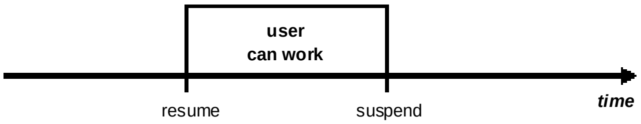
The date on which a user account is suspended and becomes invalid.

If the user has a resume date (see RESUME_DATE) that is earlier than the suspend date, the record is also invalid *before* the resume date.

If the suspend date for a record precedes its resume date, the user can work before the suspend date and after the resume date.



If the resume date for a record precedes its suspend date, then the user can work only between the resume and suspend dates.



A value for the SUSPEND_DATE property in a USER record overrides the value in a GROUP record.

Use the suspend[–] parameter with the chusr, editusr, or newusr command to modify this property.

Non-Modifiable Properties

The following properties contained in the record are modified automatically by eTrust AC and cannot be modified with selang or the Policy Manager interface.

CREATE_TIME
The date and time the record was created.

LAST_ACC_TERM
The terminal from which the last login was performed.

LAST_ACC_TIME
The date and time of the last login.

OLD_PASSWD
A list of previous passwords assigned to the user. The user may not choose a new password from this list. The maximum number of passwords saved in this list is determined by the setoptions command. This data is encrypted.

PASSWD_A_C_W
The ADMIN user who last changed the user password for this record.

PASSWD_L_A_C
The date and time on which an administrator last updated the password.

PASSWD_L_C
The date and time on which the user last updated the password.

REVACL
Lists the ACLs (access control lists) of the accessor.

SUSPEND_WHO
The administrator who activated the suspend date.

UALIAS
All the aliases of a specific user defined to one or more authentication hosts. Used by eTrust Single Sign-On and eTrust Web Access Control.

UPDATE_TIME
The date and time the record was last modified.

UPDATE_WHO
The administrator who performed the update.

GROUP Class

Each record in the GROUP class defines a group of users in the database. The properties of the group–privileges and restrictions–apply to each member unless specified in a USER record. Then the user can work only between the resume and suspend dates.

The key of the GROUP class record is the name of the group—the name that identifies the record to eTrust AC. The following list describes the properties that you can modify in a GROUP class record.

Modifiable Properties

APPLS

The list of applications that the group is authorized to access. Used by eTrust Single Sign-On and eTrust Web Access Control.

AUDIT_MODE

Identifies the activities that eTrust AC records in the audit log. You can specify any combination of the following activities:

- No logging
- All activities recorded in the trace file (UNIX only)
- Unsuccessful login attempts
- Successful logins
- Failed access attempts to resources protected by eTrust AC
- Successful accesses to resources protected by eTrust AC

A value for the AUDIT_MODE property in a USER record overrides a value in a GROUP record.

Use the audit parameter with the chgrp, editgrp, or newgrp command to modify this property.

AUTHNMTHD

The authentication method or methods to be used with the group record; from method 1 to method 32, or none. Used by eTrust Single Sign-On and eTrust Web Access Control.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization. The information in this property is identical to that in the COMMENT property in the native environment. You cannot change them separately.

Use the comment[–] parameter with the chgrp, editgrp, and newgrp commands to modify this property.

DAYTIME

Part of the profile feature. The day and time restrictions that govern when a user can access resources. A value for the DAYTIME property in the USER record overrides a value in the GROUP record. The information in this property is identical to that in the DAYTIME property in the native environment, except that the eTrust AC database can accept times that include minutes.

Use the restrictions(days and time) parameter with the chgrp, editgrp, and newgrp commands to modify this property.

EXPIRE_DATE

The date on which a USER record expires and becomes invalid. A value for the EXPIRE_DATE property in a USER record overrides a value in a GROUP record.

To reinstate the expired record, use the chgrp command with the expire– parameter. You cannot resume an expired group. You can resume a suspended group by specifying a resume date.

Use the expire[–] parameter with the chgrp, editgrp, or newgrp command to modify this property.

FULLNAME

The full name associated with a group, an alphanumeric string of up to 47 characters. eTrust AC uses the full name to identify the group in audit log messages, but not for authorization.

Use the name parameter with the chgrp, editgrp, or newgrp command to modify this property.

GAPPLS

The list of application groups that the group is authorized to access. Used by eTrust Single Sign-On and eTrust Web Access Control.

GROUP_MEMBER

The groups that are members of this group.

HOMEDIR

The home directory assigned to a new group member. Specify the full path up to 255 alphanumeric characters.

Use the homedir parameter with the chgrp, editgrp, or newgrp command to modify this property.

INACTIVE

Part of the profile feature. The number of days of inactivity that must pass before the system changes the status of group members to inactive. When the specified number of days is exceeded, the accounts are marked as inactive and the group members cannot log in.

A value for the INACTIVE property in a USER record overrides a value in a GROUP record. Both override the INACT property in the SEOS class record.

Note: In the user record, inactive users are not marked. To identify inactive users, you must compare the Last Accessed Time value with the Inactive Days value.

Use the inactive parameter with the chgrp, editgrp, and newgrp commands to modify this property.

MAXLOGINS

Part of the profile feature. The maximum number of concurrent logins (terminal sessions) a user in the group is allowed, after which the user is denied access. A zero value indicates no maximum and users in the group can log in to any number of terminal sessions concurrently. The value must be either zero or greater than 1 if users in the group need to log in and run selang or otherwise administer the database because eTrust AC considers each task (login, selang, GUI, and so forth) to be a terminal session.

A value for the MAXLOGINS property in a USER record overrides a value in a GROUP record. Both override the MAXLOGINS property in the SEOS class record. The value in the SEOS record is the default value used when there is no explicit value in the accessor record.

Use the maxlogins parameter with the chgrp, editgrp, and newgrp commands to modify this property.

MEMBER_OF

The groups that this group is a member of.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chgrp, editgrp, and newgrp commands to modify this property.

PASSWDRULES

Part of the profile feature. Specifies the password rules. This property contains a number of fields that determine how eTrust AC handles password protection. For a complete list of the rules, see the modifiable property PROFILE of the USER class.

Use the password parameter and the rules or rules- option with the setoptions command to modify this property.

POLICYMODEL

Part of the profile feature. The PMDB, which receives new passwords when you change user passwords with the sepass utility. The passwords are **not** sent to the Policy Model defined by the **parent_pmd** or **passwd_pmd** Windows registry sub-key entries if a value is entered for this property.

Use the pmdb[–] parameter with the chgrp, editgrp, and newgrp commands to modify this property.

PWD_AUTOGEN

Indicates whether the group password is automatically generated. The default is no. Used by eTrust Single Sign-On and eTrust Web Access Control.

PWD_SYNC

Indicates whether the group password is automatically kept identical for all group applications. The default is no. Used by eTrust Single Sign-On and eTrust Web Access Control.

PWPOLICY

The record name of the password policy for the group. A password policy is a set of rules for checking the validity of a new password and for defining when a password expires. The default is no validity check. Used by eTrust Single Sign-On and eTrust Web Access Control.

RESUME_DATE

Part of the profile feature. The date on which a USER record becomes valid. A value for the RESUME_DATE property in a USER record overrides the value in a GROUP record.

See SUSPEND_DATE for an explanation of how RESUME_DATE and SUSPEND_DATE work together.

Use the resume[–] parameter with the chgrp, editgrp, and newgrp commands to modify this property.

SHELL

(UNIX only) The shell program assigned to a new UNIX user when the user is a member of this group.

Use the shellprog parameter with the chgrp, editgrp, or newgrp command to modify this property.

SUPGROUP

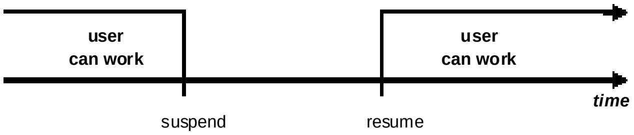
The name of the parent group (“superior” group).

Use the parent[–] parameter with the chgrp, editgrp, or newgrp command to modify this property.

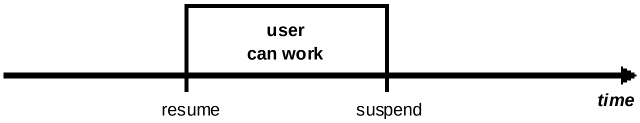
SUSPEND_DATE

The date on which group member records are suspended and become invalid. If the group has a resume date (see RESUME_DATE) that is earlier than the suspend date, the user records are also invalid *before* the resume date.

If the suspend date for a record precedes its resume date, the user can work before the suspend date and after the resume date.



If the resume date for a record precedes its suspend date, the user can work only between the resume and suspend dates.



A value for the SUSPEND_DATE property in a USER record overrides the value in a GROUP record.

Use the suspend[–] parameter with the chgrp, editgrp, or newgrp command to modify this property.

USERLIST

The list of users that belong to a group.

The user list contained in this property may be different from the one in the native environment USERS property.

Use the username parameter with the join[–] command to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

PROFUSR

A list of the users associated with this profile group.

REVACL

Lists the ACLs (access control lists) of the accessor.

SUBGROUP

The list of groups that have this group as a parent.

SUSPEND_WHO

The administrator who activated the suspend date.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

Note: The properties MIN_TIME, NGRACE, and PASSWD_INT from previous versions of eTrust AC are now part of the PASSWDRULES property.

Resource Classes

This section contains a general description of each eTrust AC database resource class and is organized alphabetically by class. Most of the classes are implemented in eTrust AC for both UNIX and Windows systems.

ADMIN Class

Each record in the ADMIN class contains the definitions that allow non-ADMIN users to administer specific classes. You must create an ADMIN record to represent each eTrust AC class that delegated users will administer. The record contains a list of accessors with the access authorities of each, and also supports conditional access control lists (CACLs).

The key of the ADMIN class record is the name of the class being protected. The following list describes the properties that you can modify in an ADMIN class record.

Modifiable Properties

ACL

The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the ADMIN class are:
  - **all**—Allows accessors to perform all operations permissible for the class
  - **create**—Allows accessors to create an ADMIN record
  - **delete**—Allows accessors to delete an ADMIN record
  - **join**—Allows accessors to add a group to a USER record and to complete the linking of a user to a group. However, the accessor must also have modify access
  - **modify**—Allows accessors to modify existing records, including adding user names to GROUP records. To complete the linking of a user to a group, however, the accessor must also have join access
  - **none**—Does not allow the accessor to perform any operations
  - **password**—Allows accessors to change the passwords of other users (This access type affects only the USER class.)
  - **read**—Allows accessors to list records in all classes

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

CALACL

The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Calendar reference—**A reference to a calendar in Unicenter TNG.

- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the ADMIN class are:
    - **all**—Allows accessors to perform all operations permissible for the class
    - **create**—Allows accessors to create an ADMIN record
    - **delete**—Allows accessors to delete an ADMIN record
    - **join**—Allows accessors to add a group to a USER record and to complete the linking of a user to a group. However, the accessor must also have modify access
    - **modify**—Allows accessors to modify existing records, including adding user names to GROUP records. To complete the linking of a user to a group, however, the accessor must also have join access
    - **none**—Does not allow the accessor to perform any operations
    - **password**—Allows accessors to change the passwords of other users (This access type affects only the USER class.)
    - **read**—Allows accessors to list records in all classes

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

CATEGORY

One or more security categories assigned to a resource. You can specify any security category that is defined in the CATEGORY class. If a resource has one or more security categories assigned to it, a user is granted access to the resource only if the user security category list contains ***all*** the security categories assigned to the resource.

Use the category[–] parameter with the chres, editres, and newres commands to modify this property.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.
- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the ADMIN class are:
  - **all**—Prevents accessors from performing any operations for the class
  - **create**—Prevents accessors from creating an ADMIN record
  - **delete**—Prevents accessors from deleting an ADMIN record
  - **join**—Prevents accessors from adding a group to a USER record
  - **modify**—Prevents accessors from modifying existing records, including adding user names to GROUP records.
  - **none**—Allows accessors to perform any operations
  - **password**—Prevents accessors from changing the passwords of other users
  - **read**—Prevents accessors from listing records in all classes

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

NOTIFY

The user notified when a resource generates an audit event. eTrust AC creates a special audit record that can be directed to the specified email address using selogrd**.**

Use the notify[–] parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

PACL

The program access control list—an ACL that applies to accessors when the access request is made by a specific program or a program that matches a program-name pattern.

If you are using a pattern, then the resource that is protected by the PACL can be accessed using a program that matches the pattern. If a program matches several patterns, the longest pattern takes precedence.

Each element in the program access control list contains the following information:

- **Program reference**—A reference to a record in the PROGRAM class, either specifically or by name-pattern matching.
- **Accessor reference**—A reference to an accessor (a user or group).
- **Permitted access**—The access allowed to the accessor when using the specified program. Refer to the ACL property for a list of valid values.

Use the via(pgm) parameter with the authorize command to add programs, accessors, and their access types to, or authorize– or remove them from, the ACL property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.
- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

SECLABEL

The security label of a resource. A security label associates a security level with security categories.

When applicable, a security label overrides any specific security level and category assignments in the record. Assigning a security label is equivalent to explicitly assigning the level and categories of the label to the user. The specified security label must be defined as a record in class SECLABEL. When a USER record includes a security label, the user is granted access to a resource only if both of the following are true:

- The user security level specified in the security label is equal to or greater than the resource security level.
- All categories specified in the resource record are included in the security category list of the user security label.

Use the label[–] parameter with the chres, editres, and newres commands to modify this property.

SECLEVEL

The security level of the user or resource. The security level is a positive integer between 0 and 255. A value of 0 means no security level is assigned. If a resource has a security level assigned to it, the user is granted access to the resource only if the security level of the user is equal to or greater than the security level of the resource.

Use the level[–] parameter with the chres, editres, and newres commands to modify this property.

UACC

The default access for the resource, which indicates the access granted to accessors who are not defined to eTrust AC or who do not appear in the ACL of the resource. Refer to the ACL property of the resource for a list of valid values.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[–] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

AAUDIT

Displays the type of activity that eTrust AC is auditing.

CREATE_TIME

The date and time the record was created.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

AGENT Class

Each record in the AGENT class defines an object that is used as an agent by eTrust Single Sign-On or eTrust Web Access Control.

The key of the AGENT class record is the name of the agent. The following list describes the properties that you can modify in an AGENT class record.

Modifiable Properties

AGENT_TYPE

The type of agent.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[-] parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

AGENT_TYPE Class

Each record in the AGENT_TYPE class defines an agent type used by eTrust Single Sign-On or eTrust Web Access Control.

The key of the AGENT_TYPE class record is the type of the agent. The following list describes the properties that you can modify in an AGENT_TYPE class record.

Modifiable Properties

AGENT_FLAG

Contains information about the attribute. The flag can contain the following values:

- **aznchk**—Indicates whether to use this attribute for authorization.
- **predef** (predefined), **freetext** (free text), or **userdir** (user directory)—Specify the source of the user attributes.
- **user** or **group**—These values indicate whether the attribute (accessor) is a user or a group.

AGENT_LIST

A list of objects in the AGENT class that were created with this AGENT_TYPE object as the value for the agent_type parameter; for example, this property is updated implicitly when creating an object in the AGENT class.

CLASSES

A multistring list of the classes or resources that are relevant to this agent.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

APPL Class

Each record in the APPL class defines an application used by eTrust Single Sign-On or eTrust Web Access Control.

The key of the APPL class record is the name of the application. The following list describes the properties that you can modify in an APPL class record.

Modifiable Properties

ACL

The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference**—A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.

- **Permitted access—**The access authority the accessor has to the resource. The valid access authorities for the APPL class are:
  - **execute—**Allows accessors to execute a program. To use this access type, the accessor must also have read access
  - **none**—Does not allow the accessor to perform any operations
  - **read—**Allows accessors to use a file or directory without changing it

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

APPLTYPE

Used by eTrust Single Sign-On and eTrust Web Access Control.

AZNACL

The authorization ACL—an ACL that allows access to a resource based on the resource description. The description is sent to the authorization engine, not the object. The object is most likely not in the database.

CALACL

The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Calendar reference—**A reference to a calendar in Unicenter TNG.
- **Permitted access—**The access authority the accessor has to the resource. The valid access authorities for the APPL class are:
  - **execute—**Allows accessors to execute a program. To use this access type, the accessor must also have read access
  - **none**—Does not allow the accessor to perform any operations
  - **read—**Allows accessors to use a file or directory without changing it

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

CAPTION

The text under the application's icon on the desktop. The caption can contain up to 47 alphanumeric characters. The default is the name of the APPL record.

CMDLINE

The file name of the application executable. Used by eTrust Single Sign-On and eTrust Web Access Control.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

CONTAINED_ITEMS

The record names of the contained applications, if the record is a container.

Use the item[–](*applName*) parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

DIALOG_FILE

The name of the eTrust Web Access Control script in the directory containing the login sequence for the application. The default directory location is /usr/sso/scripts. The default value is "no script".

Use the script[-](*fileName*) parameter with the chres, editres, and newres commands to modify this property.

GROUPS

A list of user groups authorized to use the application.

HOST

The name of the host where the application resides.

Use the host[-](*hostName*) parameter with the chres, editres, and newres commands to modify this property.

ICONFILE

The file name or full path of the file containing the icon representing the application on the desktop. eTrust AC expects to find the icon on the end user's workstation. If just a file name is entered, the search order for the file is as follows:

1. Current directory
2. Directories listed in the PATH environment variable

The default is the default icon of the workstation.

ICONID

The numeric ID (if necessary) of the icon within the icon file. If the ICONID is not specified, the default icon is used.

IS_CONTAINER

Whether the application is a container. The default is “no”.

Use the container[–] parameter with the chres, editres, and newres commands to modify this property.

IS_DISABLED

Whether the application is disabled. If the application is disabled, users cannot log into it. This feature is useful when you change an application and you do not want any users to log in to the application while you make it. The disabled application appears in the application menu list, but if a user selects the application the login is terminated with an appropriate message default is “not disabled”.

IS_HIDDEN

Whether the application icon appears on the desktop even for users who can invoke it. You may want to hide a *master* application, for example an application that only serves the purpose of supplying passwords to other applications. The default is “not hidden”.

Use the hidden[–] parameter with the chres, editres, and newres commands to modify this property.

IS_SENSITIVE

Whether re-authentication is required when the user opens the application after a preset time. The default is “not sensitive”.

Use the sensitive[-] parameter with the chres, editres, and newres commands to modify this property.

LOGIN_TYPE

The way user passwords are provided. The value is **pwd** (plain password), **otp** (One Time Password), **appticket** (a proprietary ticket for mainframe application authentication)., **none** (no password required), or **passticket** (a one-time password replacement format created by IBM and used by mainframe security packages). The default is pwd.

Use the login_type(*value*) parameter with the chres, editres, and newres commands to modify this property.

MASTER_APPL

The record name of the application that supplies the password to other applications. The default is no master.

Use the master[-](*applName*) parameter with the chres, editres, and newres commands to modify this property.

MON_RULES_FILE

In UNIX dbdump only

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.
- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the APPL class are:
  - **execute—**Prevents accessors from executing a program. To use this access type, the accessor must also have read access
  - **none**—Allows accessors to perform any operations
  - **read**—Prevents accessors from viewing a file

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

NOTIFY

The user notified when a resource generates an audit event. eTrust AC creates a special audit record that can be directed to the specified email address using selogrd**.**

Use the notify[–] parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

PGMDIR

A directory, or a list of directories, where the application's executable file resides. Used by eTrust Single Sign-On and eTrust Web Access Control.

PWD_AUTOGEN

Indicates whether the application password is automatically generated by eTrust Web Access Control. The default is no.

PWD_SYNC

Indicates whether the application password is automatically kept identical to those of the other applications. The default is no.

PWPOLICY

The record name of the password policy for the application. A password policy is a set of rules for checking the validity of a new password and for defining when a password expires. The default is no validity check.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

all—All access requests are audited.

allow—All granted access requests are audited.

deny—Only denied access requests are audited; this is the default.

none—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

SCRIPT_POSTCMD

Indicates whether one or more commands are executed after the login script.

SCRIPT_PRECMD

Indicates whether one or more commands are executed before the login script.

SCRIPT_VARS

Used by eTrust Single Sign-On and eTrust Web Access Control, a variables list with the variable values of the application script that are saved per application.

TKTKEY

Used by eTrust Single Sign-On only.

TKTPROFILE

Used by eTrust Single Sign-On only.

UACC

The default access for the resource, which indicates the access granted to accessors who are not defined to eTrust AC or who do not appear in the ACL of the resource. Refer to the ACL property of the resource for a list of valid values.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[–] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

AUTHHOST Class

Each record in the AUTHHOST class defines an authentication host in eTrust Single Sign-On and eTrust Web Access Control.

The key of the AUTHHOST class record is the name of the authorization host. The following list describes the properties that you can modify in an AUTHHOST class record.

Modifiable Properties

ACL

The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the AUTHHOST class are:
  - **none**—Does not allow the accessor to perform any operations
  - **read**—Allows accessors to log in from an authenticated host

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

AUTH_METHOD

In UNIX dbdump only.

AZNACL

The authorization ACL—an ACL that allows access to a resource based on the resource description. The description is sent to the authorization engine, not the object. The object is most likely not in the database.

CALACL

The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Calendar reference—**A reference to a calendar in Unicenter TNG.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the AUTHHOST class are:
  - **none**—Does not allow the accessor to perform any operations
  - **read**—Allows accessors to log in from an authenticated host

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

CATEGORY

One or more security categories assigned to a resource. You can specify any security category that is defined in the CATEGORY class. If a resource has one or more security categories assigned to it, a user is granted access to the resource only if the user security category list contains ***all*** the security categories assigned to the resource.

Use the category[–] parameter with the chres, editres, and newres commands to modify this property for resources.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

CONT_FORMAT

In UNIX dbdump only

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

ETHINFO

Ethernet information for a host.

