SECURANT TECHNOLOGIES

ClearTrust SecureControl

Administrator’s Guide

Version 4.6.1

May 17, 2001

ClearTrust SecureControl, Release 4.6.1

The information in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. Securant Technologies, Inc. does not warrant that this document is error-free.

Securant Technologies, Inc., 345 California Street, 23rd Floor, San Francisco, CA 94104

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com) and Tim Hudson (tjh@cryptsoft.com).

Year 2000 Compliance Statement

Securant is committed to producing the highest quality software products and services. We recognize the issues and potential problems associated with the storage and calculations of dates with two digit year fields (Year 2000 problem). All dates used within our products utilize a standard four digit year or system specific representation.

When installed and implemented in accordance with our current written specifications, ClearTrust meets or exceeds the following rigorous requirements:

(i) records, stores, processes, calculates, transmits, displays, and presents calendar dates on or after (and, if applicable, spans of time including) January 1, 2000.

(ii) the use of dates before, on or after January 1, 2000 will not adversely affect performance with respect to date-dependent data, computations, output, or other functions.

(iii) will not abnormally end or provide invalid or incorrect results as a result of date-dependent data; and

(iv) accurately recognize, manage, accommodate, and manipulate date-dependent data including leap years.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

This document describes the Administrative components of the ClearTrust SecureControl system. Using this administrative toolkit, ClearTrust system administrators can perform the following functions:

- Create User accounts in the ClearTrust system.
- Define groups of Users for more convenient administration.
- Define resources to be protected (web pages, directories, and code).
- Define groups of resources for more convenient administration.
- Define access policies for resources according to a User’s identity, group membership, or User information.
- Designate Users as Administrators to whom system administration duties can be delegated.
- Keep track of and respond to system activity including system attacks.
- Share data with external directories such as LDAP directories and Microsoft’s ActiveDirectory.

COMPONENTS OF THE ADMINISTRATIVE TOOLKIT

The Administrative Toolkit is made up of the following components:

The Entitlements Manager Web User Interface

The Web User Interface is a browser-based GUI which allows Administrators to easily control access to system resources. Using the Web GUI, Administrators can limit access for specific individuals, for individuals with specific profiles, or for members of pre-defined groups. Administrators can also use the Web UI to designate Users as “Administrative Users,” giving them the ability to themselves control access to specified system resources for other specified Users.

THE ENTITLEMENTS MANAGER JAVA CLIENT

The Entitlements Manager Java Client is a Java-based GUI which replicates the functionality of the Web UI. Using the Java Client, Administrators can limit access to system resources for specific individuals, for individuals with specific profiles, or for members of pre-defined groups. Administrators can also use the Java Client to designate Users as “Administrative Users,” giving them the ability to themselves control access to specified system resources for other specified Users.

The Java Client is a client-side program that uses SSL encryption for all communications. It may require large amounts of memory on the client machine. (See the *Installation Guide* for more information).

CLEARTRUST SECUREDETECTOR

ClearTrust SecureDetector is the threat detection and response component of the ClearTrust Administrator toolkit. Using SecureDetector, an Administrator can log every event that occurs on either the Runtime or Administrative Server, and can specify security response actions to be taken if specific events occur. These actions include disabling accounts, sending email notification of an event, and disabling suspect connections on the CheckPoint Firewall.

THE DIRECTORY REPLICATION MANAGER

The Replication Manager allows administrators to share User data with external directories to allow access control through the ClearTrust system.

The Directory Replicator can be used to replicate data stored in LDAP databases (Netscape and PeerLogic Directory Servers, using the LDIF file format) or MicroSoft ActiveDirectory databases. Once replicated and imported, the data will be synchronized with user data stored in the ClearTrust SecureControl Entitlements Database.

DOCUMENT CONVENTIONS

This Administration Guide provides a general overview of the Entitlements Managers functions, as well as information about SecureDetector and the Directory Replicator. In addition to this paper document, Securant provides an on-line Administrator reference guide that provides step-by-step instructions on how to perform Administration functions using the Entitlements Managers.

The following typographical conventions are used throughout the Administration Guide and in the on-line documentation:

Table 1.1 Typographical conventions

Convention	Meaning	Example
San-serif bold	User interface elements such as buttons, menus choices, window names, dialog boxes, field names and so on.	**1.** Select **File** ▸ **Print**. **2.** Click **Save**.
SAN-SERIF BOLD UPPERCASE	Keyboard keys, including letters and numbers as well as Tab, CTRL, ALT, and so on.	Press **CTRL**+**ALT**+**DELETE**
italics	New terms, emphasized words or book titles.	See the *Administration Guide* for more information about using the Entitlements Manager.
UPPERCASE	Environment variables, SQL commands, logical operators, device names, acronyms, registry settings, system commands, and so on.	`SELECT object_name FROM user_objects` Mount your CD-ROM drive.
`Courier`	Code examples, files, directories, class names, commands, parameters and on-screen computer output.	Edit the `Default.conf` file in the `\SecureCtrl\Configuration` directory.

`Courier bold`	Typed input (as opposed to on-screen computer output).	`Entitlements server host:`
		`Entitlements_Server`

`<`*`italics`*`>`	Information to be determined by the reader. Substitute the appropriate name, directory, or other specific information.	`print <`*`filename`*`>`
`...`	In code examples, denotes the continuation of an argument, file or command.	`print <`*`filename1`*`>, <`*`filename2`*`>...`
`[ ]`	Optional information.	`reject [-d] <`*`filename`*`>`

CHAPTER

2

THE ENTITLEMENTS MANAGER BACKGROUND CONCEPTS

The ClearTrust SecureControl Entitlements Manager allows system administrators to easily create mechanisms to control User's access to system resources. The Manager includes tools to distribute administrative duties among specified Users, to organize Users into specified groups, to allow or deny access according to specified information about the User, to test access, and to establish password policies to avoid security breaches via compromised passwords. These tools are described in this chapter in the following sections:

- Delegated Administration
- Users, Groups and Realms
- Runtime Access Control
- Protected Resources
- Passwords
- ClearTrust SecureControl Administration Task Summary

The Entitlements Manager functions can be accessed using either a Java-based UI or a browser-based GUI. Those interfaces are described in more detail in Chapter 3, *The Entitlements Manager Web UI* and Chapter 4, *The Entitlements Manager Java Client UI*.

Note: This guide refers to entities in the ClearTrust SecureControl system (Users, defined Groups of Users, web servers, files, and so on) as *Objects*. *Resources* refers to Objects that can be accessed by Users, such as web pages, files, or defined groups of files.

DELEGATED ADMINISTRATION

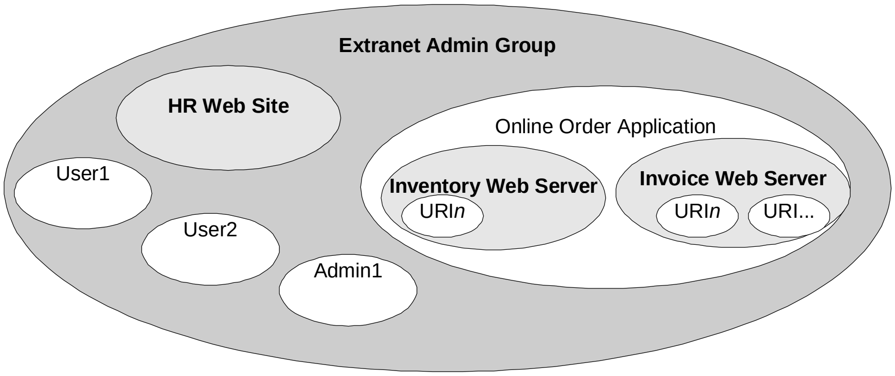
Rather than require a single System Administrator to control all the access functions for a protected system, ClearTrust SecureControl supports delegated administration via *Administrators, Administrative Roles*, and *Administrative Groups*.

Each *Administrative Role* has access to a specified set of functions in the Entitlements Manager, referred to as *privileges*. An *Administrative Group* is a specified collection of Users, Objects and system Resources. Administrative Roles and Administrative Groups are typically created by a *Super User*.

An *Administrator* is a User who has been assigned one or more Administrative Roles within an Administrative Group. Administrators can control Objects and Resources which they *own* (which are in the Administrative Group), according to the privileges of their Administrative Role.

In Figure 2.1: *Ownership of Objects by Administrative Groups* on page *2-2*, the Extranet Administrative Group owns the Online Order Application which contains the Inventory Web Server and the Invoice Web Server, which themselves in turn contain *URI*s. The Extranet Administrative Group also owns several Users and the HR Web site. Admin-1, the Administrator in the Administrative Group, can control access to these Resources according to the privileges of the Administrative Role or Roles to which Admin-1 belongs.