GROUPS

The list of GAUTHHOST or CONTAINER records a resource record belongs to.

To modify this property in an AUTHHOST class record, you must change the MEMBERS property in the appropriate CONTAINER or GAUTHHOST record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

KEY

Used by eTrust Single Sign-On only.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.
- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the AUTHHOST class are:
  - **none**—Allows accessors to perform any operations
  - **read**—Prevents accessors from logging in from an authenticated host

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

NOTIFY

The user notified when a resource generates an audit event. eTrust AC creates a special audit record that can be directed to the specified email address using selogrd**.**

Use the notify[–] parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

PATH

Used by eTrust Single Sign-On only.

PROPERTIES

In UNIX dbdump only

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.
- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

SECLABEL

The security label of a resource. A security label associates a security level with security categories.

When applicable, a security label overrides any specific security level and category assignments in the record. Assigning a security label is equivalent to explicitly assigning the level and categories of the label to the user. The specified security label must be defined as a record in class SECLABEL. When a USER record includes a security label, the user is granted access to a resource only if both of the following are true:

- The user security level specified in the security label is equal to or greater than the resource security level.
- All categories specified in the resource record are included in the security category list of the user security label.

Use the label[–] parameter with the chres, editres, and newres commands to modify this property.

SECLEVEL

The security level of the user or resource. The security level is a positive integer between 0 and 255. A value of 0 means no security level is assigned. If a resource has a security level assigned to it, the user is granted access to the resource only if the security level of the user is equal to or greater than the security level of the resource.

Use the level[–] parameter with the chres, editres, and newres commands to modify this property.

SEED

Used by eTrust Single Sign-On only.

SERNUM

The serial number of the authentication host.

UACC

The default access for the resource, which indicates the access granted to accessors who are not defined to eTrust AC or who do not appear in the ACL of the resource. Refer to the ACL property of the resource for a list of valid values.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

UNTRUST

Indicates whether the program is trusted or not. If this property is set, no one can run the program. If this property is not set, the other properties listed in the database for the program are used to determine whether the user is authorized to run the program. If a trusted program is changed in any way, eTrust AC automatically sets the UNTRUST property.

Use the trust[–] parameter with the chres, editres, or newres command to modify this property.

USER_FORMAT

Used by eTrust Single Sign-On only.

USERALIAS

Contains all the user’s aliases that are defined to a specific authhost.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[–] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

USER_DIR_PROP

The name of the user's directory.

CALENDAR Class

Each record in the CALENDAR class defines a Unicenter TNG calendar object for user, group, and resource enforced time restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals for enforcement.

The following classes have the CALENDAR property in their class records. Each object in any of these resource classes can be assigned *one and only one* CALENDAR class object.

- ADMIN
- APPL
- AUTHHOST
- CONNECT
- CONTAINER
- DOMAIN (Windows only)
- FILE
- GFILE
- GHOST
- GROUP
- GSUDO

- GTERMINAL
- HOST
- HOSTNET
- HOSTNP
- LOGINAPPL (UNIX only)
- MFTERMINAL
- PROCESS
- PROGRAM
- REGKEY (Windows only)
- SUDO
- SURROGATE
- TCP
- TERMINAL
- USER

The key to the CALENDAR class is the name of the Unicenter TNG calendar. The following list describes the properties that you can modify in a CALENDAR class record.

Modifiable Properties

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment parameter with the chres, editres, and newres commands to modify this property; use the comment- parameter to remove this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

selang syntax

To create or modify a CALENDAR record:

```
{chres | editres | newres} calendar(calendarName) \
{comment(string) owner(ownerName)}
```

To assign a calendar record to a resource:

```
{chgrp | chres | chusr | editgrp | editres | editusr | newgrp | newres | newusr} \
{className resourceName calendar(calendarName) \
groupName calendar(calendarName) \
userName calendar(calendarName) }
```

To remove a calendar record from a resource:

```
{className resourceName calendar-(calendarName) \
groupName calendar-(calendarName) \
userName calendar-(calendarName) }
```

CATEGORY Class

Each record in the CATEGORY class defines a security category in the database. When a user requests access to a resource that has been assigned one or more security categories, eTrust AC compares the list of security categories in the user record with the list of security categories in the resource record. If any security category in the resource record is not in the user record, eTrust AC denies access to the resource. If the user record contains all the security categories specified in the resource record, eTrust AC continues with other authorization checking.

The key of the CATEGORY class record is the name of the security category. The following list describes the properties that you can modify in a CATEGORY class record.

Modifiable Properties

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

Non-Modifiable Properties

CREATE_TIME The date and time the record was created.

UPDATE_TIME The date and time the record was last modified.

UPDATE_WHO The administrator who performed the update.

CONNECT Class

Each record in the CONNECT class defines the target of a connection—a remote host—and controls who can connect to the specified remote host from the local host using a TCP connection.

The key of the CONNECT class record is the name of the remote host to which connections are made. The following list describes the properties that you can modify in a CONNECT class record.

Note: When you use the TCP class for a record, do not use the CONNECT class.

Modifiable Properties

ACL The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference** A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Permitted access** The access authority the accessor has to the resource. The valid access authorities for the CONNECT class are:
  - **none**—Does not allow the accessor to perform any operations
  - **read—**Allows accessors to connect to the remote host

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

CALACL The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Calendar reference—**A reference to a calendar in Unicenter TNG.

- **Permitted access** The access authority the accessor has to the resource. The valid access authorities for the CONNECT class are:
  - **none**—Does not allow the accessor to perform any operations
  - **read—**Allows accessors to connect to the remote host

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

CATEGORY

One or more security categories assigned to a resource. You can specify any security category that is defined in the CATEGORY class. If a resource has one or more security categories assigned to it, a user is granted access to the resource only if the user security category list contains ***all*** the security categories assigned to the resource.

Use the category[–] parameter with the chres, editres, and newres commands to modify this property for resources.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of CONTAINER records a resource record belongs to.

To modify this property in a CONNECT class record, you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.
- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the CONNECT class are:
  - **none**—Allows accessors to perform any operations
  - **read—**Prevents accessors from connecting to the remote host

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

NOTIFY

The user notified when a resource generates an audit event. eTrust AC creates a special audit record that can be directed to the specified email address using selogrd**.**

Use the notify[–] parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

PACL

The program access control list—an ACL that applies to accessors when the access request is made by a specific program or a program that matches a program-name pattern.

If you are using a pattern, then the resource that is protected by the PACL can be accessed using a program that matches the pattern. If a program matches several patterns, the longest pattern takes precedence.

Each element in the program access control list contains the following information:

- **Program reference**—A reference to a record in the PROGRAM class, either specifically or by name-pattern matching.
- **Accessor reference**—A reference to an accessor (a user or group).
- **Permitted access**—The access allowed to the accessor when using the specified program. Refer to the ACL property for a list of valid values.

Use the via(pgm) parameter with the authorize command to add programs, accessors, and their access types to, or authorize– or remove them from, the ACL property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.
- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

SECLABEL

The security label of a resource. A security label associates a security level with security categories.

When applicable, a security label overrides any specific security level and category assignments in the record. Assigning a security label is equivalent to explicitly assigning the level and categories of the label to the user. The specified security label must be defined as a record in class SECLABEL. When a USER record includes a security label, the user is granted access to a resource only if both of the following are true:

- The user security level specified in the security label is equal to or greater than the resource security level.
- All categories specified in the resource record are included in the security category list of the user security label.

Use the label[–] parameter with the chres, editres, and newres commands to modify this property.

SECLEVEL

The security level of the user or resource. The security level is a positive integer between 0 and 255. A value of 0 means no security level is assigned. If a resource has a security level assigned to it, the user is granted access to the resource only if the security level of the user is equal to or greater than the security level of the resource.

Use the level[–] parameter with the chres, editres, and newres commands to modify this property.

UACC

The default access for the resource, which indicates the access granted to accessors who are not defined to eTrust AC or who do not appear in the ACL of the resource. Refer to the ACL property of the resource for a list of valid values.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[–] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME — The date and time the record was created.

UPDATE_TIME — The date and time the record was last modified.

UPDATE_WHO — The administrator who performed the update.

CONTAINER Class

Each record in the CONTAINER class defines a group of objects from other resource classes, thus simplifying the job of defining access rules when a rule applies to several different classes of objects. Members of a CONTAINER class record can be objects from any of the following classes:

- ADMIN
- APPL
- AUTHHOST
- CALENDAR
- CONNECT
- CONTAINER
- DOMAIN (Windows only)
- FILE
- GAPPL
- GAUTHHOST
- GFILE
- GHOST
- GSUDO

- GTERMINAL
- HOLIDAY
- HOST
- MFTERMINAL
- PROCESS
- PROGRAM
- REGKEY (Windows only)
- SUDO
- SURROGATE
- TCP
- TERMINAL
- USER_DIR

Note: CONTAINER records can be nested in other CONTAINER records.

Before you specify an object as a member of a CONTAINER record, you must create a record for it in its appropriate class.

If an object in the container does not have an ACL in its appropriate class record, it inherits the ACL for the CONTAINER record of which it is a member.

The key of the CONTAINER class is the name of the CONTAINER record. The following list describes the properties that you can modify in a CONTAINER class record.

Modifiable Properties

ACL

The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the CONTAINER class are any valid access types for the contained objects. See listings under specific classes.

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

CALACL

The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Calendar reference—**A reference to a calendar in Unicenter TNG.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the CONTAINER class are any valid access types for the contained objects. See listings under specific classes.

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of CONTAINER records the container record belongs to.

To modify this property you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

MEMBERS

The list of objects from any class that are members of the group.

Use the mem+ or mem- parameter with the chres, editres, and newres commands to modify this property.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.
- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the CONTAINER class are any valid access types for the contained objects. See listings under specific classes.

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

PACL

The program access control list—an ACL that applies to accessors when the access request is made by a specific program or a program that matches a program-name pattern.

If you are using a pattern, then the resource that is protected by the PACL can be accessed using a program that matches the pattern. If a program matches several patterns, the longest pattern takes precedence.

Each element in the program access control list contains the following information:

– **Program reference**—A reference to a record in the PROGRAM class, either specifically or by name-pattern matching.

– **Accessor reference**—A reference to an accessor (a user or group).

– **Permitted access**—The access allowed to the accessor when using the specified program. Refer to the ACL property for a list of valid values.

Use the via(pgm) parameter with the authorize command to add programs, accessors, and their access types to, or authorize– or remove them from, the ACL property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.
- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[–] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

selang syntax

To add member(s) to a CONTAINER object:

```
{chres | editres |newres} CONTAINER (resourceName) mem+(memberName1, \
memberName2,....) of_class(memberClassName)
```

Note that you may add several members of the same class with a single command (separated by commas), but must use a separate command to add members of different classes because of the *of_class* descriptor.

To remove a member from a CONTAINER object:

```
{chres | editres} CONTAINER (resourceName) mem-(memberName1, \
 memberName2,....) of_class(memberClassName)
```

When using the authorize command:

```
{authorize | auth} CONTAINER resourceName \
[uid({userName | *})] \
[gid(groupName)] \
[access(authority)]
```

where *authority* is any access authority valid for any class in the container.

Examples

1. Create a container named *cont1* with members from the same class:

   ```
   newres CONTAINER cont1 mem+(polaris, betelgeuse, sirius) of_class(TERMINAL)
   ```

2. Add a member from a different class:

   ```
   chres CONTAINER cont1 mem+(D:\file.txt) of_class(FILE)
   ```

3. Remove members belonging to one class:

   ```
   chres CONTAINER cont1 mem-(polaris, sirius) of_class(TERMINAL)
   ```

DOMAIN Class

(Windows only class) Each record in the DOMAIN class defines a domain in the Windows network.

The key to the DOMAIN record is the domain name. The following list describes the properties that you can modify in a DOMAIN class record.

Modifiable Properties

ACL

The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference**—A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Permitted access**—The access authority the accessor has to the resource.

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

CALACL

The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—** A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Calendar reference—** A reference to a calendar in Unicenter TNG.
- **Permitted access**—The access authority the accessor has to the resource.

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

CATEGORY

One or more security categories assigned to a resource. You can specify any security category that is defined in the CATEGORY class. If a resource has one or more security categories assigned to it, a user is granted access to the resource only if the user security category list contains ***all*** the security categories assigned to the resource.

Use the category[–] parameter with the chres, editres, and newres commands to modify this property for resources.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of CONTAINER records the record belongs to.

To modify this property in a DOMAIN class record, you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.
- **Denied access**—The type of access to the resource that the accessor is specifically denied.

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

NOTIFY

The user notified when a resource generates an audit event. eTrust AC creates a special audit record that can be directed to the specified email address using selogrd**.**

Use the notify[–] parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

PACL

The program access control list—an ACL that applies to accessors when the access request is made by a specific program or a program that matches a program-name pattern.

If you are using a pattern, then the resource that is protected by the PACL can be accessed using a program that matches the pattern. If a program matches several patterns, the longest pattern takes precedence.

Each element in the program access control list contains the following information:

- **Program reference**—A reference to a record in the PROGRAM class, either specifically or by name-pattern matching.
- **Accessor reference**—A reference to an accessor (a user or group).
- **Permitted access**—The access allowed to the accessor when using the specified program. Refer to the ACL property for a list of valid values.

Use the via(pgm) parameter with the authorize command to add programs, accessors, and their access types to, or authorize– or remove them from, the ACL property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.
- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

SECLABEL

The security label of a resource. A security label associates a security level with security categories.

When applicable, a security label overrides any specific security level and category assignments in the record. Assigning a security label is equivalent to explicitly assigning the level and categories of the label to the user. The specified security label must be defined as a record in class SECLABEL. When a USER record includes a security label, the user is granted access to a resource only if both of the following are true:

- The user security level specified in the security label is equal to or greater than the resource security level.
- All categories specified in the resource record are included in the security category list of the user security label.

Use the label[–] parameter with the chres, editres, and newres commands to modify this property.

SECLEVEL

The security level of the user or resource. The security level is a positive integer between 0 and 255. A value of 0 means no security level is assigned. If a resource has a security level assigned to it, the user is granted access to the resource only if the security level of the user is equal to or greater than the security level of the resource.

Use the level[–] parameter with the chres, editres, and newres commands to modify this property.

UACC

The default access for the resource, which indicates the access granted to accessors who are not defined to eTrust AC or who do not appear in the ACL of the resource. Refer to the ACL property of the resource for a list of valid values.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[-] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

FILE Class

Each record in the FILE class defines the access allowed to a specific file or directory, or to files that match a *file name pattern*. A file need not have been created yet in order to have a rule defined for it.

Device files and symbolic links can be protected like any other file. However, by protecting a link you do not automatically protect the file that the link points to.

When you define a script as a file, allow both **read** and **execute** access to the file. When you define a binary, **execute** access is sufficient.

For users outside the special _restricted group, the _default record in the FILE class (or if no _default record exists, the record for FILE in the UACC class) *only protects files that are part of eTrust AC*–such as the seos.ini, seosd.trace, seos.audit, and seos.error files. These files are not explicitly defined to eTrust AC, but are automatically protected by eTrust AC.

The key of the FILE class record is the name of the file or directory protected by the record. The full path must be specified. The following list describes the properties that you can modify in a FILE class record.

Modifiable Properties

ACL

The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the FILE class are:
  - **all**—Allows accessors to perform all operations permissible for the class
  - **chdir**—Allows accessors to access the directory with the equivalent of read and execute permissions
  - **chown**—Allows accessors to change the owner of the file
  - **control**—Allows accessors all accesses except delete and rename
  - **create**—Allows accessors to create a file
  - **delete**—Allows accessors to delete a file
  - **execute**—Allows accessors to execute a program. To use this access type, the accessor must also have read access.
  - **none**—Does not allow the accessor to perform any operations
  - **read**—Allows accessors to use a file or directory without changing it
  - **rename**—Allows an accessor to rename a file
  - **sec**—Allows an accessor to change the ACL of a file
  - **update**—Allows an accessor the combination of read, write, and execute permissions
  - **utime**—Allows an accessor to change the modification time of a file
  - **write**—Allows an accessor to change the file or directory

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

CALACL

The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Calendar reference—**A reference to a calendar in Unicenter TNG.

- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the FILE class are:
  - **all**—Allows accessors to perform all operations permissible for the class
  - **chdir**—Allows accessors to access the directory with the equivalent of read and execute permissions
  - **chown**—Allows accessors to change the owner of the file
  - **control**—Allows accessors all accesses except delete and rename
  - **create**—Allows accessors to create a file
  - **delete**—Allows accessors to delete a file
  - **execute**—Allows accessors to execute a program. To use this access type, the accessor must also have read access.
  - **none**—Does not allow the accessor to perform any operations
  - **read**—Allows accessors to use a file or directory without changing it
  - **rename**—Allows an accessor to rename a file
  - **sec**—Allows an accessor to change the ACL of a file
  - **update**—Allows an accessor the combination of read, write, and execute permissions
  - **utime**—Allows an accessor to change the modification time of a file
  - **write**—Allows an accessor to change the file or directory

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

CATEGORY

One or more security categories assigned to a resource. You can specify any security category that is defined in the CATEGORY class. If a resource has one or more security categories assigned to it, a user is granted access to the resource only if the user security category list contains ***all*** the security categories assigned to the resource.

Use the category[–] parameter with the chres, editres, and newres commands to modify this property for resources.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of GFILE or CONTAINER records a resource record belongs to.

To modify this property in a FILE class record, you must change the MEMBERS property in the appropriate CONTAINER or GFILE record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.
- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the FILE class are:
  - **all**—Prevents accessors from performing any operations for the class
  - **chdir**—Prevents accessors from accessing the directory with the equivalent of read and execute permissions
  - **chown**—Allows accessors to change the owner of the file
  - **control**—Prevents accessors from all accesses except delete and rename
  - **create**—Prevents accessors from creating a file
  - **execute**—Prevents accessors from executing a program. To use this access type, the accessor must also have read access.
  - **none**—Allows accessors to perform any operations
  - **read**—Prevents accessors from viewing a file
  - **rename**—Prevents accessors from renaming a file
  - **sec**—Prevents accessors from changing the ACL of a file
  - **update**—Prevents accessors from updating files

- **utime**—Prevents accessors from changing the modification time of a file
- **write**—Prevents accessors from changing the file or directory

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

NOTIFY

The user notified when a resource generates an audit event. eTrust AC creates a special audit record that can be directed to the specified email address using selogrd**.**

Use the notify[–] parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

PACL

The program access control list—an ACL that applies to accessors when the access request is made by a specific program or a program that matches a program-name pattern.

If you are using a pattern, then the resource that is protected by the PACL can be accessed using a program that matches the pattern. If a program matches several patterns, the longest pattern takes precedence.

Each element in the program access control list contains the following information:

- **Program reference**—A reference to a record in the PROGRAM class, either specifically or by name-pattern matching.
- **Accessor reference**—A reference to an accessor (a user or group).
- **Permitted access**—The access allowed to the accessor when using the specified program. Refer to the ACL property for a list of valid values.

Use the via(pgm) parameter with the authorize command to add programs, accessors, and their access types to, or authorize– or remove them from, the ACL property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.
- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

SECLABEL

The security label of a resource. A security label associates a security level with security categories.

When applicable, a security label overrides any specific security level and category assignments in the record. Assigning a security label is equivalent to explicitly assigning the level and categories of the label to the user. The specified security label must be defined as a record in class SECLABEL. When a USER record includes a security label, the user is granted access to a resource only if both of the following are true:

- The user security level specified in the security label is equal to or greater than the resource security level.
- All categories specified in the resource record are included in the security category list of the user security label.

Use the label[–] parameter with the chres, editres, and newres commands to modify this property.

SECLEVEL

The security level of the user or resource. The security level is a positive integer between 0 and 255. A value of 0 means no security level is assigned. If a resource has a security level assigned to it, the user is granted access to the resource only if the security level of the user is equal to or greater than the security level of the resource.

Use the level[–] parameter with the chres, editres, and newres commands to modify this property.

UACC

The default access for the resource, which indicates the access granted to accessors who are not defined to eTrust AC or who do not appear in the ACL of the resource. Refer to the ACL property of the resource for a list of valid values.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[–] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME	The date and time the record was created.
UPDATE_TIME	The date and time the record was last modified.
UPDATE_WHO	The administrator who performed the update.

File Name Patterns

You can create a FILE record for an individual file or for all the files that match a specified file-name pattern, or **mask**. In the mask, you can use the wildcards "**?**" (meaning "any single character except the path separator character") and "*" (meaning "zero or more characters"). eTrust AC does *not* accept the following file name masks:

- /*
- /tmp/*
- /etc/*

eTrust AC enforces access rules for several specific files even if they have no FILE records:

- (UNIX only) All users always have at least read access to the /etc/group, and *eTrustACDir*/seos.ini files. To grant write access, you can create FILE records for those files.
- (UNIX only) By default, the *eTrustACDir*/etc/loginpgms.init, *eTrustACDir*/etc/nfsdevs.init, *eTrustACDir*/etc/privpgms.init, and *eTrustACDir*/etc/xdmpgms.init files receive protection from the _default record of the FILE class, but you can give them FILE records of their own to override their default protection.
- (UNIX only) The *eTrustACDir*/bin/* files, which include the eTrust AC binary executables, can be protected by FILE records. The FILE class's _default access rule applies to these files if specific FILE records do not protect them and if the protect_bin token (in the seos.ini file on UNIX) is set to yes . The default for the token is no, which means the files are protected only by specific FILE records that apply to them, if any.

Warning! *Do not assign a _default access of none for your FILE records while the protect_bin token is set to yes. Unless all* eTrustACDir*/bin files have FILE records, that combination of specifications can make eTrust AC unusable.*

- (Windows only) All users always have at least read access to the *system_directory*\system32\pwdchange.dll and *system_directory*\system32\susrauth.dll files.