Figure 2.1 Ownership of Objects by Administrative Groups



For information about Users, see *Users, Groups and Realms* on page *2-5*. For information about Applications, Web Servers and URIs, see *Protected Resources* on page *2-16*. This section contains information about the following:

- Super Users
- Administrative Groups
- Administrative Roles
- Public and Private Objects

SUPER USERS

A *Super User* is an Administrator who has access to the highest level of the Entitlements Manager’s functionality. Super Users, and *only* Super Users, can do the following:

- “Lock out” a User. Locking out a User immediately disables all access that the User might have to protected Resources.
- Transfer ownership. Only the Super User has the ability to give ownership, remove ownership, or transfer ownership from one Administrator to another.

The initial Super User is specified during installation of the ClearTrust SecureControl system, and will automatically be created on the system as a member and Administrator of the default Administrative Group (“SecureControl_Administrative_Group”). Only a User who is an Administrator can be identified as a Super User.

> ***Warning:*** At least one Super User must exist at all times.

It is possible for the SecureControl system to function with only one Administrator, who is the Super User. However, delegated administration relieves the Super User of having to perform all the administrative tasks associated with controlling access to system Resources.

> ***Important:*** The Super User role is unique in that it’s not bound by Administrative Group or Administrative Role permissions; however, when you create objects as a Super User, the ownership is still determined by the Administrative Role you selected when you logged on to ClearTrust SecureControl Manager. For more information about Administrative Roles, see *Administrative Roles* on page *2-4*.

ADMINISTRATIVE GROUPS

Every ClearTrust SecureControl-protected Object and Resource is associated with an Administrative Group, which is its “owner.” An Administrative Group can typically modify or protect only those Objects and Resources that it owns).

The following Objects can be owned:

- **User -** A person’s account on the system. A User’s account information in the SecureControl system always includes *Fixed Attributes* (Name, e-mail, password, and so on). Administrators with the appropriate privilege can also define new *User Properties* (for example Social Security Number or security clearance grade) that can be used to control access.
- **Group -** A group of Users
- **Realm -** A group of Groups
- **Application -** A set of programs and data that has been grouped together and named
- **URI -** (Uniform Resource Identifier) A file or directory name on a web server (usually the same as a URL without the domain name).
- **Server Tree**
- **Web Server**
- **User Property Definition -** Customized information to be associated with each User account. For more information about User Properties, see *Users, Groups and Realms* on page *2-5*.

The owner of the Object or Resource is usually the Administrative Group to which the Administrator creating the entity belongs, but it is possible to create an object or resource for another Administrative Group.

Administrative Groups usually reflect organizational structure (for example “Marketing,” “Sales,” “Shipping,” and “Engineering”) or geography (New York, Chicago, and Los Angeles). Administrative Groups can include Extranet partners, customers, and others external to the organization.

> ***Note:*** A User’s password policy (expiration date, minimum length, and other characteristics) is determined by the password policy associated with the Administrative Group that owns the User. For more information about passwords, see *Passwords* on page *2-22*.

ADMINISTRATIVE ROLES

An Administrative Role is a collection of privileges that can be assigned to an Administrator in an Administrative Group. Administrative Roles are named when they are created, and are referred to by that name in the SecureControl system. Roles typically reflect an Administrator’s function in the organization (For example “Help Desk,” or “HR”). A list of possible Administrative Role privileges is below:

- **Administrative Roles -** The ability to add, modify, or delete Administrative Roles.
- **Ownership -** The ability to modify ownership of Resources.
- **Users -** The ability to add Users, modify a User’s Fixed Attributes and User Properties, and delete Users.
- **Groups -**The ability to add Groups, modify a Group’s properties, or delete Groups.
- **Realms -** The ability to add Realms, modify a Realm’s properties, or delete a Realm.
- **Applications -** The ability to add, modify, or delete Web Applications, including Application Resources (URIs).
- **Web Servers -** The ability to add, modify, or delete Web Servers.
- **Passwords -** The ability to modify (but not create or delete) a User’s password.
- **User Property Definitions -** The ability to add, delete, or modify User Property definitions.

PUBLIC AND PRIVATE OBJECTS

Objects in the SecureControl system are typically designated as “public” - that is, they can be seen in the Entitlements Manager GUI by all Administrators, regardless of whether or not they are members of the Administrative Group that owns the object (though only members of the owning Administrative Group with the appropriate privileges can modify and delete public Objects).

To control Administrators’ access to sensitive information, it is possible to designate an object as “private.” A object that is private only appears in the Entitlements Manager when the Manager is being used by Administrators of the Administrative Group that owns the object.

The following Objects can be designated as private:

- User (including all Fixed Attributes and User Properties associated with that User)
- Group
- Realm
- Application
- Web Server
- URI on an Owned Web Server
- User Property Definition

In Figure 2.2, Administrators in the Extranet Admin Group cannot see any of the Objects owned by the Intranet Admin Group (web server 1, User 2 and User 1) because these Objects have been made private. On the other hand, Administrators in the Intranet Admin Group can see the Online Order Application and User 3 owned by the Extranet Admin Group because these objects are public.

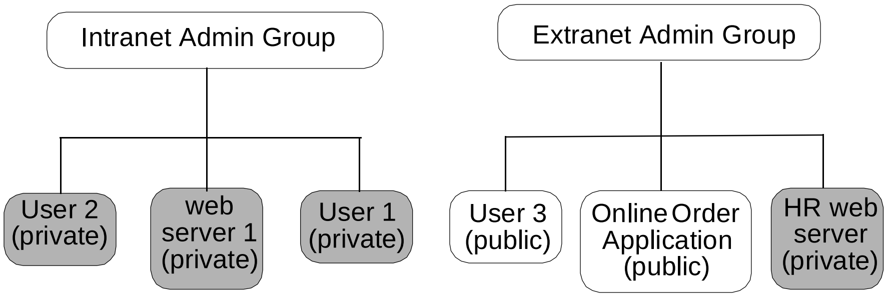


Figure 2.2 Public and Private Objects

By default, all Objects are public. An Object can be designated as private when it is being created, or modified to be private later.

> ***Warning:*** It is possible for a SuperUser to give a User access to Resources which do not belong to that User's Administrative Group and which have been designated as Private. Those Resources and their associated access permissions will not be visible to the User's Administrative Group's Administrators. This functionality should be used with discretion.

USERS, GROUPS AND REALMS

The ClearTrust SecureControl system controls access to *Resources* and *Applications* based on the characteristics of the *User*. Each User Account is associated with a unique User ID, as well as with several Fixed Attributes and, potentially, several User Properties.

Each person using the system will typically be associated with only one User account, though it is possible for several people to share an account, for a single person to have several accounts, and for User accounts to be associated with job descriptions instead of people.

To make system administration more convenient, SecureControl allows Users to be grouped into Groups, and allows Groups to be grouped into Realms. It is possible to control access to system Resources and Applications by a User's membership in a Group or Realm, instead of individually.

In the diagram below, User2 is part of Group 1, which is part of a Realm.

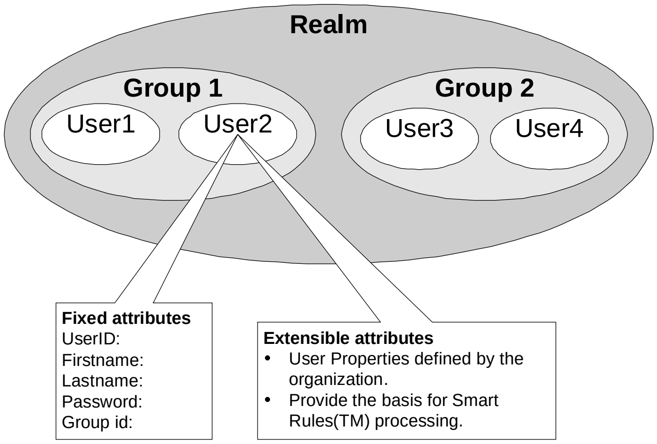


Figure 2.3 Realms Contain Groups; Groups Contain Users

For more information about *Applications* and *Resources*, see *Protected Resources* on page *2-16*. This section contains information about the following:

- Users (including Fixed Attributes and User Properties)
- Groups
- Realms

USERS

A User is an individual login account in the SecureControl system. User accounts are typically associated with one person, although it is possible for more than one person to share an account ("guest," for example). It is also possible for one person to have access to more than one account ("charlie" and "superuser," for example), and for User accounts to be associated with job descriptions instead of people (for example "HR1" or "Front Desk").

Each User account *must* have a unique Login ID, which is determined when the User is created and which cannot be changed.

Other items of information about the User besides Login ID are also specified when the User is created or modified. Some of those items of information - called *Fixed Attributes* - already have fields reserved for them in the **Create User** (or **Modify User**) dialog in the Entitlements Manager. Additional items of information about Users - called *User Properties* - can be defined by Administrators as necessary. Fields associated with User Properties will also appear in the **Create User** (or **Modify User**) dialog.

Fixed Attributes and User Properties are discussed in the rest of this sub-section. For information about controlling access via Fixed Attributes and User Properties, see *Runtime Access Control* on page *2-10*.