Note: The audit log and its backup file, the error log and its backup file, the trace log, and the seos database, seos help file, and seos messages file can be read by users but can be written only by eTrust AC, and any FILE records for them are ignored.

GAPPL Class

Each record in the GAPPL class defines a group of applications used by eTrust Web Access Control or Single Sign-On. You must create an APPL class record for each application before adding it to a GAPPL record. You must then explicitly connect records of the APPL class to the GAPPL record in order to group them.

The key of the GAPPL class record is the name of the GAPPL record. The following list describes the properties that you can modify in a GAPPL class record.

Modifiable Properties

ACL

The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference**—A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Permitted access—**The access authority the accessor has to the resource. The valid access authorities for the GAPPL class are:
  - **execute**—Allows accessors to execute a program. To use this access type, the accessor must also have read access
  - **none**—Does not allow the accessor to perform any operations
  - **read—**Allows accessors to use a file or directory without changing it

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

AZNACL

The authorization ACL—an ACL that allows access to a resource based on the resource description. The description is sent to the authorization engine, not the object. The object is most likely not in the database.

CALACL

The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Calendar reference—**A reference to a calendar in Unicenter TNG.
- **Permitted access—**The access authority the accessor has to the resource. The valid access authorities for the GAPPL class are:
    - **execute**—Allows accessors to execute a program. To use this access type, the accessor must also have read access
    - **none**—Does not allow the accessor to perform any operations
    - **read—**Allows accessors to use a file or directory without changing it

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of CONTAINER records a resource record belongs to.

To modify this property in a GAPPL class record, you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

MEMBERS

The list of objects from the APPL class that are members of the group.

Use the mem+ or mem- parameter with the chres, editres, and newres commands to modify this property.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.
- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the GAPPL class are:
    - **execute**—Prevents accessors from executing a program. To use this access type, the accessor must also have read access
    - **none**—Allows accessors to perform any operations
    - **read**—Prevents accessors from viewing a file or directory

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.
- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

UPDATE_TIME The date and time the record was last modified.

UPDATE_WHO The administrator who performed the update.

GAUTHHOST Class

Each record in the GAUTHHOST class defines a group of authentication hosts used by eTrust Web Access Control or eTrust Single Sign-On. You must create an AUTHHOST class record for each application before adding it to a GAUTHHOST record. You must then explicitly connect records of the AUTHHOST class to the GAUTHHOST record in order to group them.

The key of the GAUTHHOST class record is the name of the GAUTHHOST record. The following list describes the properties that you can modify in a GAUTHHOST class record.

Modifiable Properties

ACL The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the GAUTHHOST class are:
  - **none**—Does not allow the accessor to perform any operations
  - **read—**Allows accessors to log in from the authenticated hosts

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

AZNACL The authorization ACL—an ACL that allows access to a resource based on the resource description. The description is sent to the authorization engine, not the object. The object is most likely not in the database.

CALACL The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Calendar reference—**A reference to a calendar in Unicenter TNG.

- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the GAUTHHOST class are:
  - **none**—Does not allow the accessor to perform any operations
  - **read—**Allows accessors to log in from the authenticated hosts

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of CONTAINER records a resource record belongs to.

To modify this property in a GAUTHHOST class record, you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

MEMBERS

The list of objects from the AUTHHOST class that are members of the group.

Use the mem+ or mem- parameter with the chres, editres, and newres commands to modify this property.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.
- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the GAUTHHOST class are:
  - **none**—Allows accessors to perform any operations
  - **read—**Prevents accessors from logging in from the authenticated hosts

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.
- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

GFILE Class

Each record in the GFILE class defines the access allowed to a group of specific files, specific directories, or files that match a name pattern. You must create a FILE class record for each application before adding it to a GFILE record. You must then explicitly connect records of the FILE class to the GFILE record in order to group them. A file need not have been created yet in order to have a FILE class record defined for it.

The key of the GFILE class record is the name of the GFILE record. The following list describes the properties that you can modify in a GFILE class record.

Modifiable Properties

ACL

The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference—** A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the GFILE class are:
  - **none**—Does not allow the accessor to perform any operations
  - **read**—Allows accessors to use any file or directory in the group without changing it
  - **write**—Allows an accessor to change any file or directory in the group

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

CALACL

The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—** A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Calendar reference—** A reference to a calendar in Unicenter TNG.

- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the GFILE class are:
  - **none**—Does not allow the accessor to perform any operations
  - **read**—Allows accessors to use any file or directory in the group without changing it
  - **write**—Allows an accessor to change any file or directory in the group

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of CONTAINER records a resource record belongs to.

To modify this property in a GFILE class record, you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

MEMBERS

The list of objects from the FILE class that are members of the group.

Use the mem+ or mem- parameter with the chres, editres, and newres commands to modify this property.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.
- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the GFILE class are:
  - **none**—Allows accessors to perform any operations
  - **read**—Prevents accessors from viewing a file or directory
  - **write**—Prevents accessors from changing any file or directory in the group

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

NOTIFY

The user notified when a resource generates an audit event. eTrust AC creates a special audit record that can be directed to the specified email address using selogrd**.**

Use the notify[–] parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

PACL

The program access control list—an ACL that applies to accessors when the access request is made by a specific program or a program that matches a program-name pattern.

If you are using a pattern, then the resource that is protected by the PACL can be accessed using a program that matches the pattern. If a program matches several patterns, the longest pattern takes precedence.

Each element in the program access control list contains the following information:

- **Program reference—**A reference to a record in the PROGRAM class, either specifically or by name-pattern matching.
- **Accessor reference—**A reference to an accessor (a user or group).
- **Permitted access—**The access allowed to the accessor when using the specified program. Refer to the ACL property for a list of valid values.

Use the via(pgm) parameter with the authorize command to add programs, accessors, and their access types to, or authorize– or remove them from, the ACL property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

all—All access requests are audited.

allow—All granted access requests are audited.

deny—Only denied access requests are audited; this is the default.

none—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[–] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

GHOST Class

Each record in the GHOST class defines a group of hosts. You must create a HOST class record for each host before adding it to a GHOST record. The services must be defined to the system using the /etc/services file (for UNIX), \system32\drivers\etc\services file (for Windows), or another service name resolution method. When authorizing services, you may identify the services by their port numbers in the TCP/IP protocol rather than by their names. When adding services, you may identify the services by their port numbers in the TCP/IP protocol rather than by their names. You must then explicitly connect records of the HOST class to the GHOST record in order to group them.

GHOST records define access rules that govern the access other stations (hosts) belonging to the group of hosts have to the local host when using Internet communication. For each client group (GHOST record), the INETACL property lists the service rules that govern the services the local host may provide to hosts belonging to the client group.

The key of the GHOST class record is the name of the GHOST record. The following list describes the properties that you can modify in a GHOST class record.

Modifiable Properties

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

ETHINFO

Ethernet information for a host (not available with this release).

GROUPS

The list of CONTAINER records a resource record belongs to.

To modify this property in a GHOST class record, you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

INETACL

The services the local host is allowed to provide to the group of client hosts and what their access types are. Each element in the access control list contains the following information:

- **Services reference**—A reference to a service (a port number or name). To specify all the services, enter an asterisk (*) as the services reference.

- **Permitted access**—The types of access the client hosts have to the service. The valid access types and the permissions they give are:
  - **read**—Allows the local host to provide the service to the host group.
  - **none**—Does not allow the local host to provide the service to the host group.

Use the access(*type-of-access*), service, and stationName parameters with the authorize[–] command to modify accessors and their access types in the INETACL property.

INSERVRANGE

Similar to the INETACL property. Instead of explicitly specifying the services the local host provides to the group of client hosts, this property specifies a range of services.

Use the service(*serviceRange*) parameter with the authorize[–] command to modify accessors and their access types in the INSERVRANGE property.

MEMBERS

The list of objects from the HOST class that are members of the group.

Use the mem+ or mem- parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.
- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[–] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME The date and time the record was created.

UPDATE_TIME The date and time the record was last modified.

UPDATE_WHO The administrator who performed the update.

GSUDO Class

Each record in the GSUDO class defines groups of actions that Task Delegation—the DO (sesudo)—allows a user to execute or prevents a user from executing. You must create a SUDO class record for each action before adding it to a GSUDO record.

Use GSUDO to define access rules for a group of SUDO resources rather than specifying the same access rule for each resource. You must explicitly connect records of the SUDO class to the GSUDO record in order to group them.

The key of the GSUDO class record is the name of the group. The following list describes the properties that you can modify in a GSUDO class record.

Modifiable Properties

ACL The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference**—A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the GSUDO class are:
  - **execute**—Allows accessors to execute a program.
  - **none**—Does not allow the accessor to perform any operations

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

CALACL The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.

- **Calendar reference—**A reference to a calendar in Unicenter TNG.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the GSUDO class are:
  - **execute**—Allows accessors to execute a program.
  - **none**—Does not allow the accessor to perform any operations

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of CONTAINER records a resource record belongs to.

To modify this property in a GSUDO class record, you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

MEMBERS

The list of objects from the SUDO class that are members of the group.

Use the mem+ or mem- parameter with the chres, editres, and newres commands to modify this property.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.

- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the GSUDO class are:
  - **execute**—Prevents accessors from executing a program.
  - **none**—Allows accessors to perform any operations

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.
- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[–] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

GTERMINAL Class

Each record in the GTERMINAL class defines a group of terminals. You must create a TERMINAL class record for each terminal before adding it to a GTERMINAL record. You must then explicitly connect records of the TERMINAL class to the GTERMINAL record in order to group them.

Terminal groups are useful when defining access rules. You can use a single command to specify an access rule for a group of terminals rather than having to specify the same access rule for each terminal. Similarly, you may apply a rule for a group of terminals by a single command to a group of users.

The key of the GTERMINAL class record is the name of the terminal group. The following list describes the properties that you can modify in a GTERMINAL class record.

Modifiable Properties

ACL

The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the GTERMINAL class are:
  - **none**—Does not allow the accessor to perform any operations
  - **read**—Allows accessors to log in from any terminal in the group.
  - **write**—Allows accessors to administer eTrust AC from any terminal in the group.

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

CALACL

The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Calendar reference—**A reference to a calendar in Unicenter TNG.

- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the GTERMINAL class are:
  - **none**—Does not allow the accessor to perform any operations
  - **read**—Allows accessors to log in from any terminal in the group.
  - **write**—Allows accessors to administer eTrust AC from any terminal in the group.

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of CONTAINER records a resource record belongs to.

To modify this property in a GTERMINAL class record, you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

MEMBERS

The list of objects from the TERMINAL class that are members of the group.

Use the mem+ or mem- parameter with the chres, editres, and newres commands to modify this property.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference**—A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.

- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the GTERMINAL class are:
  - **none**—Allows accessors to perform any operations
  - **read**—Prevents accessors logging in from any terminal in the group
  - **write**—Prevents accessors from administering eTrust AC from any terminal in the group.

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.
- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[-] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

HOLIDAY Class

Each record in the HOLIDAY class defines one or more periods when users need extra permission to log in.

Each user has the same access for all the time periods in a record. This means that if you include more than one holiday period in a holiday record, you cannot allow a user to log in during some of those periods and prevent that user from logging in during others. For example, if you want to allow a specific user to log in during New Year's Day but not during Christmas, then the two holidays must be defined in different records.

If you do not specify the year, the holiday is considered annual.

You can override HOLIDAY class restrictions for individual users by specifying the IGN_HOL attribute in the newusr, chusr, or editusr command.

The key of the HOLIDAY class record is the name of the HOLIDAY record. The following list describes the properties that you can modify in a HOLIDAY class record.

Modifiable Properties

ACL

The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference**—A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Permitted access—**The access authority the accessor has to the resource. The valid access authorities for the HOLIDAY class are:
  - **none**—Does not allow the accessor to perform any operations
  - **read**—Allows accessors to log in during the holiday specified in the record.

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

CALACL

The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.

- **Calendar reference—** A reference to a calendar in Unicenter TNG.
- **Permitted access—** The access authority the accessor has to the resource. The valid access authorities for the HOLIDAY class are:
  - **none**—Does not allow the accessor to perform any operations
  - **read**—Allows accessors to log in during the holiday specified in the record.

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

CATEGORY

One or more security categories assigned to a resource. You can specify any security category that is defined in the CATEGORY class. If a resource has one or more security categories assigned to it, a user is granted access to the resource only if the user security category list contains ***all*** the security categories assigned to the resource.

Use the category[–] parameter with the chres, editres, and newres commands to modify this property for resources.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of CONTAINER records a resource record belongs to.

To modify this property in a HOLIDAY class record, you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

HOL_DATE

Specifies the period during which users cannot log in.

The following rules apply to the HOL_DATE property:

- If you do not specify a year, it means the period or holiday is annual. You can specify the year with two digits or four digits, for example: 99 or 1999.
- If you do not specify a start time then the start of the day (midnight) is used; and if you do not specify an end time then the end of the day (midnight) is used.
- If you do not specify an interval of time, but only a date, then the holiday lasts for one whole day.

Use the dates parameter with the chres, editres, and newres commands to modify this property.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.
- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the HOLIDAY class are:
  - **none**—Allows accessors to perform any operations
  - **read**—Prevents accessors from logging in during the holidays specified in the record

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

NOTIFY

The user notified when a resource generates an audit event. eTrust AC creates a special audit record that can be directed to the specified email address using selogrd**.**

Use the notify[–] parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.

- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

SECLABEL

The security label of a resource. A security label associates a security level with security categories.

When applicable, a security label overrides any specific security level and category assignments in the record. Assigning a security label is equivalent to explicitly assigning the level and categories of the label to the user. The specified security label must be defined as a record in class SECLABEL. When a USER record includes a security label, the user is granted access to a resource only if both of the following are true:

- The user security level specified in the security label is equal to or greater than the resource security level.
- All categories specified in the resource record are included in the security category list of the user security label.

Use the label[–] parameter with the chres, editres, and newres commands to modify this property.

SECLEVEL

The security level of the user or resource. The security level is a positive integer between 0 and 255. A value of 0 means no security level is assigned. If a resource has a security level assigned to it, the user is granted access to the resource only if the security level of the user is equal to or greater than the security level of the resource.

Use the level[–] parameter with the chres, editres, and newres commands to modify this property.

UACC

The default access for the resource, which indicates the access granted to accessors who are not defined to eTrust AC or who do not appear in the ACL of the resource. Refer to the ACL property of the resource for a list of valid values.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[-] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME	The date and time the record was created.
UPDATE_TIME	The date and time the record was last modified.
UPDATE_WHO	The administrator who performed the update.

HOST Class

Each record in the HOST class defines access rules that govern the access that the other stations (hosts) have to the local host when they are using Internet communication. Records in the HOST class represent these clients of the local host. For each client (HOST record), the INETACL property lists the service rules that govern the services the local host may provide to the client.

The names you add to the HOST class must be defined to the system as hosts—that is, they must appear in the /etc/hosts file (for UNIX), \system32\drivers\etc\hosts file (for Windows), or be defined to the NIS or DNS system.

The services must be defined to the system using the /etc/services file (for UNIX), \system32\drivers\etc\services file (for Windows), or another service name resolution method. When authorizing services, you may identify the services by their port numbers in the TCP/IP protocol rather than by their names.

eTrust AC also supports dynamic port names assigned by the portmapper as specified by the /etc/rpc file (for UNIX) or \etc\rpc file (for Windows).

eTrust AC permits aliases for a host name, but records that represent aliases are never used for authorization checks. Calls to an alias are always directed to the real—canonical—name. You must know the true name of an IP address in order for eTrust AC to protect the connection to and from that machine.

The key of the HOST class record is the name of the host. The following list describes the properties that you can modify in a HOST class record.

Modifiable Properties

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

ETHINFO

Ethernet information for a host (not available with this release).

GROUPS

The list of GHOST or CONTAINER records a resource record belongs to.

To modify this property in a HOST class record, you must change the MEMBERS property in the appropriate CONTAINER or GHOST record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

INETACL

The services the local host is allowed to provide to the group of client hosts and what their access types are. Each element in the access control list contains the following information:

- **Services reference**—A reference to a service (a port number or name). To specify all the services, enter an asterisk (*) as the services reference.
- **Permitted access**—The types of access the client hosts have to the service. The valid access types and the permissions they give are:
  - **read**—Allows the local host to provide the service to the host group.
  - **none**—Does not allow the local host to provide the service to the host group.

Use the access(*type-of-access*), service, and stationName parameters with the authorize[–] command to modify accessors and their access types in the INETACL property.

INSERVRANGE

Similar to the INETACL property. Instead of explicitly specifying the services the local host provides to the group of client hosts, this property specifies a range of services.

Use the service(serviceRange) parameter with the authorize[–] command to modify accessors and their access types in the INSERVRANGE property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.
- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[–] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

HOSTNET Class

Each record in the HOSTNET class defines a group consisting of all hosts on a particular network. HOSTNET records define access rules that govern the access other stations (hosts) on the specific network have to the local host when using Internet communication. The name of each HOSTNET record consists of a set of **mask** and **match** values for the IP address. For each group of hosts (HOSTNET record), the INETACL property lists the service rules that govern the services the local host may provide to the hosts in the group.

The key of the HOSTNET class record is the name of the HOSTNET record. The following list describes the properties that you can modify in a HOSTNET class record.

Modifiable Properties

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of CONTAINER records a resource record belongs to.

To modify this property in a HOSTNET class record, you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

INETACL

The services the local host is allowed to provide to the group of client hosts and what their access types are. Each element in the access control list contains the following information:

- **Services reference**—A reference to a service (a port number or name). To specify all the services, enter an asterisk (*) as the services reference.
- **Permitted access**—The types of access the client hosts have to the service. The valid access types and the permissions they give are:
  - **read**—Allows the local host to provide the service to the host group.
  - **none**—Does not allow the local host to provide the service to the host group.

Use the access(*type-of-access*), service, and stationName parameters with the authorize[–] command to modify accessors and their access types in the INETACL property.

INSERVRANGE

Similar to the INETACL property. Instead of explicitly specifying the services the local host provides to the group of client hosts, this property specifies a range of services.

Use the service(serviceRange) parameter with the authorize[–] command to modify accessors and their access types in the INSERVRANGE property.

INMASKMATCH

The mask and match values that identify the network. The mask and match are applied to the IP address of the requesting host to determine whether it belongs to the network.

Use the mask and match parameters with the chres, editres, or newres command to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.
- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

WARNING — Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[–] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME — The date and time the record was created.

UPDATE_TIME — The date and time the record was last modified.

UPDATE_WHO — The administrator who performed the update.

HOSTNP Class

Each record in the HOSTNP class defines a group of hosts that have similar host names. HOSTNP records define access rules that govern the access other stations (hosts) that match name pattern in the record have to the local host when using Internet communication. For each mask (HOSTNP record), the INETACL property lists the service rules that govern the services the local host may provide to the group of hosts.

The key of the HOSTNP class record is the name pattern used to filter the host names of the hosts protected by this HOSTNP record. The following list describes the properties that you can modify in a HOSTNP class record.

Modifiable Properties

CALENDAR — Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

COMMENT — Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of CONTAINER records a resource record belongs to.

To modify this property in a HOSTNP class record, you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

INETACL

The services the local host is allowed to provide to the group of client hosts and what their access types are. Each element in the access control list contains the following information:

- **Services reference—**A reference to a service (a port number or name). To specify all the services, enter an asterisk (*) as the services reference.
- **Permitted access—**The types of access the client hosts have to the service. The valid access types and the permissions they give are:
  - **read**—Allows the local host to provide the service to the host group.
  - **none**—Does not allow the local host to provide the service to the host group.

Use the access(*type-of-access*), service, and stationName parameters with the authorize[–] command to modify accessors and their access types in the INETACL property.

INSERVRANGE

Similar to the INETACL property. Instead of explicitly specifying the services the local host provides to the group of client hosts, this property specifies a range of services.

Use the service(serviceRange) parameter with the authorize[–] command to modify accessors and their access types in the INSERVRANGE property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.
- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[–] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME The date and time the record was created.

UPDATE_TIME The date and time the record was last modified.

UPDATE_WHO The administrator who performed the update.

LOGINAPPL Class

(UNIX only class) Each record in the LOGINAPPL class defines a login application, identifies who can use the program to log in, and controls the way the login program is used.

The key of the LOGINAPPL class record is the name of the application, that is, a logical name that represents a login application. This logical name is associated, in the LOGINPATH property, with the full path name of the executable.

eTrust AC presets the property values for records in the LOGINAPPL class for standard login programs. ***You should list and verify the existing settings before making any changes***.

Note: The LOGINAPPL class in UNIX replaces the **loginpgms.init** file used in releases prior to eTrust AC 5.0.

Important! LOGINAPPL does not use the *_default entry.*

Modifiable Properties

ACL

The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the LOGINAPPL class are:
  - **execute**—Allows accessors to execute the login application
  - **none**—Does not allow the accessor to perform any operations

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

CALACL

The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Calendar reference—**A reference to a calendar in Unicenter TNG.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the LOGINAPPL class are:
  - **execute**—Allows accessors to execute the login application
  - **none**—Does not allow the accessor to perform any operations

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

LOGINFLAGS

Controls special features of the login application, including changes in device number and decrements to the grace logins number. Valid values are:

- **nograce**—Indicates that grace logins should not be decremented when users log in through this application
- **nograceroot**—Indicates that grace logins should not be decremented when root logs in through this application.

Use the loginflags parameter with the chres, editres, or newres command to modify this property.

LOGINMETHOD

Indicates whether the login application is a pseudo login program for the purposes of eTrust AC protection. Valid values are:

- **normal**—Indicates that this login application executes setuid and setgid calls itself. seosd checks the rules of the specified program.
- **pseudo**—Indicates that this login application calls another program to execute setuid and setgid calls. seosd checks the rules on the other program.