Important: If you are going to control access to a resource via a User Property, you should define that User Property before creating any Users, so that you can specify the value of that User Property for each User as they are being created. (For more information about controlling access via a User Property, see *SmartRules* on page *2-12*).

Fixed Attributes

Fixed Attributes are items of information associated with an individual User Account. Fixed Attributes can be specified when the User is being created, or can be modified later (except for Login ID, which cannot be modified). Some Fixed Attributes are required, some are optional, and some will probably be used only rarely (for example, **Locked Out**). Following is a table of Fixed Attributes.

Table 2.1 Fixed Attribute Descriptions

Fixed Attribute	Description	Notes
UserID	Login ID for the User	Required
First Name	User's first name	Optional
Last Name	User's last name	Optional
Email Address	Email address for the User	Optional
DN	Distinguished name (X.500 schema)	Optional
Account Start	Date and time the User's account becomes active	The default is the host machine time when the User's information is saved (thus, when the User is "created").
Account Expiry	Date and time the account will expire	The default is 1 year after Account Start.
Owner	Administrative Group that owns the User account	The default is the Administrative Group of the Administrator that created the User.
Password status	Indicates whether the password is *active* or has *expired*	

Table 2.1 Fixed Attribute Descriptions

Fixed Attribute	Description	Notes
Password expiration date	The date the password will expire. (It is also possible to force expiration of a password by checking the “Force Password Expiration” checkbox. Among other uses, this can be used to force newly created Users to change their passwords the first time they log in).	The default lifetime of a password is determined by the password policy associated with the Administrative Group that owns the User.
Private	Identifies the User account as private; only the owning Administrative Group will be able to view this User and their associated account information.	The default is public. Private Users can only be seen by an Administrator in the same Administrative Group as the Administrator who created the User.
Super User	Creates the User as a Superuser. Super Users can perform any action on any Object or Resource.	This checkbox is only enabled if the Administrator creating or modifying the User is a Super User. The User must be an Administrator. Assign with caution.
Locked Out	Immediately disables any permissions granted to the User, and blocks them from accessing protected Resources.	Only Super Users can enable this feature.

User Properties

User Properties are items of information that are created by Administrators specifically for their organization. User Properties must be one of five specific data types, which are described in the table below. (Note that Fixed Attributes can also be categorized according to these data types).

Table 2.2 User Property types and examples

Type	Description	Example
BOOLEAN	"True" or "False"	Current depositor? External User? Customer?
STRING	A character string	The User's street address
INT	An integer	The User's zip code The User's level of security clearance
FLOAT	A floating point decimal value	The User's account balance The User's shoe size
DATE	A date	The User's birthday The User's retirement date

Using the SecureControl system, it is possible to allow or deny a User access to system Resources according to the values of their User Properties (for example, to only allow current customers to access a mail program, or only allow Users over the age of 18 to access certain directories on the web server). To do this, Administrators use SmartRules. For more information about SmartRules, see *SmartRules* on page *2-12*.

Creating User Properties

User Property definitions can be created in several ways:

- By an Administrator using the **Create User Property** dialog in the Entitlements Manager (see the on-line documentation for the Entitlements Manager Web UI and Java Client for more information).
- Automatically, by specifying a customizable action in *SecureDetector*.
- Automatically, by the `createUserPropertyDefinition` function in the ClearTrust SecureControl API.

Specifying and changing User Property values

The values of User Properties for individual Users can be updated in several ways:

- Directly, via the **Modify User** dialog in the Entitlements Manager (see Chapter 3, *The Entitlements Manager Web UI* and Chapter 4, *The Entitlements Manager Java Client UI* for more information).
- Indirectly, using a custom Application that changes the value of the User Property via the ClearTrust SecureControl API.

- By importing new data from an external database via ClearTrust's Database Replicator tool. (See Chapter 5, *Integrating Other Directories and ClearTrust* for more information).

GROUPS

Groups are simply specified groups of Users. A Group must have a unique name, and may also have an associated description. A User can belong to more than one Group.

Access to system Resources can be controlled according to Group membership as well as according to the individual User. How Users are Grouped will depend on the needs of the organization. A school, for example, might create a Group called "Teachers," with access to word processing software, database software, student records, assignments and test answers, a Group called "Students," with access only to software and assignments, and a Group called "Administration," with access to all of the above plus teacher's salaries.

REALMS

Realms are specified groups of Groups. A Realm must have a unique name, and may also have an associated description. Groups can belong to more than one Realm.

Access to system Resources can be controlled according to Realm membership, as well as according to Group membership or individual User. How Groups are grouped into Realms will depend on the needs of the organization.

RUNTIME ACCESS CONTROL

Using the SecureControl system, it is possible to limit a User's access to system Resources in two ways - *explicitly*, by the identity of the User or by their membership in a Group or Realm, and *implicitly*, according to the value of the User's *User Properties*. Limits based on the User, Group or Realm are called *Basic Entitlements*. Limits based on User Properties are called *SmartRules*. Basic Entitlements and SmartRules are discussed further in the rest of this section.

Basic Entitlements and SmartRules control access to system Resources in conjunction with A*pplications* (specified groups of system Resources) and *Application Functions* (sets of access rules customized for different functionalities within the Application). By default, each Application is automatically associated with a general "ACCESS" Application Function when it is created. It is also possible to create custom Application Functions to fulfill work-flow, application portal, or other specialized requirements; to do so, you must create applications that implement the ClearTrust SecureControl API.

See *Protected Resources* on page *2-16* for information about Applications. See the *Developer's Guide* for details about creating custom Application Functions.This section discusses the following:

- Basic Entitlements
- SmartRules

BASIC ENTITLEMENTS

A Basic Entitlement explicitly *allows* or *denies* access to a specific Resource (typically an Application). Basic Entitlements can be specified at the User, Group or Realm level.

- Basic Entitlements assigned at the User level affect only that User.
- Basic Entitlements assigned at the Group level affect all of the Users contained in that Group.
- Basic Entitlements granted at the Realm level affect all Users in all Groups within that Realm.

If a Group is granted access rights to a Resource through a Basic Entitlement, all the Users in the Group have access rights to the Resource unless they are specifically excluded. If a Realm is granted access to a Resource through a Basic Entitlement, all Groups and Users in the Realm have access to the Resource unless excluded at the Group or User level.

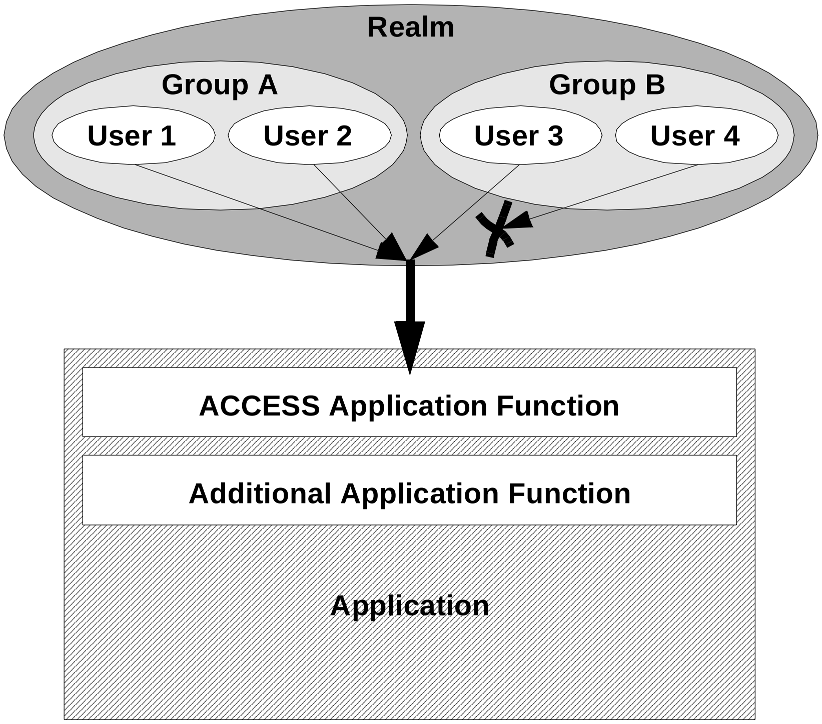
Resolving Multiple or Contradictory Entitlements

Since Entitlements can exist at several levels, Users can belong to multiple Groups, and Groups can belong to multiple Realms, it’s possible to create contradictory Basic Entitlements. If Basic Entitlements are in conflict, access to Resources is resolved as follows:

- The Entitlement at the more specific level takes higher priority - User is a more specific level than Group, Group more specific than Realm.
- All Entitlements at the same level must be *allow* for access at that level to be allowed. (If a User is a member of more than one Group, all the Groups’ Entitlements must be set to *allow* or the User will be denied access).

Thus, if a User has an explicit *allow* as a member of a Group that has been granted access but also has an explicit *deny* based on the individual User account, that User will be denied access to the Application. Similarly, if a User is a member of one Group that has an explicit *allow*, but another that has an explicit *deny*, that User will be denied.