Warning! *We recommend that you not modify this preset property.*

Use the loginmethod parameter with the chres, editres, or newres command to modify this property.

LOGINPATH

The full path to the login application.

Use the loginpath parameter with the chres, editres, or newres command to modify this property.

LOGINSEQUENCE

The sequence of seteuid, setuid, setgid, and setgroups events that seosd processes to set the user from the daemon starting the login process (usually inetd under root) to the user who is actually logged on. (You may define up to eight system events.)

The login interception sequence always starts with setgid or setgroups events, which are called **triggers**. It ends with a setuid event that changes the user’s identity to the real user who logged in.

To successfully accomplish login, the program needs to perform all the specified processes in sequence starting with setgroups or setgid and ending with setuid or seteuid.

Setting the right LoginSequence for a program is a difficult task. Most login programs work well with the default SGRP,SUID setting; this setting means the program issues a setgroups system call and then a setuid command to change the user’s identity to the target user. However, if the SGRP, SUID setting does not work, you must use the following flags to specify the proper order:

– **SEID—**First seteuid event

– **SUID—**First setuid event

– **SGID—**First setgid event

– **SGRP—**First setgroup event

– **FEID—**Second seteuid event

– **FUID—**Second setuid event

– **FGID—**Second setgid event

– **FGRP—**Second setgroup event

– **N3EID—**Third seteuid event

– **N3UID—**Third setuid event

– **N3GID—**Third setgid event

– **N3GRP—**Third setgroup event

Note: If you do not know the sequence of system calls that the login program performs, you can view the trace and look for the setuid event that changed the user to the target uid, and then look at prior trace events starting with the first setgid or setgroups event.

For example, if you there is one setgroups event and then only the third setuid call sets the target user, you must set loginsequence to SGRP,SUID,FUID,N3UID:

```
SETGRPS : P=565302 to 0,2,3,7,8,10,11,250,220,221,230
SUID  > P=565302 U=0    (R=0    E=0    S=0   ) to (R=0  E=0    S=0   ) () BYPASS
SUID  > P=565302 U=0    (R=0    E=0    S=0   ) to (R=0  E=0    S=-1  ) () BYPASS
LOGIN  : P=565302 User=target Terminal=mercury
```

- The SETGRPS process indicates the trigger.
- The first SUID command should be discounted because you can see that the root simply changed back to root, not the trigger user. (This is the SUID in the sequence.)
- The second SUID command should be discounted as well because you can see that the root changed back to root, not the trigger user. (This is the FUID in the sequence.)
- The LOGIN event is the actual SETUID event causing the login. (Because it is the third event, it is the N3UID flag in the sequence.)

Use the loginsequence parameter with the chres, editres, or newres command to modify this property.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.
- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the LOGINAPPL class are:
  - **execute**—Prevents accessors from executing the login application
  - **none**—Allows accessors to perform any operations

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

NOTIFY

The user notified when a resource generates an audit event. eTrust AC creates a special audit record that can be directed to the specified email address using selogrd**.**

Use the notify[–] parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.
- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

UACC

The default access for the resource, which indicates the access granted to accessors who are not defined to eTrust AC or who do not appear in the ACL of the resource. Refer to the ACL property of the resource for a list of valid values.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[–] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME — The date and time the record was created.

UPDATE_TIME — The date and time the record was last modified.

UPDATE_WHO — The administrator who performed the update.

MFTERMINAL Class

Each record in the MFTERMINAL class defines a Mainframe computer that is used to administer eTrust AC. It has the same characteristics as the TERMINAL class, but is not intercepted by eTrust AC.

The key of the MFTERMINAL class is the name of the mainframe computer. The following list describes the properties that you can modify in an MFTERMINAL class record.

Modifiable Properties

ACL

The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the MFTERMINAL class are:
  - **none**—Does not allow the accessor to perform any operations
  - **read**—Allows accessors to log in from the Mainframe terminal
  - **write**—Allows accessors to administer eTrust AC from the Mainframe terminal

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

CALACL

The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Calendar reference—**A reference to a calendar in Unicenter TNG.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the MFTERMINAL class are:
  - **none**—Does not allow the accessor to perform any operations
  - **read**—Allows accessors to log in from the Mainframe terminal
  - **write**—Allows accessors to administer eTrust AC from the Mainframe terminal

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

CATEGORY

One or more security categories assigned to a resource. You can specify any security category that is defined in the CATEGORY class. If a resource has one or more security categories assigned to it, a user is granted access to the resource only if the user security category list contains ***all*** the security categories assigned to the resource.

Use the category[–] parameter with the chres, editres, and newres commands to modify this property for resources.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of CONTAINER records a resource record belongs to.

To modify this property in a MFTERMINAL class record, you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference**—A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.
- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the MFTERMINAL class are:
  - **none**—Allows accessors to perform any operations
  - **read**—Prevents accessors from logging in from the Mainframe terminal
  - **write**—Prevents accessors from administering eTrust AC from the Mainframe terminal

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

NOTIFY

The user notified when a resource generates an audit event. eTrust AC creates a special audit record that can be directed to the specified email address using selogrd**.**

Use the notify[–] parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

PACL

The program access control list—an ACL that applies to accessors when the access request is made by a specific program or a program that matches a program-name pattern.

If you are using a pattern, then the resource that is protected by the PACL can be accessed using a program that matches the pattern. If a program matches several patterns, the longest pattern takes precedence.

Each element in the program access control list contains the following information:

- **Program reference—**A reference to a record in the PROGRAM class, either specifically or by name-pattern matching.
- **Accessor reference—**A reference to an accessor (a user or group).
- **Permitted access—**The access allowed to the accessor when using the specified program. Refer to the ACL property for a list of valid values.

Use the via(pgm) parameter with the authorize command to add programs, accessors, and their access types to, or authorize– or remove them from, the ACL property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.
- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

SECLABEL

The security label of a resource. A security label associates a security level with security categories.

When applicable, a security label overrides any specific security level and category assignments in the record. Assigning a security label is equivalent to explicitly assigning the level and categories of the label to the user. The specified security label must be defined as a record in class SECLABEL. When a USER record includes a security label, the user is granted access to a resource only if both of the following are true:

- The user security level specified in the security label is equal to or greater than the resource security level.
- All categories specified in the resource record are included in the security category list of the user security label.

Use the label[–] parameter with the chres, editres, and newres commands to modify this property.

SECLEVEL

The security level of the user or resource. The security level is a positive integer between 0 and 255. A value of 0 means no security level is assigned. If a resource has a security level assigned to it, the user is granted access to the resource only if the security level of the user is equal to or greater than the security level of the resource.

Use the level[–] parameter with the chres, editres, and newres commands to modify this property.

UACC

The default access for the resource, which indicates the access granted to accessors who are not defined to eTrust AC or who do not appear in the ACL of the resource. Refer to the ACL property of the resource for a list of valid values.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[–] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

UPDATE_TIME The date and time the record was last modified.

UPDATE_WHO The administrator who performed the update.

PROCESS Class

Each record in the PROCESS class defines a program—an executable file—that runs in its own address space and that needs to be protected from being killed. Major utilities and database servers are good candidates for such protection since these processes are the main targets for denial-of-service attacks.

eTrust AC can protect against three terminate (kill) signals: the regular terminate signal (SIGTERM) and the two signals that an application cannot mask (SIGKILL and SIGSTOP):

Environment	Signal	Number
Windows	KILL	Win32 API
UNIX	Terminate Process	9
UNIX and Windows	STOP	Machine Dependent
UNIX and Windows	TERM	15

Other signals, such as SIGHUP or SIGUSR1, are passed to the process that they target and that process decides whether to ignore the terminate signal or whether to react to it in some way.

Windows Note: When defining a program in the PROCESS class, you must also define it in the FILE class. The order in which you create the records is not important.

The key of the PROCESS class record is the name of the program the record protects. Specify the full path. The following list describes the properties that you can modify in a PROCESS class record.

Modifiable Properties

ACL The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.

- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the PROCESS class are:
  - **none**—Does not allow the accessor to perform any operations
  - **read**—Allows accessors to kill the process

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

CALACL

The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Calendar reference—**A reference to a calendar in Unicenter TNG.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the PROCESS class are:
  - **none**—Does not allow the accessor to perform any operations
  - **read**—Allows accessors to kill the process

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

CATEGORY

One or more security categories assigned to a resource. You can specify any security category that is defined in the CATEGORY class. If a resource has one or more security categories assigned to it, a user is granted access to the resource only if the user security category list contains ***all*** the security categories assigned to the resource.

Use the category[–] parameter with the chres, editres, and newres commands to modify this property for resources.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of CONTAINER records a resource record belongs to.

To modify this property in a PROCESS class record, you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.
- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the PROCESS class are:
  - **none**—Allows accessors to perform any operations
  - **read**—Prevents accessors from killing the process

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

NOTIFY

The user notified when a resource generates an audit event. eTrust AC creates a special audit record that can be directed to the specified email address using selogrd**.**

Use the notify[–] parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

PACL

The program access control list—an ACL that applies to accessors when the access request is made by a specific program or a program that matches a program-name pattern.

If you are using a pattern, then the resource that is protected by the PACL can be accessed using a program that matches the pattern. If a program matches several patterns, the longest pattern takes precedence.

Each element in the program access control list contains the following information:

- **Program reference—**A reference to a record in the PROGRAM class, either specifically or by name-pattern matching.
- **Accessor reference—**A reference to an accessor (a user or group).
- **Permitted access—**The access allowed to the accessor when using the specified program. Refer to the ACL property for a list of valid values.

Use the via(pgm) parameter with the authorize command to add programs, accessors, and their access types to, or authorize– or remove them from, the ACL property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.
- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

SECLABEL

The security label of a resource. A security label associates a security level with security categories.

When applicable, a security label overrides any specific security level and category assignments in the record. Assigning a security label is equivalent to explicitly assigning the level and categories of the label to the user. The specified security label must be defined as a record in class SECLABEL. When a USER record includes a security label, the user is granted access to a resource only if both of the following are true:

- The user security level specified in the security label is equal to or greater than the resource security level.
- All categories specified in the resource record are included in the security category list of the user security label.

Use the label[–] parameter with the chres, editres, and newres commands to modify this property.

SECLEVEL

The security level of the user or resource. The security level is a positive integer between 0 and 255. A value of 0 means no security level is assigned. If a resource has a security level assigned to it, the user is granted access to the resource only if the security level of the user is equal to or greater than the security level of the resource.

Use the level[–] parameter with the chres, editres, and newres commands to modify this property.

UACC

The default access for the resource, which indicates the access granted to accessors who are not defined to eTrust AC or who do not appear in the ACL of the resource. Refer to the ACL property of the resource for a list of valid values.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[–] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

PROGRAM Class

Each record in the PROGRAM class defines a program that is considered part of the trusted computing base. Programs in this class are trusted not to have security breaches because they are monitored by the Watchdog to ensure they are not modified. If a trusted program is altered, eTrust AC automatically marks the program as untrusted, and the program is prevented from executing.

Each PROGRAM record contains several properties that define information about the trusted program file.

UNIX Notes:

- You can define any program as a trusted programs within eTrust AC. However, when you define a program access rule (a PACL) for a resource, eTrust AC automatically adds the specified program to the PROGRAM class if the program is not already defined in that class. Therefore, the PROGRAM class may also contain programs that are not marked as setuid or setgid.

Notes:

- You must also create a record for the trusted executable file in the FILE class in order to track the last accessor information (properties ACCSTIME and ACCSWHO). eTrust AC checks the FILE class first for authorization, and only then checks the PROGRAM class.
- A program cannot be used in a program access control list (PACL) unless it is defined in the PROGRAM class. (However, a program is automatically added to the PROGRAM class when it is added to a PACL.)
- Directories cannot be defined in the PROGRAM class.

The key of the PROGRAM class record is the file name of the program the record protects. You must specify the full path of the file as the object name. The following list describes the properties that you can modify in a PROGRAM class record.

Modifiable Properties

ACL

The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference**—A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the PROGRAM class are:
  - **execute**—Allows accessors to execute a program
  - **none**—Does not allow the accessor to perform any operations

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

BLOCKRUN

(UNIX only) Specifies whether to check if the program is trusted and blocks the execution of untrusted programs. The execution blocking is performed regardless whether the program is a setuid or a regular program.

Usage example:

```
newres program /usr/bin/login defaces(x) owner(nobody) blockrun.
```

Use the blockrun[–] parameter with the chres, editres, and newres commands to modify this property for resources.

CALACL

The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Calendar reference—**A reference to a calendar in Unicenter TNG.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the PROGRAM class are:
  - **execute**—Allows accessors to execute a program
  - **none**—Does not allow the accessor to perform any operations

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

CATEGORY

One or more security categories assigned to a resource. You can specify any security category that is defined in the CATEGORY class. If a resource has one or more security categories assigned to it, a user is granted access to the resource only if the user security category list contains ***all*** the security categories assigned to the resource.

Use the category[–] parameter with the chres, editres, and newres commands to modify this property for resources.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of CONTAINER records a resource record belongs to.

To modify this property in a PROGRAM class record, you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference—** A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.
- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the PROGRAM class are:
  - **execute**—Prevents accessors from executing a program
  - **none**—Allows accessors to perform any operations

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

NOTIFY

The user notified when a resource generates an audit event. eTrust AC creates a special audit record that can be directed to the specified email address using selogrd**.**

Use the notify[–] parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

PACL

The program access control list—an ACL that applies to accessors when the access request is made by a specific program or a program that matches a program-name pattern.

If you are using a pattern, then the resource that is protected by the PACL can be accessed using a program that matches the pattern. If a program matches several patterns, the longest pattern takes precedence.

Each element in the program access control list contains the following information:

– **Program reference—**A reference to a record in the PROGRAM class, either specifically or by name-pattern matching.

– **Accessor reference—**A reference to an accessor (a user or group).

– **Permitted access—**The access allowed to the accessor when using the specified program. Refer to the ACL property for a list of valid values.

Use the via(pgm) parameter with the authorize command to add programs, accessors, and their access types to, or authorize– or remove them from, the ACL property.

PGMINFO

Program information automatically generated by eTrust AC.

The Watchdog automatically verifies the information stored in this property. If it is changed, eTrust AC defines the program as untrusted.

You can select any of the following flags to **exclude** the associated information from this verification process:

– **crc**—The cyclic redundancy check

– **device**—The logical disk on which the file resides

– **group**—The UNIX group that owns the program file

– **inode**—The file system address of the program file

– **mode**—The UNIX security mode (permissions) for the program file

– **mtime**—The time the program file was last modified

– **owner**—The UNIX user who owns the program file

– **size**—The size of the program file

Use the flags, flags+, or flags– parameter with the chres, editres, or newres command to modify the flags in this property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

– **all**—All access requests are audited.

– **allow**—All granted access requests are audited.

– **deny**—Only denied access requests are audited; this is the default.

– **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

SECLABEL

The security label of a resource. A security label associates a security level with security categories.

When applicable, a security label overrides any specific security level and category assignments in the record. Assigning a security label is equivalent to explicitly assigning the level and categories of the label to the user. The specified security label must be defined as a record in class SECLABEL. When a USER record includes a security label, the user is granted access to a resource only if both of the following are true:

- The user security level specified in the security label is equal to or greater than the resource security level.
- All categories specified in the resource record are included in the security category list of the user security label.

Use the label[–] parameter with the chres, editres, and newres commands to modify this property.

SECLEVEL

The security level of the user or resource. The security level is a positive integer between 0 and 255. A value of 0 means no security level is assigned. If a resource has a security level assigned to it, the user is granted access to the resource only if the security level of the user is equal to or greater than the security level of the resource.

Use the level[–] parameter with the chres, editres, and newres commands to modify this property.

UACC

The default access for the resource, which indicates the access granted to accessors who are not defined to eTrust AC or who do not appear in the ACL of the resource. Refer to the ACL property of the resource for a list of valid values.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

UNTRUST

Indicates whether the program is trusted or not. If this property is set, no one can run the program. If this property is not set, the other properties listed in the database for the program are used to determine whether the user is authorized to run the program. If a trusted program is changed in any way, eTrust AC automatically sets the UNTRUST property.

Use the trust[–] parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[–] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

ACCSTIME

(UNIX only) The date and time the record was last accessed.

ACCSWHO

(UNIX only) The administrator who last accessed the record.

CREATE_TIME

The date and time the record was created.

MD5

The RSA–MD5 signature of the file.

SNEFRU

The SNEFRU file signature

UNTRUSTREASON

In UNIX dbdump only.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

PWPOLICY Class

Each record in the PWPOLICY class defines a password policy. These policies are sets of rules for both the validity of new passwords, and for the length of time the passwords are valid.

The key to the PWPOLICY class is the name of the password policy. The following list describes the properties that you can modify in a PWPOLICY class record.

Modifiable Properties

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of CONTAINER records a resource record belongs to.

To modify this property in a PWPOLICY class record, you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

PASSWDRULES

Specifies the password rules. This property contains a number of fields that determine how eTrust AC handles password protection. For a complete list of the rules, see the modifiable property PROFILE of the USER class.

Use the password parameter and the rules or rules- option with the setoptions command to modify this property.

Non-Modifiable Properties

APPLS

The list of eTrust Web Access Control applications that are linked to the password policy.

CREATE_TIME

The date and time the record was created.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

REGKEY Class

(Windows only class) Each record in the REGKEY class defines the tree structure of a key in the registry where Windows configuration information is saved.

By default eTrust AC protects the eTrust AC registry entries. The root of this registry is located at:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrustAccessControl
```

eTrust AC also protects the following link and its contents:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
```

The key to the REGKEY record is the full registry path to the key. The following list describes the properties that you can modify in a REGKEY class record.

Note: You can use a wildcard as part of a file name pattern. The wildcards are * (meaning “zero or more characters”) and ? (meaning “one character”).

Modifiable Properties

ACL

The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the REGKEY class are:
  - **all**—Allows accessors to perform all operations permissible for the class
  - **delete**—Allows accessors to delete a Windows registry key
  - **none**—Does not allow the accessor to perform any operations
  - **read**—Allows accessors to list the contents of the Windows registry key
  - **write**—Allows an accessor to change the Windows registry key

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

CALACL

The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Calendar reference—**A reference to a calendar in Unicenter TNG.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the REGKEY class are:
  - **all**—Allows accessors to perform all operations permissible for the class
  - **delete**—Allows accessors to delete a Windows registry key
  - **none**—Does not allow the accessor to perform any operations
  - **read**—Allows accessors to list the contents of the Windows registry key
  - **write**—Allows an accessor to change the Windows registry key

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of CONTAINER records a resource record belongs to.

To modify this property in a REGKEY class record, you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference**—A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.
- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the REGKEY class are:
    - **all**—Prevents accessors from performing any operations for the class
    - **delete**—Prevents accessors from deleting a Windows registry key
    - **none**—Allows accessors to perform any operations

- **read**—Prevents accessors from changing a Windows registry key
- **write**—Prevents accessors from changing a Windows registry key

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

NOTIFY

The user notified when a resource generates an audit event. eTrust AC creates a special audit record that can be directed to the specified email address using selogrd**.**

Use the notify[–] parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

PACL

The program access control list—an ACL that applies to accessors when the access request is made by a specific program or a program that matches a program-name pattern.

If you are using a pattern, then the resource that is protected by the PACL can be accessed using a program that matches the pattern. If a program matches several patterns, the longest pattern takes precedence.

Each element in the program access control list contains the following information:

- **Program reference—**A reference to a record in the PROGRAM class, either specifically or by name-pattern matching.
- **Accessor reference—**A reference to an accessor (a user or group).
- **Permitted access—**The access allowed to the accessor when using the specified program. Refer to the ACL property for a list of valid values.

Use the via(pgm) parameter with the authorize command to add programs, accessors, and their access types to, or authorize– or remove them from, the ACL property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.

- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

UACC

The default access for the resource, which indicates the access granted to accessors who are not defined to eTrust AC or who do not appear in the ACL of the resource. Refer to the ACL property of the resource for a list of valid values.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[-] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

RESOURCE_DESC Class

Each record in the RESOURCE_DESC class defines all of the names that new user-defined class objects are allowed to access in eTrust Web Access Control. You cannot create a new object in the RESOURCE_DESC class; you can only modify the existing ones.

The following list describes the properties that you can modify in a RESOURCE_DESC class record.

Modifiable Properties

CLASS_RIGHT** Of the 32 optional access rights; all are modifiable. The defaults for the first four rights are:

- CLASS_RIGHT1—read
- CLASS_RIGHT2—write
- CLASS_RIGHT3—execute
- CLASS_RIGHT4—rename

COMMENT Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

OWNER The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

RESPONSE_LIST The name of the object in the RESPONSE_TAB class that contains this object's name.

Non-Modifiable Properties

CREATE_TIME The date and time the record was created.

UPDATE_TIME The date and time the record was last modified.

UPDATE_WHO The administrator who performed the update.

RESPONSE_TAB Class

Each record in the RESPONSE_TAB class defines an eTrust Web Access Control response table to different authorization decisions.

A response is a personalized answer that is returned to application after an authorization request is granted or denied. It consists of KEY=VALUE pairs that are understood by the specific application. The response provides the ability to personalize the portal site according to the user's specific needs and authorization permissions.

The following list describes the properties that you can modify in a RESPONSE_TAB class record.

Modifiable Properties

CLASS_RIGHT** 32 optional response properties are lists of strings containing KEY=VALUE pairs (for example, button1=yes, picture2=no, and so on). There should be one property for each access value.

COMMENT Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

OF_RESOURCE The name of the object in the RESOURCE_DESC class that refers to the same user-defined class.

OWNER The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

Non-Modifiable Properties

CREATE_TIME The date and time the record was created.

UPDATE_TIME The date and time the record was last modified.

UPDATE_WHO The administrator who performed the update.

SECFILE Class

Each record in the SECFILE class defines a file to be monitored. SECFILE class records provide verification for important files in the system. However, they cannot appear in a conditional access control list.