In the example below, all the members of the Realm have been allowed access to the ACCESS function of the Application, but User4 has been explicitly denied.



SMARTRULES

Basic Entitlements enable you to specify access to Resources on a per-User, per-Group, or per-Realm basis. However, some organizations may want more flexibility and control than Basic Entitlements provide. ClearTrust's SmartRules let you apply access rules directly to *Resources* (rather than to Users, Groups, or Realms) based on User Properties.

By basing access on User Properties, rather than via a static Basic Entitlement, it is possible to change a given User's access privileges immediately and simultaneously throughout the system. Thus, for example, if an organization has implemented a User Property called Employment Status (a Boolean value), then when employees are terminated the Smart Rule based on Employment Status can instantly revoke all access privileges as soon as that one property is changed.

This sub-section contains information about the following:

- Forms of SmartRules
- Types of SmartRules
- Combining SmartRules
- Testing
- Examples of Smart Rule usage

Important: SmartRules decide a User's access to a specified Application ***only*** if no relevant Basic Entitlement exists at any level (User, Group, or Realm). Basic Entitlements ***always*** take precedence over SmartRules.

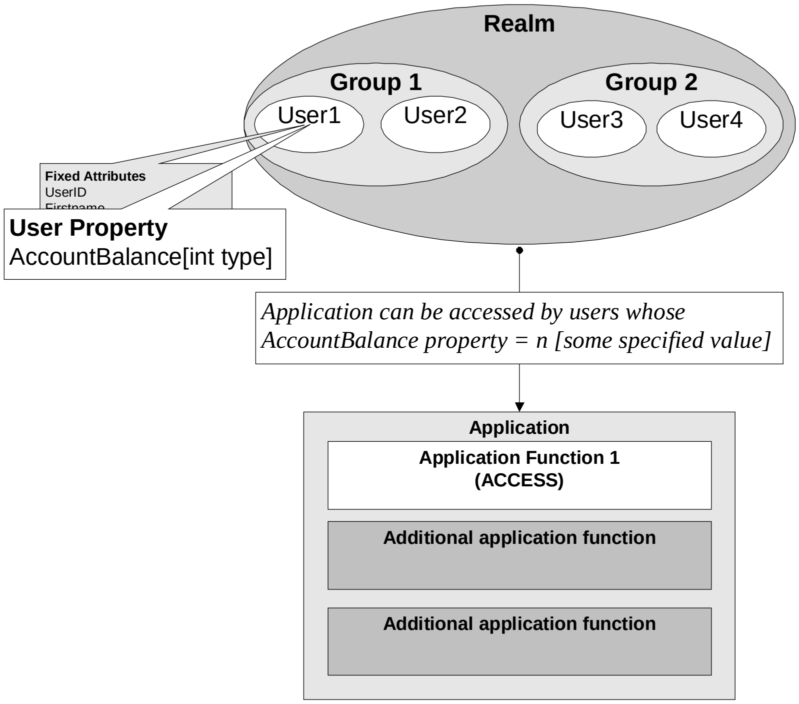
Forms of SmartRules

A Smart Rule compares the value of a User's User Property to a specified value (a *comparison criterion)* according to a *comparison operator*. Smart Rule operators are described in the following table:

Table 2.3 Smart Rule Operators

User Property	Operator
Date	Before, After
Boolean	Is Not, Is
String	Does Not Contain, Ends With, Equals, Starts With, Contains (you can also apply numeric operators to Strings).
Integer, Float	>=, <, +, >, <=, !=

In the following figure, a Smart Rule "Allow if AccountBalance = *n*," based on the created User Property "AccountBalance," is used to limit access to the Application to Users who have an account balance equal to *n*, where *n* is some specified value.


Realm
Group 1
Group 2
User1
User2
User3
User4
Fixed Attributes
UserID
Firstname
User Property
AccountBalance[int type]
Application can be accessed by users whose
AccountBalance property = n [some specified value]
Application
Application Function 1
(ACCESS)
Additional application function
Additional application function

Types of SmartRules

SmartRules can be created in one of three types — `ALLOW`, `DENY`, or `REQUIRE`. These types are explained further in Table 2.4.

Table 2.4 Smart Rule types

Type	Processing Order (default)	Logic for Multiple Rules of This Type	Usage Notes
Deny	First	OR	If the value of the User Property meets the condition, the User is denied access immediately; no further rules are evaluated.
Allow	Second	OR	If the User Property meets the condition, the User can access the Application Function immediately; no further rules are evaluated
Require	Last	AND	If the value of the User Property meets the condition, SecureControl evaluates the next Require rules. If all Require rules are fulfilled and Allow and Deny rules allow access, the User is granted access.