Add sensitive system files that are not frequently modified to this class to verify that an unauthorized user has not altered them. The following are some examples of the type of files to include in class SECFILE:

For UNIX	For Windows
/.rhosts	\system32\etc\direvers\etc\hosts
/etc/services	\system32\etc\direvers\etc\services
/etc/protocols	\system32\etc\direvers\etc\protocols
/etc/hosts	
/etc/hosts.equiv	

The Watchdog scans these files and ensures the information known about these files is not modified.

Note: Directories cannot be defined in the SECFILE class.

The key of the SECFILE class record is the name of the file that the SECFILE record protects. Specify the full path. The following list describes the properties that you can modify in a SECFILE class record.

Modifiable Properties

AIXACL

AIX system ACLs.

AICEXTI

AIX system extended information.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of CONTAINER records a resource record belongs to.

To modify this property in a SECFILE class record, you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

HPUXACL

HP-UX system ACLs.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

PGMINFO

Program information automatically generated by eTrust AC.

The Watchdog automatically verifies the information stored in this property. If it is changed, eTrust AC defines the program as untrusted.

You can select any of the following flags to **exclude** the associated information from this verification process:

- **crc**—The cyclic redundancy check
- **device**—The logical disk on which the file resides
- **group**—The UNIX group that owns the program file
- **inode**—The file system address of the program file
- **mode**—The UNIX security mode (permissions) for the program file
- **mtime**—The time the program file was last modified
- **owner**—The UNIX user who owns the program file
- **size**—The size of the program file

Use the flags, flags+, or flags– parameter with the chres, editres, or newres command to modify the flags in this property.

UNTRUST

Indicates whether the program is trusted or not. eTrust AC automatically sets the UNTRUST property if a change to the file matches the flags you have set.

Use the trust[–] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

MD5

The RSA–MD5 signature of the file.

SNEFRU

The SNEFRU file signature.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

SECLABEL Class

Each record in the SECLABEL class associates a security level with security categories. A security label overrides the specific security level and security category assignments in the USER record if the SECLABEL class is active. Assigning a security label is equivalent to explicitly assigning the security level and security categories of the security label to the user.

When a USER record includes a security label, the user is granted access to a resource only if the following conditions are met:

- The user security level specified in the security label is equal to or greater than the resource security level.
- All categories specified in the resource record are included in the security category list of the user security label.

Windows Note: Each security label defined to eTrust AC must have a record in the SECLABEL class.

The key of the SECLABEL class record is the name of the security label. This name is used to identify the security label when assigning it to a user or resource. The following list describes the properties that you can modify in a SECLABEL class record.

Modifiable Properties

CATEGORY

One or more security categories assigned to a resource. You can specify any security category that is defined in the CATEGORY class. If a resource has one or more security categories assigned to it, a user is granted access to the resource only if the user security category list contains ***all*** the security categories assigned to the resource.

Use the category[–] parameter with the chres, editres, and newres commands to modify this property for resources.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

SECLEVEL

The security level of the user or resource. The security level is a positive integer between 0 and 255. A value of 0 means no security level is assigned. If a resource has a security level assigned to it, the user is granted access to the resource only if the security level of the user is equal to or greater than the security level of the resource.

Use the level[–] parameter with the chres, editres, and newres commands to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

SEOS Class

The SEOS class controls the behavior of the eTrust AC authorization system.

The class contains only one record, called SEOS, which specifies general security and authorization options. The following list describes the properties that you can modify in the SEOS class record.

Modifiable Properties

ACCPACL

Indicates the order in which the UACC (defaccess) and PACL lists are scanned during authorization.

When ACCPACL is active and explicit access is provided for a user through an ACL, then that accessor is the allowed access. If there is no explicit access through an ACL but explicit access is defined through a PACL, then the PACL access is the allowed access. If neither ACL nor PACL contains explicit access, defaccess is checked for access definitions.

If ACCPACL is not activated, the ACL is still checked first for explicit access. If the ACL contains no explicit access definitions for the resource being checked, defaccess definitions are checked next. If no explicit access is defined in defaccess, then the PACL access definitions are checked.

When eTrust AC is installed, the value of this property is set to yes.

Use the accpacl or accpacl- parameter with the setoptions command to modify this property.

ADMIN
Indicates whether the ADMIN class is active. Normally the ADMIN class is active and controls permission to perform security administration tasks. If the ADMIN class were inactive, all users could work as eTrust AC administrators.

APPL
Indicates whether the APPL class is active.

AUTHHOST
Indicates whether the AUTHHOST class is active.

CALENDAR
Indicates whether the CALENDAR class is active.

CATEGORY
Indicates whether the CATEGORY class is active.

CNG_ADMIN_PWD
Indicates whether a user with the PWMANAGER attribute can change an ADMIN user password using selang. The default is yes.

Use the class+ or class– parameter and the CNG_ADMIN_PWD option with the setoptions command to activate or inactivate this property.

CNG_OWN_PWD
Indicates whether users can change their own passwords using selang.

Use the class+ or class– parameter and the CNG_OWN_PWD option with the setoptions command to activate or inactivate this property.

COMMENT
Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

CONNECT
Indicates whether the CONNECT class is active. When the CONNECT class is active, records in the class protect the outgoing connections.

If the HOST class is active, the CONNECT class is not used as an active class, even when activated.

If the TCP class is active, the CONNECT class is not used as an active class.

DAYTIMERES
(UNIX only) Indicates whether eTrust AC checks the daytime restrictions on resources.

DOMAIN
(Windows only) Indicates whether the DOMAIN class is active.

FILE
Indicates whether the FILE class is active. When the FILE class is active, records in the class protect files and directories.

GRACCR
Indicates whether eTrust AC checks the accumulated group rights of users.

Use the class+ or class– parameter and the GRACCR option with the setoptions command to activate or inactivate this property.

HOLIDAY

Indicates whether the HOLIDAY class is active. When the HOLIDAY class is active, users need extra permission to log in during defined Holiday periods.

HOST

Indicates whether the HOST class is active. When the HOST class is active, eTrust AC protects incoming TCP/IP service requests from remote hosts.

If the HOST class is active, the TCP and CONNECT classes are not used as active classes, even when activated.

The default for the HOST class is active.

INACT

Indicates the number of inactive days after which user login is suspended. An inactive day is a day in which the user does not log in.

Use the inactive or inactive- parameter with the setoptions command to update this property.

LOGINAPPL

(UNIX only) Indicates whether the LOGINAPPL class is active.

MAXLOGINS

The maximum number of concurrent logins (terminal sessions) a user is allowed, after which the user is denied access. A zero value indicates no maximum and the user can log in to any number of terminal sessions concurrently. The value must be either zero or greater than 1 if the user wants to log in and run selang or otherwise administer the database, because eTrust AC considers each task (login, selang, GUI, and so forth) to be a terminal session.

A value for the MAXLOGINS property in a USER record overrides a value in a GROUP record. Both override the MAXLOGINS property in the SEOS class record. The value in the SEOS record is the default value used when there is no explicit value in the accessor record.

Use the maxlogins parameter with the chres, editres, and newres commands to modify this property for the SEOS class.

MFTERMINAL

Indicates whether the MFTERMINAL class is active.

PASSWDRULES

Indicates the password rules. This property contains a number of fields that determine how eTrust AC handles password protection. For a complete list of the rules, see the modifiable property PROFILE of the USER class.

Use the password parameter and the rules or rules- option with the setoptions command to modify this property.

PASSWORD

Indicates whether password checking is active.

Use the class+ or class– parameter and the PASSWORD option with the setoptions command to activate or inactivate this property.

PROCESS

Indicates whether the PROCESS class is active. When the PROCESS class is active, records in the class protect defined processes from kill attempts.

The file must also be defined in the FILE class.

PROGRAM

Indicates whether the PROGRAM class is active. When the PROGRAM class is active, records in the class protect defined programs that were marked as Trusted.

PWPOLICY

Indicates whether the PWPOLICY class is active.

REGKEY

(Windows only) Indicates whether the REGKEY class is active.

RESOURCE_DESC

Indicates whether the RESOURCE_DESC class is active.

RESPONSE_TAB

Indicates whether the RESPONSE_TAB class is active.

SECLABEL

Indicates whether the SECLABEL class is active.

SECLEVEL

Indicates whether the SECLEVEL class is active.

SUDO

Indicates whether the SUDO class, used by sesudo, is active.

SURROGATE

Indicates whether the SURROGATE class is active. When the SURROGATE class is active, eTrust AC protects surrogate requests.

TCP

Indicates whether the TCP class is active. When the TCP class is active, eTrust AC protects incoming and outgoing TCP services such as mail, ftp, and http.

If the HOST class is active, the TCP class is not used as an active class, even when activated.

If the TCP class is active, the CONNECT class is not used as an active class.

TERMINAL

Indicates whether the TERMINAL class is active. When the TERMINAL class is active, eTrust AC performs a terminal access check during sign-on and protects X-window sessions.

USER_ATTR

Indicates whether the USER_ATTR class is active.

USER_DIR

Indicates whether the USER_DIR class is active.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

ENDTIME The date and time the database files were last closed in an orderly manner.

STARTTIME The date and time the database files were last opened.

UPDATE_TIME The date and time the record was last modified.

UPDATE_WHO The administrator who performed the update.

selang syntax

To view the current status of SEOS class properties, enter the selang command:

```
setoptions list
```

To change the activation status of a class, enter the selang command:

```
setoptions class+(className)
```

or

```
setoptions class-(className)
```

The properties CNG_ADMIN_PWD, CNG_OWN_PWD, GRACCR and PASSWORD are treated as classes for the purpose of changing their activation status.

SPECIALPGM Class

The SPECIALPGM class gives specified programs special security privileges.

Each record in the SPECIALPGM class has one of two functions:

- Registering backup, DCM, PBF, PBN, STOP, and REGISTRY functions in Windows or registering xdm, backup, mail, DCM, PBF, and PBN programs in UNIX.
- Associating an application that needs special eTrust AC authorization protection with a logical user ID. This effectively allows setting access permissions according to *what* is being done rather than *who* is doing it.

Use the SPECIALPGMTYPE property to register system services, daemons, or other special programs.

Use the SEOSUID and NATIVEUID properties to assign a logical user to a program.

The key of the SPECIALPGM class record is a path to the special program or to a range, or pattern, of special programs. The following list describes the properties that you can modify in a SPECIALPGM class record.

Modifiable Properties

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

NATIVEUID

Indicates the user invoking the program or process. Use * to specify all eTrust AC users.

Use the nativeuid parameter with the chres, editres, or newres command to modify this property.

Note: For backward compatibility with older versions of eTrust AC, you can use the UNIXUID property instead of the NATIVUID property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

SEOSUID

Indicates the logical user authorized to run this special program. This logical user must be defined in the database with a USER record.

Use the seosuid parameter with the chres, editres, or newres command to modify this property.

SPECIALPGMTYPE

Determines the types of access checks that eTrust AC bypasses when granting access.

The types are **backup, dcm, pbf, pbn**, **stop**, **registry** or a combination of them for Windows and **backup**, **mail**, **xdm**, **dcm**, **pbf**, **pbn** or any combination of them for UNIX. You can also specify **surrogate** to bypass a database check for setuid and setgid programs.

Type	Description
backup	Bypasses READ, CHDIR, and UTIME access.
dcm	Bypasses all program checks for all events, except STOP events.
mail	(UNIX only.) Bypasses database checks for setuid and setgid events.
pbf	Bypasses database checks for file handling events.

Type	Description
pbn	Bypasses database checks for network- related events.
registry	(Windows only.) Bypasses database checks for programs that manipulate the Windows registry.
stop	(Windows only.) Bypasses database checks for the STOP feature.
surrogate	(UNIX only.) Bypasses database checks for setuid and setgid events.
xdm	(UNIX only.) Bypasses surrogate events.

Use the pgmtype parameter with the chres, editres, or newres command to modify this property.

For example, for UNIX you might issue the following command:

```
chres SPECIALPGM /bin/login pgmtype(surrogate)
```

For Windows, you might issue the following command if you want to provide full bypass for the program for all events:

```
newres SPECIALPGM ("c:\winnt\system32\wbem\winmgmt.exe") pgmtype(DCM,STOP)
```

Non-Modifiable Properties

CREATE_TIME The date and time the record was created.

UPDATE_TIME The date and time the record was last modified.

UPDATE_WHO The administrator who performed the update.

selang Example for UNIX

To protect a file that resides in /DATABASE/data/*, the database manager uses a file server daemon called firmdb_filemgr. This file server resides on /opt/dbfirm/bin/firmdb_filemgr. This daemon usually runs under root, making the data accessible to any root-shell hack.

In the following example, the logical user is defined as the only accessor of these files; access by others is restricted:

1. Define the “sensitive” files to eTrust AC using the command:

   ```
   newres file /DATABASE/data/* defaccess(NONE)owner(nobody)
   ```

2. Define the logical user to access the files:

   ```
   newusr firmDB_mgr
   ```

3. Allow only the logical user firmDB_mgr to access the files.

   ```
   Authorize file /DATABASE/data/* uid(firmDB_mgr) access(ALL).
   ```

4. Finally, make firmdb_filemgr run with logical user firmDB_mgr

   ```
   newres SPECIALPGM /opt/dbfirm/bin/firmdb_filemgr unixuid(root) \
   seosuid(firmDB_mgr).
   ```

Consequently, when the daemon accesses the files, eTrust AC recognizes the logical user as the accessor of the files, and not root. A hacker who attempts to access the files as root does not succeed.

selang Example for Windows

To protect files that reside in C:\DATABASE\data, the database manager uses a file server service called firmdb_filemgr.exe. This file server resides on C:\Program Files\dbfirm\bin\firmdb_filemgr.exe. This service usually runs under the system account, making the data accessible to any system hack.

In the following example, the logical user is defined as the only accessor of these files; access by others is restricted:

1. Define the "sensitive" files to eTrust AC using the following command:

   ```
   newres file C:\DATABASE\data\* defaccess(NONE)owner(nobody)
   ```

2. Define a logical user to access the files:

   ```
   newusr firmDB_mgr
   ```

3. Allow only the logical user firmDB_mgr to access the files:

   ```
   Authorize file C:\DATABASE\data\* uid(firmDB_mgr) access(ALL)
   ```

4. Finally, make firmdb_filemgr run with logical user firmDB_mgr:

   ```
   newres SPECIALPGM ("C:\Program Files\dbfirm\bin\firmdb_filemgr.exe") \
   nativeuid(system) seosuid(firmDB_mgr)
   ```

Consequently, when the service accesses the files, eTrust AC recognizes the logical user as the accessor of the files, and not the system account. A hacker who attempts to access the files in the system account does not succeed.

SUDO Class

Each record in the SUDO class identifies a command for which a user can borrow permissions from another user.

The key of the SUDO class record is the name of the SUDO record. This name is used instead of the command name when a user executes the commands in the SUDO record. The following list describes the properties that you can modify in a SUDO class record.

Note: The sesudo command cannot execute interactive processess when the SeOS Task Delegation service runs under a user account other than the SYSTEM account on a machine where Terminal Servicesare installed.

Modifiable Properties

ACL

The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the SUDO class are:
  - **execute**—Allows accessors to execute a program
  - **none**—Does not allow the accessor to perform any operations

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

CALACL

The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Calendar reference—**A reference to a calendar in Unicenter TNG.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the SUDO class are:
  - **execute**—Allows accessors to execute a program
  - **none**—Does not allow the accessor to perform any operations

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

CATEGORY

One or more security categories assigned to a resource. You can specify any security category that is defined in the CATEGORY class. If a resource has one or more security categories assigned to it, a user is granted access to the resource only if the user security category list contains ***all*** the security categories assigned to the resource.

Use the category[–] parameter with the chres, editres, and newres commands to modify this property for resources.

COMMENT

The command that sesudo executes. The alphanumeric string can contain up to 255 characters. This parameter was alternately know as DATA in earlier version of eTrust AC.

Note: This use of the COMMENT property is different than in other classes.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of CONTAINER records a resource record belongs to.

To modify this property in a SUDO class record, you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.
- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the SUDO class are:
  - **execute**—Prevents accessors from executing a program
  - **none**—Allows accessors to perform any operations

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

NOTIFY

The user notified when a resource generates an audit event. eTrust AC creates a special audit record that can be directed to the specified email address using selogrd**.**

Use the notify[–] parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

PACL

The program access control list—an ACL that applies to accessors when the access request is made by a specific program or a program that matches a program-name pattern.

If you are using a pattern, then the resource that is protected by the PACL can be accessed using a program that matches the pattern. If a program matches several patterns, the longest pattern takes precedence.

Each element in the program access control list contains the following information:

- **Program reference—**A reference to a record in the PROGRAM class, either specifically or by name-pattern matching.
- **Accessor reference—**A reference to an accessor (a user or group).
- **Permitted access—**The access allowed to the accessor when using the specified program. Refer to the ACL property for a list of valid values.

Use the via(pgm) parameter with the authorize command to add programs, accessors, and their access types to, or authorize– or remove them from, the ACL property.

PASSWORDREQ

(UNIX only) Indicates whether the sesudo command requests the target user password before executing.

Use the password parameter with the chres, editres, or newres command to modify this property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all—**All access requests are audited.
- **allow—**All granted access requests are audited.

- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

SECLABEL

The security label of a resource. A security label associates a security level with security categories.

When applicable, a security label overrides any specific security level and category assignments in the record. Assigning a security label is equivalent to explicitly assigning the level and categories of the label to the user. The specified security label must be defined as a record in class SECLABEL. When a USER record includes a security label, the user is granted access to a resource only if both of the following are true:

- The user security level specified in the security label is equal to or greater than the resource security level.
- All categories specified in the resource record are included in the security category list of the user security label.

Use the label[–] parameter with the chres, editres, and newres commands to modify this property.

SECLEVEL

The security level of the user or resource. The security level is a positive integer between 0 and 255. A value of 0 means no security level is assigned. If a resource has a security level assigned to it, the user is granted access to the resource only if the security level of the user is equal to or greater than the security level of the resource.

Use the level[–] parameter with the chres, editres, and newres commands to modify this property.

TARGUSR

(UNIX only) Indicates the target uid, which identifies the user whose permissions are to be borrowed for executing the command. The default is root.

Use the targuid parameter with the chres, editres, or newres command to modify this property.

UACC

The default access for the resource, which indicates the access granted to accessors who are not defined to eTrust AC or who do not appear in the ACL of the resource. Refer to the ACL property of the resource for a list of valid values.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[–] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

SURROGATE Class

(UNIX only class) Each record in the SURROGATE class defines restrictions that protect a user from other users when they make substitute user ID (su) requests eTrust AC treats the request as an abstract object that can be accessed only by authorized users.

A record in the SURROGATE class represents each user or group who has surrogate protection. Two special records—USER._default and GROUP._default—represent users and groups who do not have individual SURROGATE records. If there is no need to differentiate between the default for users and the default for groups, you may use the _default record for the SURROGATE class instead.

The key of the SURROGATE class record is the name of the SURROGATE record. The following list describes the properties that you can modify in a SURROGATE class record.

Modifiable Properties

ACL

The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.

- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the SURROGATE class are:
  - **none**—Does not allow the accessor to perform any operations
  - **read**—Allows an accessor to make su requests to the user.

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

CALACL

The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Calendar reference—**A reference to a calendar in Unicenter TNG.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the SURROGATE class are:
  - **none**—Does not allow the accessor to perform any operations
  - **read**—Allows an accessor to make su requests to the user.

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

CATEGORY

One or more security categories assigned to a resource. You can specify any security category that is defined in the CATEGORY class. If a resource has one or more security categories assigned to it, a user is granted access to the resource only if the user security category list contains ***all*** the security categories assigned to the resource.

Use the category[–] parameter with the chres, editres, and newres commands to modify this property for resources.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of CONTAINER records a resource record belongs to.

To modify this property in a SURROGATE class record, you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.
- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the SURROGATE class are:
  - **none**—Allows accessors to perform any operations
  - **read**—Prevents accessors from making su requests to the user

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

NOTIFY

The user notified when a resource generates an audit event. eTrust AC creates a special audit record that can be directed to the specified email address using selogrd**.**

Use the notify[–] parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

PACL

The program access control list—an ACL that applies to accessors when the access request is made by a specific program or a program that matches a program-name pattern.

If you are using a pattern, then the resource that is protected by the PACL can be accessed using a program that matches the pattern. If a program matches several patterns, the longest pattern takes precedence.

Each element in the program access control list contains the following information:

– **Program reference—**A reference to a record in the PROGRAM class, either specifically or by name-pattern matching.

– **Accessor reference—**A reference to an accessor (a user or group).

– **Permitted access—**The access allowed to the accessor when using the specified program. Refer to the ACL property for a list of valid values.

Use the via(pgm) parameter with the authorize command to add programs, accessors, and their access types to, or authorize– or remove them from, the ACL property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

– **all**—All access requests are audited.

– **allow**—All granted access requests are audited.

– **deny**—Only denied access requests are audited; this is the default.

– **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

SECLABEL

The security label of a resource. A security label associates a security level with security categories.

When applicable, a security label overrides any specific security level and category assignments in the record. Assigning a security label is equivalent to explicitly assigning the level and categories of the label to the user. The specified security label must be defined as a record in class SECLABEL. When a USER record includes a security label, the user is granted access to a resource only if both of the following are true:

- The user security level specified in the security label is equal to or greater than the resource security level.
- All categories specified in the resource record are included in the security category list of the user security label.

Use the label[–] parameter with the chres, editres, and newres commands to modify this property.

SECLEVEL

The security level of the user or resource. The security level is a positive integer between 0 and 255. A value of 0 means no security level is assigned. If a resource has a security level assigned to it, the user is granted access to the resource only if the security level of the user is equal to or greater than the security level of the resource.

Use the level[–] parameter with the chres, editres, and newres commands to modify this property.

UACC

The default access for the resource, which indicates the access granted to accessors who are not defined to eTrust AC or who do not appear in the ACL of the resource. Refer to the ACL property of the resource for a list of valid values.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[–] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

Restricting SURROGATE requests

To define a new SURROGATE record to eTrust AC using selang, enter:

```
newres SURROGATE USER. userName
```

Note: You must inform eTrust AC whether the object you are referring to in a surrogate record is a user or group, since eTrust AC allows you to give a user and a group the same name. This is done by preceding the object name with the word “USER” or GROUP” and a period, as shown in the example.

TCP Class

Each record in the TCP class defines a record for TCP/IP services such as mail, ftp, and http. When the TCP class is active and being used for authorization, hosts can obtain services from the local host only if the TCP resources explicitly or implicitly grant access. Likewise, users or groups can use these services to access remote hosts only if the TCP resources explicitly or implicitly grant access.

Note: When you use the TCP class to define a record, do not use the CONNECT class for the same record.

This class is helpful because you can set rules based on IP addresses, not just on host names. When a domain name changes, you can still protect the host set by the IP address.

The ACL for each record can specify access types not only for individual hosts that may request the service, but also for host groups (GHOST), networks (HOSTNET), and sets of hosts defined by a name pattern (HOSTNP).

In addition, the CACL for the record can specify the particular users and groups that can use the service to access specific hosts or groups of hosts (GHOST, HOSTNET, or HOSTNP resources).

If the HOST class or the CONNECT class is active (that is, are being used as a criterion for access), the TCP class cannot effectively be active.

The key of the TCP record is the name of the TCP/IP service. The TCP class controls outgoing services **and** incoming services.

This name identifies the service to eTrust AC. The following list describes the properties that you can modify in a TCP class record.

Modifiable Properties

ACL

The list of hosts (resources of type HOST, GHOST, HOSTNET and HOSTNP resources) for which the local host provides service and access types. Each element in the access control list contains the following information:

- **Host reference—**A reference to a record in the HOST, GHOST, HOSTNET, or HOSTNP class.
- **Permitted access**—The access authority the host reference has to the resource. The valid access authorities for the TCP class are:
  - **none—**Does not allow the host reference to perform any operations
  - **read**—Allows an host reference to obtain TCP service from the local host

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

CACL

The list of the users and groups granted access to the service and the host or hosts they can access. Each element in the conditional access control list contains the following information:

- **Accessor reference—**The name of the user or group.
- **Host reference—**A reference to record in the HOST, GHOST, HOSTNET, or HOSTNP class.
- **Permitted access—**The types of access the accessor has to the service. The valid access types and the permissions they give are:
- **write**—Allows the accessor to use this service to access the host or group of hosts.
- **none**—Does not allow the accessor to use this service to access the host or group of hosts.

Use the authorize or authorize– command to modify the this property.

CALACL

The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Calendar reference—**A reference to a calendar in Unicenter TNG.
- **Permitted access**—The access authority the host reference has to the resource. The valid access authorities for the TCP class are:
  - **none—**Does not allow the host reference to perform any operations
  - **read**—Allows an host reference to obtain TCP service from the local host

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of CONTAINER records a resource record belongs to.

To modify this property in a TCP class record, you must change the MEMBERS property in the appropriate CONTAINER record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.
- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the TCP class are:
  - **none**—Allows the host reference to perform any operations
  - **read**—Prevents a host reference from obtaining TCP service from the local host

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

NOTIFY

The user notified when a resource generates an audit event. eTrust AC creates a special audit record that can be directed to the specified email address using selogrd**.**

Use the notify[–] parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

PACL

The program access control list—an ACL that applies to accessors when the access request is made by a specific program or a program that matches a program-name pattern.

If you are using a pattern, then the resource that is protected by the PACL can be accessed using a program that matches the pattern. If a program matches several patterns, the longest pattern takes precedence.

Each element in the program access control list contains the following information:

– **Program reference—**A reference to a record in the PROGRAM class, either specifically or by name-pattern matching.

– **Accessor reference—**A reference to an accessor (a user or group).

– **Permitted access—**The access allowed to the accessor when using the specified program. Refer to the ACL property for a list of valid values.

Use the via(pgm) parameter with the authorize command to add programs, accessors, and their access types to, or authorize– or remove them from, the ACL property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

– **all**—All access requests are audited.

– **allow**—All granted access requests are audited.

– **deny**—Only denied access requests are audited; this is the default.

– **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

UACC

The default access for the resource, which indicates the access granted to accessors who are not defined to eTrust AC or who do not appear in the ACL of the resource. Refer to the ACL property of the resource for a list of valid values.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[-] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME The date and time the record was created.

UPDATE_TIME The date and time the record was last modified.

UPDATE_WHO The administrator who performed the update.

TERMINAL Class

Each record in the TERMINAL class defines a terminal of the local host, another host on the network, or an X terminal from which a login session can be made. Terminal permissions are checked during the user login procedure, so that users cannot succeed in logging in from terminals they have not been authorized to use.

The TERMINAL class also controls administrative access. ADMIN users can only administer eTrust AC from terminals for which they have appropriate access permissions.

When you define a new TERMINAL record, eTrust AC tries to convert the name you provide to a fully qualified name. If it succeeds it stores the fully qualified name in the database. If it fails, it stores the name you specified. When you issue subsequent commands referencing this record (chres, showres, rmres, authorize, and so on), you must use the name as it appears in the database.

The key of the TERMINAL record is the name of the terminal. This name identifies the terminal to eTrust AC. The following list describes the properties that you can modify in a TERMINAL class record.

Modifiable Properties

ACL The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.

- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the TERMINAL class are:
  - **none**—Does not allow the accessor to perform any operations
  - **read**—Allows accessors to log in from the terminal
  - **write**—Allows accessors to administer eTrust AC from the terminal

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

CALACL

The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Calendar reference—**A reference to a calendar in Unicenter TNG.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the TERMINAL class are:
  - **none**—Does not allow the accessor to perform any operations
  - **read**—Allows accessors to log in from the terminal
  - **write**—Allows accessors to administer eTrust AC from the terminal

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

CATEGORY

One or more security categories assigned to a resource. You can specify any security category that is defined in the CATEGORY class. If a resource has one or more security categories assigned to it, a user is granted access to the resource only if the user security category list contains ***all*** the security categories assigned to the resource.

Use the category[–] parameter with the chres, editres, and newres commands to modify this property for resources.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DAYTIME

The day and time restrictions that govern when a user can access the resource.

Use the restrictions(days and time) parameter with the chres, editres, and newres commands to modify this property.

GROUPS

The list of GTERMINAL or CONTAINER records a resource record belongs to.

To modify this property in a TERMINAL class record, you must change the MEMBERS property in the appropriate CONTAINER or GTERMINAL record.

Use the mem+ or mem- parameter with the chres, editres or newres command to modify this property.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.
- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the TERMINAL class are:
  - **none**—Allows accessors to perform any operations
  - **read**—Prevents accessors from logging in from the terminal
  - **write**—Prevents accessors from administering eTrust AC from the terminal

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

NOTIFY

The user notified when a resource generates an audit event. eTrust AC creates a special audit record that can be directed to the specified email address using selogrd**.**

Use the notify[–] parameter with the chres, editres, and newres commands to modify this property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

PACL

The program access control list—an ACL that applies to accessors when the access request is made by a specific program or a program that matches a program-name pattern.

If you are using a pattern, then the resource that is protected by the PACL can be accessed using a program that matches the pattern. If a program matches several patterns, the longest pattern takes precedence.

Each element in the program access control list contains the following information:

- **Program reference—**A reference to a record in the PROGRAM class, either specifically or by name-pattern matching.
- **Accessor reference—**A reference to an accessor (a user or group).
- **Permitted access—**The access allowed to the accessor when using the specified program. Refer to the ACL property for a list of valid values.

Use the via(pgm) parameter with the authorize command to add programs, accessors, and their access types to, or authorize– or remove them from, the ACL property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.
- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

SECLABEL

The security label of a resource. A security label associates a security level with security categories.

When applicable, a security label overrides any specific security level and category assignments in the record. Assigning a security label is equivalent to explicitly assigning the level and categories of the label to the user. The specified security label must be defined as a record in class SECLABEL.

When a USER record includes a security label, the user is granted access to a resource only if both of the following are true:

- The user security level specified in the security label is equal to or greater than the resource security level.
- All categories specified in the resource record are included in the security category list of the user security label.

Use the label[–] parameter with the chres, editres, and newres commands to modify this property.

SECLEVEL

The security level of the user or resource. The security level is a positive integer between 0 and 255. A value of 0 means no security level is assigned. If a resource has a security level assigned to it, the user is granted access to the resource only if the security level of the user is equal to or greater than the security level of the resource.

Use the level[–] parameter with the chres, editres, and newres commands to modify this property.

UACC

The default access for the resource, which indicates the access granted to accessors who are not defined to eTrust AC or who do not appear in the ACL of the resource. Refer to the ACL property of the resource for a list of valid values.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[–] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

UACC Class

Each record in the UACC class defines the default access allowed to a resource class. The UACC record also determines the access level allowed to a resource of that class that is not protected by eTrust AC.

UACC is applicable to most, but not all, classes. For the FILE class, UACC is applied in a nonstandard way (see the following table). The following table shows how each class uses the UACC class.

UACC Usage	Class
Standard	ADMIN, APPL, AUTHHOST, CALENDAR, CONNECT, CONTAINER, DOMAIN, GAPPL, GAUTHHOST, GHOST, GSUDO, GTERMINAL, HOLIDAY, HOST, HOSTNET, HOSTNP, MFTERMINAL, PROCESS, PROGRAM, REGKEY, SUDO, SURROGATE, TCP, TERMINAL, USER_DIR, User Defined Classes
Nonstandard	FILE, GFILE
None	AGENT, AGENT_TYPE, CATEGORY, GROUP, PWPOLICY, RESOURCE_DESC, RESPONSE_TAB, SECFILE, SECLABEL, SEOS, SPECIALPGM, USER, USER_ATTR

For users outside the special _restricted group, the record for FILE in the UACC class only protects files that are part of eTrust AC–such as the seos.ini, seosd.trace, seos.audit, and seos.error files. These files are not explicitly defined to eTrust AC, but are automatically protected by eTrust AC.

The key of the UACC class record is the name of the class whose UACC properties are being defined. The following list describes the properties that you can modify in a UACC class record.

Modifiable Properties

ACL

The list of accessors (users and groups) permitted to access the resource and their access types. Each element in the access control list contains the following information:

- **Accessor reference**—A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the UACC class are any valid access type for the class it is defining.

Use the access(*authority*) parameter with the authorize or authorize– command to modify the ACL property.

ALLOWACCS

A list of all allowed accesses for this class.

CALACL

The calendar access control list—The list of accessors (users and groups) permitted to access the resource according to the Unicenter TNG calendar status. Each element in the access control list contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the ACL, enter an asterisk (*) as the accessor reference.
- **Calendar reference—**A reference to a calendar in Unicenter TNG.
- **Permitted access**—The access authority the accessor has to the resource. The valid access authorities for the UACC class are any valid access type for the class it is defining.

Access is allowed only when the calendar is ON. Access is denied in all other cases.

Use the calendar parameter with the authorize command to permit user or group access to the resource according to the ACL access.

CALENDAR

Represents a Unicenter TNG calendar object for user, group, and resource restrictions in eTrust AC. eTrust AC retrieves Unicenter TNG active calendars at specified time intervals.

Use the calendar and calendar– parameters with the chusr, editusr, and newusr commands to modify this property.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

NACL

The list of accessors (users and groups) that are denied access to the resource the type of access denied. Each element in the NACL contains the following information:

- **Accessor reference—**A reference to an accessor (a user or group). To specify all the users defined to eTrust AC in the NACL, enter an asterisk (*) as the accessor reference.
- **Denied access**—The type of access to the resource that the accessor is specifically denied. The valid access authorities for the UACC class are any valid access type for the class it is defining.

Use the deniedaccess(*accesstype*) parameter with the authorize command or the deniedaccess- parameter with the authorize- command to modify the NACL property.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

– **all**—All access requests are audited.

– **allow**—All granted access requests are audited.

– **deny**—Only denied access requests are audited; this is the default.

– **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

UACC

The default access for the resource, which indicates the access granted to accessors who are not defined to eTrust AC or who do not appear in the ACL of the resource. Refer to the ACL property of the resource for a list of valid values.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

CREATE_TIME

The date and time the record was created.

UPDATE_TIME

The date and time the record was last modified.

UPDATE_WHO

The administrator who performed the update.

USER_ATTR Class

Each record in the USER_ATTR class defines the valid user attributes of an eTrust Web Access Control user directory.

The following list describes the properties that you can modify in a USER_ATTR class record.

Modifiable Properties

ATTR_PREDEFS

The list of allowed values for a specific attribute.

COMMENT

Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

DBFIELD

The name of the field in the userdir database. Since different databases can contain different attributes, the attribute fields should be synchronized.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.
- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

USERATTR_FLAGS

Contains information about the attribute. The flag can contain the following values:

- **aznchk—**Indicates whether to use this attribute for authorization.
- **predef** (predefined), **freetex** (free text), or **userdir** (user directory)—These three values specify the source of the user attributes.
- **user** or **group—**These values indicate whether the attribute (accessor) is a user or a group.

WARNING

Indicates whether warning mode is enabled. When warning mode is enabled, all access requests are granted. If an access request violates an access rule, a record is written to the audit log.

Note: In Warning Mode, eTrust AC does not create warning messages for resource groups.

Use the warning[–] parameter with the chres, editres, or newres command to modify this property.

Non-Modifiable Properties

ATTRNAME — The name of the attribute.

CREATE_TIME — The date and time the record was created.

FIELDID — The ID of the DB field

UPDATE_TIME — The date and time the record was last modified.

UPDATE_WHO — The administrator who performed the update.

USER_DIR_PROP — The name of the user's directory.

USER_DIR Class

Each record in the USER_DIR class defines an eTrust Web Access Control user directory.

The key of the USER_DIR record is the name of the directory. The following list describes the properties that you can modify in a USER_DIR class record.

Modifiable Properties

ADMIN_NAME — Login name of the administrator of the directory.

ADMIN_PWD — Password of the administrator of the directory. The password is stored in clear text format. It is not displayed in selang but can be obtained with seadmapi functions.

AZNACL — The authorization ACL—an ACL that allows access to a resource based on the resource description. The description is sent to the authorization engine, not the object. The object is most likely not in the database.

COMMENT — Additional information you want to include in the record. The alphanumeric string can contain up to 255 characters. eTrust AC does not use this information for authorization.

Use the comment[–] parameter with the chres, editres, and newres commands to modify this property.

CONTOBJ_CLS

The names of the classes the container object inherits from (needed for creation of new login info containers in LDAP.)

DIR_TYPE

The type of directory. Valid values are: ETRUST_AC, LDAP, ODBC, NT_Domain or none.

GRPOBJ_CLS

The names of the classes the group object inherits from (needed for creation of new groups in LDAP.)

LICONTOBJ_CLS

The names of the classes the login info container object inherits from (needed for creation of new login info containers in LDAP.)

LIOBJ_CLS

The names of the classes the login info object inherits from (needed for creation of new login information in LDAP.)

MAX_RET_ITEMS

The maximum number of items retrieved. The default depends on the directory type.

OWNER

The user or group that is the owner of the record.

Use the owner parameter with the chres, editres, and newres commands to modify this property.

PATH

The relative distinguishing name in the LDAP tree to begin all queries.

PORT_NUM

The port number on the host computer used to access the directory.

RAUDIT

The types of access events that eTrust AC records in the audit log. Valid values are:

- **all**—All access requests are audited.
- **allow**—All granted access requests are audited.
- **deny**—Only denied access requests are audited; this is the default.
- **none**—No access requests are audited.

Use the audit parameter with the chres, editres, or newres command to modify this property.

TIMEOUT_CON

The time (in seconds) the system waits to connect to the directory before issuing a Timeout error message.

UACC

The default access for the resource, which indicates the access granted to accessors who are not defined to eTrust AC or who do not appear in the ACL of the resource. Refer to the ACL property of the resource for a list of valid values.

Use the defaccess parameter with the chres, editres, or newres command to modify this property.

USERATTR_LIST The list of objects in the USER_ATTR class that was created with this USER_DIR object as the value for the USER_DIR parameter.

USERDIR_HOST The name of the host computer for the directory. This property must be defined in the class record.

USROBJ_CLS The names of the classes the user object inherits from (needed for creation of new users in LDAP.)

VERSION The version number of the directory.

Non-Modifiable Properties

CREATE_TIME The date and time the record was created.

UPDATE_TIME The date and time the record was last modified.

UPDATE_WHO The administrator who performed the update.

User Defined Classes

Each record in the User Defined class defines access to a custom-made class that meets your own needs. The only restriction on the name of user-defined classes is that the name cannot be all uppercase letters.

For example, a site may use a database to store and display proprietary data. Each database view—record—can be defined as a member of a user-defined class that indicates what type of authority is required to create each database view. Before users are permitted to create a database view, eTrust AC checks the authorization level of the user.

The key of a User Defined class record is the name of the record.

Unicenter TNG User-Defined Classes

eTrust AC lets you define Unicenter TNG asset classes as resources. You can create, delete, activate, and disable the Unicenter TNG user-defined classes.

You can find Unicenter TNG user-defined classes in the UACC class.

Modifiable Properties

Any property defined for a regular eTrust AC class can be used in User Defined classes.

Non-Modifiable Properties

CREATE_TIME	The date and time the record was created.
UPDATE_TIME	The date and time the record was last modified.
UPDATE_WHO	The administrator who performed the update.

Chapter

7

Managing Policy Model Databases Remotely

This chapter discusses the selang commands available in the pmd environment of the selang command shell. In the pmd environment, the selang commands are used to add, delete, modify, and list the subscribers of a PMDB (PMDB). You can also clear the error log and truncate the update file with these commands.

This chapter includes the following sections:

- An introduction to the pmd command shell environment
- A list of selang commands
- A detailed reference of all the selang commands that are supported in the pmd command shell environment

Managing the PMDB Remotely

Using selang, you can now remotely administer a PMDB by working in the pmd remote management command environment.

With remote PMDB management you can:

- Create and delete PMDBs
- Administer subscribers
- Truncate the update file
- Manage the error file of the PMDB

You can control a PMDB that resides on one machine by logging into it from any other machine. Using the host command, access the host where the PMDB resides. Use the pmd environment to type the desired commands.

Changing To and From the pmd Environment

When the selang command shell is set to the pmd environment, the selang commands operate on the PMDB of the selected host. The following instructions show you how to change to and from the pmd environment.

To enter the pmd Environment:

1. Invoke the selang command shell by typing the following command:

   ```
   selang
   ```

   The selang command shell is invoked in the eTrust environment. The following prompt appears:

   ```
   eTrustAC>
   ```

2. Check that you are updating the correct host. If you are not updating that host, change to the host by using the hosts command.
3. Change to the pmd environment by entering the following command:

   ```
   environment pmd
   ```

   The prompt changes to the following:

   ```
   eTrust(pmd)>
   ```

   The syntax of the selang commands that operate in this environment is discussed in the following pages.

To exit the pmd environment, enter the command:

```
environment eTrust
```

or

```
environment native
```

The prompt changes to eTrust or to eTrust (native) as appropriate.

Getting Help

You can get help on the pmd environment at any time that you are working in the selang command shell.

You must be in the pmd environment to get help on the selang pmd commands. From inside the pmd environment, use help.

For a specific command, type help *command name*. Then follow the instructions on the screen to get help on a particular selang pmd command.

Permissions

To work in the pmd remote management command environment a user must have the following:

- Permission to invoke selang on the accessor computer
- Permission to host from the accessor computer to the station where the pmd resides
- Administrator privileges for the PMDB

Example

To remotely manage terminal *Baker* from terminal *Skyblue*:

1. Invoke selang on *Skyblue.*
2. Host from *Skyblue* to *Baker.*
3. Type env pmd to switch to the pmd environment. The following prompt appears:

   ```
   eTrust(pmd)>
   ```

   You are now in the pmd environment

Commands

This section contains a complete list of selang commands for the pmd environment, arranged alphabetically.

Command	**Description**
createpmd	Creates a PMDB
deletepmd	Deletes a PMDB
findpmd	Gives the names of all PMDBs in the station
listpmd	Does one or more of the following: ■ lists subscribers and their status ■ describes the PMDB and its status ■ lists the commands in the update file and their offsets ■ lists the contents of the error log
pmd	Does one or more of the following: ■ removes the subscriber from the list of unavailable

Command	Description
	subscribers ▪ starts the PMDB daemon ▪ shuts down the PMDB daemon ▪ deletes entries from the update file ▪ deletes entries from the error log
subs	Does one or more of the following: ▪ adds a subscriber to the PMDB ▪ assigns a parent PMDB to the PMDB
subspmd	Assigns a parent PMDB to the local database
unsubs	Removes a subscriber from the PMDB

createpmd

Purpose

The createpmd defines a PMDB on a remote host. You can designate one or more users as administrator, auditor, and password managers for the PMDB. You can also define the PMDB's parent and subscriber PMDBs. The createpmd utility must be run locally, though it can also be run through a remote shell.

Syntax

```
createpmd pmdname [options]
```

Arguments

admins(*user1 [user2 ...]*)

Specifies the name of the PMDB administrators. You can specify more than one by separating them with spaces.

auditors(*user1 [user2 ...]*)

Specifies the user who can view the audit file of the PMDB. You can specify more than one by separating them with spaces.

pwmans(*user1 [user2 ...]*)

Specifies the PMDB password manager. You can specify more than one by separating them with spaces.

parentpmd(pmdname@*host)*
Specifies the name of the parent PMDB of the one you are creating.

desktop(*host1 [host2 ...])*
Specifies the host from which administrators can administer the PMDB. You can specify more than one by separating them with spaces. The default is the host of the new PMDB.

subscribers(*host1 | pmd1 [host2 | pmd2 ...])*
Specifies the host or PMDB to be a subscriber of the new PMDB. You can specify more than one by separating them with spaces.

pwdfile(*filename)* Specifies the PMDB password file.

grpfile(*filename)* Specifies the PMDB group file.

nis Performs an NIS setup on the new PMDB's host, and creates a filter file to filter out all UNIX updates.

deletepmd

Purpose

The deletepmd command removes the following items from the remote host:

- The PMDB's selang protection files:
  - pmd.ini
  - database files
  - socket file
- The contents of the PMDB directory
- The PMDB directory

Note: To prevent serious operational problems, avoid removing the PMDB by manually deleting its files. Always use either the deletepmd command for remote PMDBs, or the sepmdadm -c command for local PMDBs (for information on this command, see the *Utilities Guide*).

Syntax

```
deletepmd pmdname
```

findpmd

Purpose

The findpmd command gives you a list of all PMDBs in the machine, and indicates whether their daemons are loaded.

Syntax

```
findpmd
```

listpmd

Purpose

The listpmd command lists information about the PMDB and its subscribers, update file, and error log.

Syntax

```
listpmd pmdname \
        [all_errors][next]] \
        [cmd(offset)][next]] \
        [errors][next]] \
        [info][next]] \
        [subscriber(subName)][next]]
```

Arguments

cmd(*offset*)
Displays all commands in the update file and their offsets. The offset indicates the location of the update inside the file. If an offset is specified, the list starts from *offset*. If no offset is specified, the display begins from the beginning of the update file.

all_errors
Displays the PMDB error log. Displays all errors in the PMDB error log including connection failures.

errors
Displays the PMDB error log. Only non-connection failure errors are displayed.

info
Displays general information about the PMDB *pmdname*, including password file name, group file name, and whether the identified PMDB has a parent. This information is derived from the PMDB’s pmd.ini file.

next — Displays more of the list. This option is useful when the query list is larger than the set query size.

subscriber(*subName*) — Lists the subscribers of the PMDB and their status, including number of errors, availability, offset, and the next command to be propagated. The argument subname lets you select a subset of subscribers.

Notes

- The update file contains updates that must be, or have been, propagated by the PMDB. The offset indicates the location of the next update that must be sent to a subscriber. The update file's initial and latest offsets are displayed.
- The maximum query size limit is determined by the query_size token in the [lang] section of the seos.ini file. The query size limit default is set at 100. When the full listing cannot be displayed, the user sees the following message:

  ```
  Warning! Only 100(query size limit) items are displayed.
  ```

Examples

- If you want to display a list of subscribers, you can display a part of it that matches a pattern by using the following command:

  ```
  listpmd parentname subscriber(pmdpattern).
  ```

  One way to do this is to use a wildcard character (*), which matches any string including an empty string.
- If you run the following command and there are four subscribers named dawn, pmdb1, pmdb2, and pmdb3, only the three subscribers with names that begin with pmdb are displayed:

  ```
  listpmd parentname subscriber(pmdb*)
  ```
- If you run the following command all the subscribers are displayed.

  ```
  listpmd parentname subscriber(*)
  ```

pmd

Purpose

The pmd command clears the Policy Model error log, updates the subscriber list, releases subscribers, starts and stops the Policy Model service, truncates the update file, and reloads the initialization files.

Syntax

```
pmd pmdName  {                    \
     backup                       \
     operation                    \
    [{clrerr|clrerror}]           \
    [killog]                      \
    [release(subName)]            \
    [reloadini]                   \
    [startlog]                    \
    [start]                       \
    [stop]                        \
    [{trunc|truncate}(offset)] }
```

Arguments

backup

Moves the Policy Model to backup status.

clrerror | clrerr

Clears the PMDB error log

killlog

Disables the PMDB general log file.

Warning: Do not use the kill command to shut down the PMDB daemon.

operation

Moves the PMDB from backup to operational status.

release(*subName*)

Removes the subscriber specified by *subName* from the list of unavailable subscribers. This means that the subscriber can receive updates immediately. *subName* specifies the subscriber that is to become available for update.

Normally, if a subscriber is down and cannot receive updates from the PMDB, sepmdd tries to send updates to that subscriber only after a certain period. This interval is determined by the _retry_timeout_ token in the seos.ini file. The default value is 30 minutes. If the release option is used, however, sepmdd skips the waiting period and tries to send updates to the subscriber immediately.

reloadini

Rereads the Policy Model pmd.ini file and the seos.ini file, enabling values of certain tokens to change without having to reload the Policy Model service.

startlog

Enables the Policy Model general log file for writing.

start

Starts the PMDB daemon. Use this option to start the daemon when you do not have any other commands to execute.

stop

Shuts down the PMDB daemon.

Warning: Do not use the kill command to shut down the PMDB daemon.

truncate | trunc [*offset*]

Deletes entries from the update file. If you are using *offset* (manual cutting) only the updates up to the offset are cut; you can determine the offset by running listpmd *pmdname* subscriber(*). The full list of subscribers and their offsets appears.

Note: You must now use the true offset provided by **listpmd pmdname subscriber** to truncate the file, and not an offset derived by subtracting from the start offset.

You can prevent the need to run listpmd *pmdname* subscriber(*) by selecting auto.

If you are using auto, the utility calculates the offset of the first unpropagated entry and deletes all previous entries.

If a subscriber received fewer than all updates before the specified offset, an error message appears and the file is not truncated. If you want to truncate the file in any case, do the following:

- unsubscribe the subscriber that was not updated
- truncate the file
- re-subscribe the subscriber to the PMDB

If you truncate in this way, the subscriber fails to receive one or more updates from the PMDB. The subscriber's offset changes to the last offset of the updates file.

subs

Purpose

The subs command adds a subscriber to a parent PMDB or subscribes a database to a parent PMDB.

Syntax

```
subs pmdName   \
{parentpmd(pmdName2@host) | subs(subsName) | newsubs(subsName) }
```

Arguments

parentpmd(*pmdname2@host*)

Sets the parent_pmd token in the pmd.ini file of pmdname to *pmdName2@host*, making it the parent pmd of *pmdName*.

newsubs(*subsName*) Subscribes *subName* to policy model *pmdName*, and sends the new subscriber the contents of the whole PMDB, password, and group files.

subs(*subsName*) Assigns a subscriber to the PMDB.

When you subscribe a host to a PMDB:

- The host must be up
- eTrust AC must be running on that host
- The PMDB must be the parent PMDB of the subscribed host. This relationship is set by the token parent_pmd in the subscriber's seos.ini file, which must contain the name of the PMDB to which the host is being subscribed.

When you subscribe a PMDB to another PMDB:

- the token parent_pmd in the pmd.ini file of the subscribed PMDB must contain the name of the PMDB to which it is subscribing (its parent PMDB)
- eTrust AC must be running on the host in which the subscribed PMDB resides.

A PMDB should have only one parent. If you decide to establish a PMDB with more than one parent give the parent_pmd token the name of a file containing a list of the parent PMDBs.

However, establishing more than one parent is not recommended because you risk inundating your database with unreliable instructions from multiple sources.

subspmd

Purpose

The subspmd command changes the parent of the database in the host to which you are connected. The new parent PMDB is specified by *pmdName@host*.

Syntax

```
subspmd parentpmd (pmdname@host)
```

Arguments

parentpmd(*pmdname2@host*)

Sets the parent_pmd token in the pmd.ini file of pmdname to *pmdName2@host*, making it the parent pmd of *pmdName*.

unsubs

Purpose

The unsubs command removes the subscriber subName from the subscriber list of the PMDB specified by pmdName.

Syntax

```
unsubs pmdName subs(subsname)
```

Chapter

8

selang Commands in the UNIX Environment

This chapter discusses the commands available in the UNIX environment of the selang command shell. In the UNIX environment, use the selang commands to add, delete, modify, and list the users and groups in the local UNIX host and through the NIS system, if implemented. You can also modify and list the UNIX file permission and ownership settings.

Working in the UNIX Environment

This section explains how to work in the UNIX security environment of the selang command shell.

Changing to the UNIX Environment

When you set the selang command shell to the UNIX environment, the selang commands operate on the security files of the local UNIX host. This section shows you how to change to the UNIX environment.

To set the UNIX environment:

1. From directory *eTrustACDir*/bin, invoke the selang command shell by typing the following command:

   ```
   selang
   ```

   This invokes the selang command shell in the eTrust environment. The following prompt appears:

   ```
   eTrustAC>
   ```

2. Change to the UNIX environment by entering the following command:

   ```
   environment native
   ```

   The prompt changes to the following:

   ```
   eTrust(native)>
   ```

From this point on, all selang commands operate on the UNIX security files, instead of on the eTrust AC database. The following pages discuss the syntax of the selang commands.

To return to the eTrust environment, enter the following command:

```
environment eTrust
```

The prompt changes to the following:

eTrustAC>

Tip: To change environments, you can also type the prefix only of the environment you want to change to. For example, to change to the eTrust environment, you could also type one of the following:

```
env e
env et
```

Getting Help

You can get help on the UNIX environment at any time you are working in the selang command shell. You do not have to be in the UNIX environment to get help on the selang UNIX commands.

The command for getting help on the UNIX environment is:

```
help [unix]
```

Use the **help unix** command if you are inside the eTrust environment. From inside the UNIX environment, use only help.

Then follow the instructions on the screen to get help on a particular selang UNIX command.

Setting the System Defaults

This section shows you how to set up eTrust AC for management of the UNIX security system.

Defining the Default User File

The default file for updating UNIX users is /etc/passwd. You can change the default in the seos.ini file. Changing the seos.ini file is normally required on the NIS server machine only if you are working under NIS.

To instruct eTrust AC to use a different file when updating UNIX users, specify the file along with its full path specification in the YpServerPasswd token in the passwd section of the seos.ini file.

```
YpServerPasswd = passwdMapSourcePath
```

Defining a Shadow Password File

To change the location of the shadow password file, if used, set the YpServerSecure token in the [passwd] section of the seos.ini file. Specify the full path of the file.

```
YpServerSecure = shadowPasswdFilePath
```

Updating the passwd NIS Map

Specify the NIS directory and the make command by adding the following lines to the passwd section of the seos.ini file:

```
YpMakeDir = /var/yp
YpGrpCmd = make passwd group
```

Defining a Default File for Updating Groups

The default file used when updating UNIX groups is /etc/group. You can change the default in the seos.ini file. Changing the seos.ini file is normally required only if you are working under NIS.

To assign a different file for use when updating UNIX groups, specify the file along with its full path specification in the YpServerGroup token in the passwd section of the seos.ini file.

```
YpServerGroup = groupMapSourcePath
```

Automatic Backup of the UNIX User and Group Files

Before the first update of a UNIX user in a session and before the first update of a UNIX group in a session, eTrust AC creates a backup copy of the files /etc/passwd or /etc/group. The backup files are called /etc/passwd.SeOS.bak and /etc/group.SeOS.bak, respectively. If an error occurs when updating the UNIX system, the original information is recoverable. Backups are made only before the first change to the UNIX system in a selang command shell session.

Commands by Category

This section contains a complete list of selang commands for the UNIX environment, arranged by the following categories:

- Commands for managing users
- Commands for managing groups
- Commands for managing files
- Miscellaneous commands

Some commands appear in more than one category.

User Commands

Command	Description
Chusr	Changes the definition of an existing UNIX user.
Editusr	Adds a new user or changes the definition of an existing user.
Join	Joins users to a group.
join-	Disjoins users from a group.
Newusr	Adds a new user to UNIX.
Rmusr	Removes a user from UNIX.
Showusr	Lists the UNIX properties of a user.

Group Commands

Command	Description
Chgrp	Changes the definition of an existing UNIX group.
Editgrp	Changes the definition of an existing UNIX group.
Join	Joins users to a group.
join-	Disconnects users from a group.
Newgrp	Adds a new group to UNIX.
Rmgrp	Removes a group from UNIX.
Showgrp	Lists the UNIX properties of a group.

File Commands

Command	Description
Chfile	Changes the file attributes of a file in the UNIX file system.
Editfile	
Showfile	Lists the UNIX file attributes of a file.

Miscellaneous Commands

Command	Description
environment	Sets the security environment to eTrust or UNIX.
Help	Displays help text.
History	Displays a list of all commands entered so far in the current session.

Command Reference for UNIX

This section contains a complete reference to all the selang commands available in the UNIX environment, arranged alphabetically.

Organization

The first remarks in each entry explain what the command does, followed by these subsections:

- **Purpose**—Explains what the command does.
- **Syntax**—Describes the format of the command and any required or optional arguments. The syntax descriptions consist of the following elements:
  - Keywords (in normal text) and required punctuation. You must type keywords as shown. Note that some keywords have an abbreviated form that you can use instead of typing the keyword in full.
  - Variable parameters (in *italics*). You must replace each variable with a valid expression, as described in the description of the parameter.

  - Optional elements enclosed in square brackets ([]). For example, the command

    `password [userName]`

    indicates that the *userName* variable parameter is optional in the password command. Sometimes, optional clauses contain other optional clauses. Square brackets are used only for describing command syntax and are not to be typed. Do not confuse them with parentheses (), which are actually elements of selang commands.

  - Lists (usually enclosed in braces, with a pipe separating mutually exclusive item). *Do not* include the braces ({}) or the pipe (|) when you type one of the items. For example, the following parameter list means "*either* a user name *or* a group name":

    `{ username | groupname }`

  The list that follows the command syntax describes the parameters.

- **Notes**—Discusses techniques for using the command, and notes any special cases you should know about.
- **See Also**—Refers you to related commands and applicable sections of the eTrust AC documentation.
- **Examples**—Contains examples on using the command.

chfile / editfile

Purpose

The chfile and editfile commands change the settings of one or more UNIX files.

Syntax

```
{{chfile | cf} fileName \
 {editfile | ef} fileName} \
    [owner(userName)] \
    [group(groupName)] \
    [ mode( \
        [fowner(string)] \
        [fgroup(string)] \
        [fother(string)] \
    )]
```

Arguments

fileName

The name of the file whose settings are to be changed. Enter at least one UNIX file name. When changing more than one file, enclose the list of file names in parentheses and separate the file names with a space or a comma.

group(*groupName*)

Changes the group to which the file belongs. Specify a valid group name.

mode

Updates the access modes of the file.

fowner(*string*)

Specifies the access modes for the owner of the file. Use the letters r, w, and x in *string* to assign read, write, and execute permissions, respectively. Use the letter s to make a file setuid.

Specify a plus sign (+) at the beginning of *string* to add permissions to the existing permissions. Specify a minus sign (-) at the beginning of *string* to remove the permissions. If you do not specify a prefix, the previous permissions are reset to *string*.

fgroup(*string*)

Specifies the access modes for the file's group. Use the letters r, w, and x in *string* to assign read, write, and execute permissions, respectively. Use the letter s to make a file setgid.

Specify a plus sign (+) at the beginning of *string* to add permissions to the existing permissions. Specify a minus sign (-) at the beginning of *string* to remove the permissions. If you do not specify a prefix, the previous permissions are reset to *string*.

fother(*string*)

Specifies the access modes that apply to other accessors. Use the letters r, w, and x in *string* to assign read, write, and execute permissions, respectively. Specify a plus sign (+) at the beginning of *string* to add permissions to the existing permissions. Specify a minus sign (-) at the beginning of *string* to remove the permissions. If no prefix is specified, the previous permissions are reset to *string*.

owner(*userName*)

Changes the owner of the file. Specify the user name of a valid UNIX user.

See also

The showfile command in this chapter.

chgrp / editgrp / newgrp

Purpose

The chgrp command changes a group's attributes in the UNIX system. The editgrp command either adds a new group to UNIX like the newgrp command or changes the definition of an existing group like the chgrp command. The newgrp command adds new groups to the UNIX system.

New groups are added to and existing groups are updated in the file specified in the seos.ini file; by default, the groups are added to the /etc/group file. See Defining a Default File for Updating Groups in this chapter for more information.

Syntax

```
{chgrp | cg | editgrp | eg | newgrp | ng} (groupName) | (groupNames...)   \
    [groupid(integer)] \
    [userlist(userNames)]
```

Arguments

groupid(*integer*)
Sets the group ID of the group. Enter a positive integer representing the group's unique numeric ID. eTrust AC does not allow a group ID of zero.

groupName
The name of the group to be modified. Specify the name of an existing UNIX group. When altering more than one group, enclose the list of group names in parentheses and separate group names with a space or a comma.

userlist(*userNames*)
Specifies a new member list. Each user name must already be defined to UNIX. When more than one user is in the list, separate the user names with a space or comma. The user list specified here replaces any previous user list defined to the group.

See Also

- The rmgrp, showgrp, join, and join- commands in this chapter.
- Setting the System Defaults in this chapter.

chusr / editusr / newusr

Purpose

The chusr command modifies the definition of one or more users in the UNIX system. The editusr command can define a new user or change the properties of an existing user. The newusr command defines one or more new users to the UNIX system.

The users are added to or modified in the file specified in the seos.ini file, by default, the /etc/passwd file. See Defining the Default User File in this chapter for more information.

Syntax

```
{{chusr | cu} userName \
 {editusr | eu} userName \
 {newusr | nu} userName} \
    [enable] \
    [gecos(string)] \
    [homedir({path | nohomedir})] \
    [password(string)] \
    [pgroup(groupName)] \
    [shellprog(path)] \
    [userid(number)]
```

Arguments

enable
Enables the login of a user account that was disabled for any reason. This is a chusr and editusr parameter.

gecos(*string*)
Specifies a string containing general comments about the user, such as the user's full name. Enclose the string in single quotation marks.

homedir(*path*)
Specifies the full path of the user's home directory. eTrust AC attempts to create the directory. The UNIX file is updated, regardless of whether eTrust AC successfully creates the home directory.

No homedir
Skips creating a homedir for the user.

password(*string*)
Assigns a password to the user. Specify any character except a blank space. The password is valid for one login only. When the user next logs in to the system, a new password must be set.

pgroup(*groupName*)
Specifies the user's primary group name.

shellprog(*path*)
Specifies the full path of the initial program or shell that is executed after the user invokes the login command or the su command.

userid(*number*) Specifies the user’s unique numeric ID, used for unique discretionary access control. Enter a decimal number greater than 100; values less than 100 are not accepted.

userName The name of an existing UNIX user. When changing more than one user, enclose the list of user names in parentheses and separate the names with a space or a comma.

See Also

- The rmusr, showusr, join, and join- commands in this chapter.
- Setting the System Defaults in this chapter.

environment

Purpose

The environment command sets the security environment. eTrust AC supports the eTrust and UNIX security environments. When the selang command shell is invoked, the eTrust environment is selected by default.

Syntax

```
{environment | env} {etrust | pmd | seos | unix}
```

Arguments

eTrust

Specifies the eTrust security environment. The selang commands affect the local eTrust AC database. Some commands support simultaneous updates to the UNIX security settings. In the eTrust environment, the selang prompt is as follows:

```
eTrustAC>
```

pmd

Specifies the selang commands in the remote management environment. When the command shell is set to the pmd environment, the selang commands operate on the PMDB of the selected host. In the pmd environment, the selang prompt is as follows:

```
eTrustAC> (pmd)
```

unix

Specifies the UNIX security environment. The selang commands operate on the UNIX security system. In the UNIX environment, the selang prompt is as follows:

```
eTrust(native)>
```

find file

Purpose

The find file command lists all the files that match the mask, which is a string. The files are ordered chronologically in one column.

Syntax

```
find file /[directory][/mask]
```

Arguments

/directory/
List all the files in the directory *directory*.

/directory/mask
List all the files in the directory *directory* that match the *mask* variable. The *mask* may include wildcard characters.

Wildcard Matching

selang supports the following wildcard characters:

Character	Matches
* (asterisk)	Any sequence of zero or more characters.
? (question mark)	Any single character.

To make a single character a “do not care” character that will match any other single character, use a question mark (?), as in the following examples:

Specify this...	To do this...
mmc?	mmc3, mmcx, mmc5
mmc?.t	mmc1.t, mmc2.t
mmc04.?	mmc04.a, mmc04.1

To match any string of zero or more characters, use an asterisk (*), as in the following examples:

Specify this...	To do this...
i.c	main.c, list.c
st*.h	stdio.h, stdlib.h, string.h
*	All records of the specified class

join

Purpose

The join command adds users to a group. The specified users and group must already be defined to UNIX..

Authorization

To use the join command, at least one of the following must be true:

- You have the ADMIN attribute in your eTrust AC user record.
- The group record is within the scope of a group in which you have the GROUP-ADMIN attribute.
- You are the owner of the group record in the database.
- You have JOIN or MODIFY access authority in the access control list of the GROUP record in the ADMIN class.

Note: Both the MODIFY and JOIN properties are required if an ADMIN is to have the authority to modify eTrust AC GROUP records and UNIX groups

Syntax

```
{join | j} userName group(groupName)
```

Arguments

group(*groupName*)

Specifies the UNIX group to which the users are being added.

userName

The user name of the UNIX user who is being connected to the group specified by the group parameter. When specifying more than one user, enclose the user names in parentheses and separate the user names with a space or a comma.

See Also

The chgrp, rmgrp, showgrp, and join-commands in this chapter.

Example

The user Eli wants to join the user Bob to the group “staff.”

Known	**Command**	**Defaults**
Eli has the ADMIN attribute and the current environment is UNIX.	join Bob group(staff)	none

join-

Purpose

The join- command removes users from a group..

Authorization

To use the join- command, one of the following conditions must be true:

- You have the ADMIN attribute.
- The group record is within the scope of a group in which you have the GROUP-ADMIN attribute.
- You are the owner of the group record in the database.
- You have JOIN or MODIFY access authority in the access control list of the GROUP record in the ADMIN class.

If you only have ownership of the user's profile, you do not have sufficient authority to remove the user from a group. Both the MODIFY and JOIN properties are required if an ADMIN is to have the authority to modify eTrust AC records and UNIX groups

Syntax

```
{join- | j-} userName group(groupName)
```

Arguments

group(*groupName*)

Specifies the UNIX group from which to remove the user.

userName

The user name of the user you want to remove from the group. When removing more than one user from the group, enclose the list of user names in parentheses and separate the user names with a space or a comma.

See Also

The chgrp, newgrp, rmgrp, showgrp, and join commands in this chapter.

Example

The user Bill wants to remove the users sales25 and sales43 from the PAYROLL group.

Known	Command
The user Bill has the ADMIN attribute and the current environment is UNIX.	join- (sales25 sales43) group(PAYROLL)

rmgrp

Purpose

The rmgrp command deletes one or more groups from the UNIX system. The groups are removed from the file specified in the seos.ini file; by default, the groups are removed from the /etc/group file. See Defining a Default File for Updating Groups in this chapter for more information.

Syntax

```
{rmgrp | rg} groupName
```

Arguments

groupName The name of the group to be deleted. The group name must be an existing UNIX group name. Specify one or more group names. When removing more than one group, enclose the list of group names in parentheses and separate the group names with a space or a comma.

See Also

- The chgrp, newgrp, and showgrp commands in this chapter.
- Setting the System Defaults in this chapter.

rmusr

Purpose

The rmusr command removes one or more users from the UNIX system. The users are removed from the file specified in the seos.ini file. By default, the users are removed from the /etc/passwd file. See Defining the Default User File in this section for more information.

Syntax

```
{rmusr | ru} userName
```

Arguments

userName The user name of an existing UNIX user. When removing more than one user, enclose the list of user names in parentheses and separate the user names with a space or a comma.

See Also

- The chusr, newusr, and showusr commands in this chapter.
- Setting the System Defaults in this chapter.

ruler

Purpose

The ruler command determines which properties eTrust AC displays whenever the showusr, showgrp, showres, or showfile command is executed. By default, eTrust AC displays all the properties of a class except for electronic signatures. By using this command, you can choose to display only properties that interest you. All users can use this command.

The ruler command only applies to the hosts of the current session and displays the rulers of all the hosts of the current session. The properties of each host are displayed in a separate list. If you change hosts, the ruler command does not change the display of properties in the new hosts.

If you do not enter at least one property name when executing this command, eTrust AC displays the names of the properties that are in the current ruler.

Only the following users can issue this command:

- Users with the ADMIN, AUDITOR, or OPERATOR attribute.
- Users who have access read in class ADMIN for the class whose ruler they are trying to set. For example, if you have access read in class ADMIN for the record representing class TERMINAL, you can set the ruler for class TERMINAL.

Syntax

```
ruler className [props(all | propName)]
```

Arguments

className The name of the class whose display you want to change

props() Specifies the properties to be displayed:

- **all**—Specifies that all the properties of the class are to be displayed.
- ***propName***—Specifies the names of the one or more eTrust AC properties to be displayed. When specifying more than one property, enclose the property names in parentheses and separate the names with a space or a comma.

See Also

The showfile, showgrp, and showusr commands in this chapter.

Examples

- The user admin wants eTrust AC to display only two properties for each user: the owner and the user who is notified about changes.

Known	Command
The class USER is defined to eTrust AC.	ruler USER props(NOTIFY OWNER)

- The user admin wants to display the properties in the current ruler for class USER.

Known	Command
The class USER is defined to eTrust AC.	ruler USER

- The user admin wants eTrust AC to revert to the default ruler—to display all the properties in the class USER.

Known	Command
The class USER is defined to eTrust AC.	ruler USER props(all)

showfile

Purpose

The showfile command lists the UNIX details of one or more UNIX files.

Syntax

```
{showfile | sf} fileName [next] \
[{props|useprops|addprops} (propNames)]
```

Arguments

fileName

The name of the file whose details are to be listed. Enter one or more UNIX file names. When specifying more than one file, enclose the list of file names in parentheses and separate the individual names with a space or a comma.

next

Display parts of the requested data. This option is useful when the query data is larger than the set query size.

The maximum query size is determined by the query_size token in the lang section of the seos.ini file. The query size default is set at 100.

Set Properties

In addition to working in the ruler command, you can now set the properties to display directly in showfile, showres, showusr, and showgrp.

Parameter	Argument	Description
props	list of property names	Sets the properties (ruler) to be displayed. The ruler remains set for future queries.
useprops	list of property names	Sets the properties (ruler) to be displayed. The current ruler is ignored.

Parameter	Argument	Description
		The ruler is set for this query only.
addprops	list of property names	Sets the properties (ruler) to be displayed. The list of properties is added to the current ruler. The ruler is set for this query only, and reverts to the previously set ruler.

See Also

The chfile command in this chapter.

Example

You want to list the details of the UNIX file /tmp/foo.

Known	Command
You are not in the UNIX environment of the selang command shell.	environment(unix) showfile /tmp/foo

showgrp

Purpose

The showgrp command displays the details of one or more groups in the UNIX system. The properties are read from the file specified in the seos.ini file; by default, the properties are read from the /etc/group file. For more information, see Defining a Default File for Updating Groups in this chapter.

Syntax

```
{showgrp | sg} groupName [next]
```

Arguments

groupName

The name of the group whose details are to be displayed. The group name must be an existing UNIX group name. Specify one or more group names. When listing more than one group, enclose the list of group names in parentheses and separate the group names with a space or a comma.

next

Display parts of the requested data. This option is useful when the query data is larger than the set query size.

The maximum query size is determined by the query_size token in the lang section of the seos.ini file. The query size default is set at 100.

Set Properties

In addition to working in the ruler command, you can now set the properties to appear directly in showfile, showres, showusr, and showgrp.

Parameter	Argument	Description
props	list of property names	Sets the properties (ruler) to be displayed. The ruler remains set for future queries.
useprops	list of property names	Sets the properties (ruler) to be displayed. The current ruler is ignored. The ruler is set for this query only.
addprops	list of property names	Sets the properties (ruler) to be displayed. The list of properties is added to the current ruler. The ruler is set for this query only, and reverts to the previously set ruler.

See Also

- The newgrp, chgrp, and rmgrp commands in this chapter.
- Setting the System Defaults in this chapter.

Example

List details of the UNIX group “research”.

Known	Command
You are currently in the UNIX environment of the selang command shell.	showgrp security

showusr

Purpose

The showusr command displays the properties of one or more users defined in the UNIX system. The properties are read from the file specified in the seos.ini file; by default, the user information is read from the /etc/passwd file. For more information, see Defining the Default User File in this chapter.

Syntax

```
{showusr | su} userName [next]
```

Arguments

userName

The name of the user whose UNIX properties are to be displayed. Specify an existing UNIX user name. When listing the properties of more than one user, enclose the list of user names in parentheses and separate the names with a space or a comma.

next

Display parts of the requested data. This option is useful when the query data is larger than the set query size.

The maximum query size is determined by the query_size token in the lang section of the seos.ini file. The query size default is set at 100.

Set Properties

In addition to working in the ruler command, you can now set the properties to appear directly in showfile, showres, showusr, and showgrp.

Parameter	Argument	Description
props	list of property names	Sets the properties (ruler) to be displayed. The ruler remains set for future queries.
useprops	list of property names	Sets the properties (ruler) to be displayed. The current ruler is ignored. The ruler is set for this query only.
addprops	list of property names	Sets the properties (ruler) to be displayed. The list of properties is added to the current ruler. The ruler is set for this query only, and reverts to the previously set ruler.

See Also

- The newusr, chusr, and rmusr commands in this chapter.
- Setting the System Defaults in this chapter.

Example

List the details of the UNIX user "leslie."

Known	Command
You are currently in the UNIX environment; that is, you have the following prompt in the selang command shell: `eTrust(native)>`	showusr leslie

Common Procedures

This section shows you how to perform frequently used procedures in the UNIX environment of the selang command shell.

Switching to the UNIX Environment

When the selang command shell is invoked, the eTrust environment is active by default. In order to work in the UNIX environment, switch to the UNIX environment.

1. Invoke the selang command shell you want to use.
2. Enter the following command:

   ```
   environment(unix)
   ```

   The command prompt changes to the following:

   ```
   eTrust(native)>
   ```

Defining a New User to UNIX

This section shows you how to add a new user to UNIX. First, add the user tom using the eTrust AC default values. Then, we will add the user gil with some non-default properties.

Example: Using Default Settings

Enter the following command:

```
newusr tom
```

The user “tom” is defined to UNIX, with the following settings:

Property	Value
user name	tom
home directory	/home/tom
primary group	The group whose group ID is 1.
Shell program	/bin/sh
User ID	the number greater by 1 than the largest number previously used on the host

Example: Overriding Default Settings

Enter the following command:

```
newusr gil gecos(‘I defined this user yesterday’) \
 homedir(/usr/home/projectA/gil) pgroup(Sales) \
 shellprog(/bin/tcsh) userid(225)
```

The user “gil” is defined to UNIX, with the following settings:

Property	Value
user name	gil
home directory	/usr/home/projectA/gil
primary group	Sales
Shell program	/bin/tcsh
User ID	225

Changing the Definition of a UNIX User

This example shows you how to modify a UNIX user’s properties. We’ll change tom’s shell program to /bin/tsch:

```
chusr tom shellprog(/bin/tsch)
```

Removing a User from UNIX

This section shows you how to delete users. To delete the users tom and gil, enter the command:

```
rmusr (tom,gil)
```

Defining a New Group to UNIX

This section shows you how to define a new group to UNIX.

First, define the group Sales with default properties. Next, define the group ACCOUNTS to UNIX, and assign the users tom and gil as members of the new group.

Example: A New Group for UNIX, with Default Properties

Enter the following command:

```
newgrp Sales
```

The group Sales was defined with the following default properties:

Property	Value
Group ID	eTrust AC searches for the largest group ID currently defined to UNIX and increments the value by one.

Example: Adding a New Group for UNIX, with Member Users

1. Define the users tom and gil to UNIX by entering the following command:

   ```
   newusr (tom,gil)
   ```

2. Define the group ACCOUNTS to UNIX by entering the following command:

   ```
   newgrp ACCOUNTS userlist(tom,gil)
   ```

Assigning Users to an Existing UNIX Group

Once a group has been defined to UNIX, you can change the group's user list in two ways:

- By means of the chgrp command, in which case the complete user list must be typed in, since the new user list replaces the existing user list.
- If you use the join and join- commands, which is easier; you do not have to enter the entire user list.

The use of both methods is explained in this section.

Example: Adding/Removing a User with the chgrp Command

1. Define the user mary to UNIX, by entering the following command:

   ```
   newusr mary
   ```

2. Add the user mary to the user list of the ACCOUNTS group, by entering the following command:

   ```
   chgrp ACCOUNTS userlist(tom,gil,mary)
   ```

3. To view the group's properties, enter the following command:

   ```
   showgrp ACCOUNTS
   ```

   The properties of the group appear on the screen. Note the list of users.

Use the same method to remove member users from the group. Remember that the new user list always replaces the previous member list.

Example: Removing a User with the join- Command

1. Remove the user mary from the ACCOUNTS group by entering the following command:

   ```
   join- mary group(ACCOUNTS)
   ```

2. List the properties of the ACCOUNTS group by entering the following command:

   ```
   showgrp ACCOUNTS
   ```

3. Note that the user mary no longer appears in the user list.

Example: Adding Users with the join Command

1. List the properties of the Sales group by entering the following command:

   ```
   showgrp Sales
   ```

   The user list should be empty, since we created the group without specifying member users.

2. To add the users gil and mary to the Sales group, enter the following command:

   ```
   join (gil,mary) group(Sales)
   ```

3. List the properties of the Sales group by entering the following command:

   ```
   showgrp Sales
   ```

   The user list contains the users gil and mary.

Removing Groups from UNIX

This section shows you how to remove the groups you defined in the previous sections. In addition, delete the member users we created, so that your UNIX files are restored to their original states.

1. To remove the groups Sales and ACCOUNTS, enter the following command:

   ```
   rmgrp (Sales,ACCOUNTS)
   ```

2. Remove the users tom, gil, and mary from UNIX by entering the following command:

   ```
   rmusr (tom,gil,mary)
   ```

3. Remove the home directories of the users Tom, Gil, and Mary.

Your UNIX files are now as they were before you started these procedures.

Viewing the Properties of a File

This section shows you how to view the UNIX file attributes of a file. In this exercise, you create a file and then view its UNIX attributes.

1. Create the file /tmp/foo by entering the following command at the operating system prompt:

   ```
   touch /tmp/foo
   ```

2. Invoke the selang command shell. To invoke selang, enter the following command:

   ```
   selang
   ```

3. Change to the UNIX environment by entering the following command:

   ```
   environment native
   ```

4. Display the file's UNIX attributes by entering the following command:

   ```
   showfile /tmp/foo
   ```

Changing the UNIX File Attributes of a File

This section explains how to change a file's UNIX attributes from within the selang command shell.

In this exercise, you learn how to change the /tmp/foo file's attributes. You change the permissions to the file so that the owner of the file can read and write to the file, members of the owner's group can only read the file, and all other users can neither read nor write to the file.

1. To change the permissions, enter the following selang command:

   ```
   chfile /tmp/foo mode(fowner(rw) fgroup(r) fother(-rwx))
   ```

2. To display the changed attributes of the file, enter the following command:

   ```
   showfile /tmp/foo
   ```

Appendix

A Windows Values

This appendix describes the following:

- Windows attributes that can be assigned to a file
- Windows flags that can be assigned to a user's account
- Windows permissions that are relevant for the SHARE resource type
- Windows privileges that can be assigned to user and group accounts

Windows File Attributes

Attributes can be assigned to a file by using the chfile or editfile command. Attributes determine the character of the file. For more information on these commands, see chfile/editfile in the chapter "selang Commands in the Windows Environment" in this guide.

Note: Although the full name for these file attributes is FILE_ATTRIBUTE_name, eTrust AC only requires you to enter the *name* portion (for example, ARCHIVE or COMPRESSED).

The following table lists and describes the file attributes that you cant modify in Windows.

Value	Description
FILE_ATTRIBUTE_ARCHIVE	An archival file; a file marked for backup or removal.
FILE_ATTRIBUTE_HIDDEN	A hidden file. Hidden files are not normally included in an ordinary directory listing.
FILE_ATTRIBUTE_NORMAL	A file with no other attributes. This value is only valid when used alone.
FILE_ATTRIBUTE_READONLY	A read-only file. Applications can read the file, but cannot write in it or delete it.

Value	Description
FILE_ATTRIBUTE_SYSTEM	An operating system file or a file used exclusively by the operating system.
FILE_ATTRIBUTE_TEMPORARY	A file being used for temporary storage.

The following table lists and describes the file attributes that you cannot modify in Windows.

Value	Description
FILE_ATTRIBUTE_COMPRESSED	A compressed file or directory. For files, this means all the data in the file is compressed; for directories, this means that all newly created files and subdirectories are compressed by default.
FILE_ATTRIBUTE_DIRECTORY	A directory.

Windows Account Flags

Flags can be assigned to a user's account to specify particular attributes of that account by using the chusr, editusr, and newusr commands. You can apply more than one flag to each account. For more information on these commands, see chusr/editusr/newusr in the chapter "selang Commands in the Windows Environment" in this guide.

Note: eTrust AC does not require you to enter the complete name of the flag. You can use the shortcuts provided in the table.

Following are the account flags available in Windows.

Shortcut	Flag	Description
blank	UF_PASSWRD_NOTREQD	Indicates that no password is required for the user's account.
cant_change	UF_PASSWORD_CANT_CHANGE	Indicates that the user cannot change the password for the account.
disable	UF_ACCOUNTDISABLE	Indicates the user's account is disabled.
dont_expire	UF_DONT_EXPIRE_PASSWORD	Indicates that the password for this account never expires.

Shortcut	Flag	Description
homedir	UF_HOMEDIR_REQUIRED	Indicates the home directory is required. This value is ignored in Windows.
interdomain	UF_INTERDOMAIN_TRUST_ACCOUNT	Indicates a permit to trust account.
lockout	UF_LOCKOUT	Indicates that the user's account is currently locked out; to unlock a locked account, remove this flag
normal	UF_NORMAL_ACCOUNT	Indicates a default account type that represents a normal user.
notreq	UF_PASSWRD_NOTREQD	Indicates that no password is required for the user's account.
protect	UF_PASSWORD_CANT_CHANGE	Indicates that the user cannot change the password for the account.
script	UF_SCRIPT	Indicates that the login script, which executes disk mapping, is activated when the user starts an application. This flag must be set for LAN Manager 2.0 or Windows.
server	UF_SERVER_TRUST_ACCOUNT	Indicates an account for a Windows NT Backup Domain Controller in this domain.
temp	UF_TEMP_DUPLICATE_ACCOUNT	Indicates a user with an account in another domain; provides access to the domain for this account, but not a trust account.
trust	UF_INTERDOMAIN_TRUST_ACCOUNT	Indicates a permit to trust account.
workstation	UF_WORKSTATION_TRUST_ACCOUNT	Indicates an account for a workstation or server that is a member of this domain.

Windows Permissions

In the SHARE resource type, you can give access permissions to accessors. For more information on the SHARE resource type, see the chapter “Windows Environment Classes and Properties.”

Following are the access permissions available in Windows.

Value	Description
ACCESS_ALL	Permission to read, write, create, execute, and delete resources and to modify their attributes and permissions.
ACCESS_ATTRIB	Permission to modify the resource’s attributes.
ACCESS_CREATE	Permission to create a resource, including writing data to it as it’s being created.
ACCESS_DELETE	Permission to delete the resource.
ACCESS_EXEC	Permission to execute the resource.
ACCESS_NONE	No access.
ACCESS_PERM	Permission to modify the permissions assigned to a user or an application for a resource.
ACCESS_READ	Permission to read data from a resource and, by default, to execute in the resource.
ACCESS_WRITE	Permission to write data to the resource.

Windows Privileges

Windows privileges can be assigned to individual user accounts and groups. Administrators can assign privileges to a user with the chusr or editusr command, or to a group with the chgrp or editgrp command. Users who are added to a group automatically gain all the privileges assigned to the group. For more information on these commands, see the chapter ”selang Commands in the Windows Environment” in this guide.

You can use the name of the privilege, or user right, exactly as it appears in the list, or you can add Se to the beginning and Privilege to the end of the name (except for BatchLogon, InteractiveLogon, NetworkLogon, and ServiceLogon, to which you add Right instead of Privilege).

Following are the privileges available in Windows.

Privilege	Default Assignment	Description
AssignPrimaryToken	None	Allows a user to modify the security access token of a process.
Audit	None	Generates security audits.
Backup	Administrators Backup Operators	Allows a user to back up files and directories. This privilege replaces all file and directory permissions.
BatchLogon	None	Allows a user to log in as a batch job.
ChangeNotify	Everyone	Usually, rights to files and subdirectories flow downward; that is, users who do not have rights to a specific directory do not also have rights to access the subdirectories below that directory. This privilege allows a user to access subdirectories, even if that user has no rights to the parent directories.
CreatePagefile	None	Allows a user to create a page file. Security is determined by a user's access to the key: \CurrentControlSet\Control\ SessionManagement
CreatePermanent	None	Allows a user to create special permanent objects, such as \\Device
CreateToken	None	Creates a token object. Only the Local Security Authority can do this. The Local Security Authority ensures that the user has permission to access the system. It is not possible to audit the use of this right. For C2 certification, we recommend that it not be assigned to any user.
Debug	Administrator	Debugs programs or objects such as threads. You cannot audit this privilege. For C2 certification, we recommend that it not be assigned to any user, including system administrators.
IncreaseBasePriority	Administrators Power Users	Allows a user to increase the execution priority of a process.
IncreaseQuota	None	Allows a user to increase the object quotas.
InteractiveLogon	Most groups	Allows the user to log in interactively.
LoadDriver	Administrators	Allows a user to install and remove device drivers.
LockMemory	None	Allows a user to lock pages in the memory of the computer so the pages cannot be automatically backed up on a backing store like PAGEFILE.SYS.

Privilege	Default Assignment	Description
MachineAccount	None	Allows a user to add a new machine to a domain.
NetworkLogon	Everyone	Allows users to connect to a computer from anywhere in the network. This means users do not have to be at a specific place or terminal to log into their computer.
ProfileSingleProcess	Administrators Power Users	Allows a user to use performance-monitoring tools in order to monitor the performance of a single process.
RemoteShutdownPrivilege	Administrators Power Users	Allows a user to shut down a Windows system remotely.
Restore	Administrators Backup Operators	Allows a user to restore backed-up files and directories. This right replaces all file and directory permissions.
Security	Administrators	Allows a user to specify what types of resource access (such as file access) are to be audited, and to view and clear the security log. **Note:** This privilege does not allow the user to set system auditing policies using the Audit command from the Policy menu in Microsoft's User Manager. Administrators always have the ability to view and clear the security log.
ServiceLogon	None	Enables a process to register with the system as a service.
Shutdown	Administrators Backup Operators Everyone Power Users Users	Allows the user to shut down the system from the system console.
SystemEnvironment	Administrators	Allows a user to modify the system environment variables. This enables the user to set up the system environment at their workstation, and ensure that all other users working on the same workstation use the same setup.
SystemProfile	Administrators	Allows a user to perform profiling (performance sampling) on the system.
SystemTime	Administrators Power Users	Allows a user to set the time for the internal clock of the computer.

Privilege	Default Assignment	Description
TakeOwnership	Administrators	Allows a user to become the owner of files, directories, printers, and other objects on the computer. This right replaces all permissions protecting objects.
Tcb	None	Enables a process to perform as a secure, trusted part of the operating system. Some subsystems are granted this privilege.