The three kinds of SmartRules can be combined in various ways to implement business rules and control access to an Application.

Important: If a User has a User Property of value “N/A” (not yet entered), a Deny rule based on that User Property will consider the condition not met (will not Deny) if the Authorization Server is set to *active* mode, but will consider the condition met (will Deny) if the Authorization Server is set to *passive* mode. The Authorization Server mode is set in the `Default.conf` file, by the `securecontrol.aserver.authorization_mode` parameter. By default, the parameter is set equal to active. (See the *Installation and Configuration Guide* for information on changing the setting.)

Combining SmartRules

An individual Smart Rule applies a single condition to one particular User Property. To create more complex conditions for access, you can define and combine multiple SmartRules. For example, say the Application Function ACCESS for a particular Application has these two SmartRules associated with it:

```
ALLOW if State = CA
DENY if Age < 21
```

and User Joe has values set for each of these properties, as follows:

```
State = CA
Age = 18
```

If the default processing order for ACCESS (**Deny->Allow**) is in effect, then the SmartRules are evaluated as follows:

1. **DENY** if Age < 21
2. **ALLOW** if State = CA

Joe will be denied access because of the value in his User Property for Age. The second Smart Rule is never evaluated.

Deny ->Allow is the default processing order of SmartRules. Administrators can reverse the order—so that Allow Rules are processed before Deny Rules - by changing the priority in the associated Application Function.

In the previous example, access was ultimately denied. Changing the processing priority to **Allow->Deny** in the example changes the processing order as follows:

1. **ALLOW** if State = CA
2. **DENY** if Age < 21

Joe would be granted access because he meets the **ALLOW** condition. The **DENY** condition is never evaluated.

Following are some more complex examples of Smart Rule use.

Testing

Before implementing a security policy based on created SmartRules, it's a good idea to test the defined rules to see if they are operating as intended. The testing tool in the Entitlements Manager allows administrators to simulate a specific User attempting to access a resource in order to test created SmartRules.

Note: If you have just created a User or changed a User's User Properties, that User will not be represented properly in the Entitlement Server's cache. To update the cache, you must explicitly flush its contents. The Entitlements Manager includes a "Flush Cache" function.

Examples of Smart Rule usage

Example One

In this example, the organization using the ClearTrust SecureControl system is an insurance company with customers throughout the south- and north-west United States. At the beginning of its fiscal year, the company decides to make a special offer available to residents of California, Texas, and Oregon via its Web site. To accomplish this the insurance company creates three SmartRules to control access to the area of the Web Server containing the special offer (having already created a User Property called "State," normally used as part of the customer's mailing address):

- **ALLOW** if State = CA
- **ALLOW** if State = TX
- **ALLOW** if State = OR

This simple setup accomplishes the desired goal. Residents of California, Texas, and Oregon can access the special offer, and everyone else is denied access.

A month later, the insurance company decides it must limit the offer to Users with good credit ratings. Since there is already another User Property called “bad-credit,” (a Boolean which is set to yes if the account has been flagged for non-payment), adding another Smart Rule is straightforward:

- **DENY** if bad-credit = true
- **ALLOW** if State = CA
- **ALLOW** if State = TX
- **ALLOW** if State = OR

Since the priority for this Application Function is set to its default value, **DENY -> ALLOW**, Deny rules will be evaluated first. Now only Users with good credit from California, Texas, or Oregon can access the insurance company’s “special offer” web page.

Example Two

It is also possible to combine SmartRules of the `REQUIRE` type. In this example, a company wants to limit access to an area of its Web site to retail customers that have account balances over $100. In this case, both parts of the condition must be met or the User should be denied access. The ClearTrust Administrator creates two SmartRules:

- **REQUIRE** Account Balance> 100
- **REQUIRE** Account Type = Retail

At runtime, only retail Users with account balances in excess of $100 will be allowed access to the site.

PROTECTED RESOURCES

The ClearTrust SecureControl allows Administrators to control Users’ access to Resources such as files (including cgi files), directories, and software. Before these Resources can be protected, however, they must be identified to the system. An individual Resource in the SecureControl system is identified by its *URI* (Universal Resource Identifier). A specific, named, group of URIs is known as an *Application*.

To specify a resource (an Application or URI), it is necessary to first identify the Web Server or Web Servers on which it resides. Web Servers are identified by a name that has been explicitly assigned to them in the SecureControl system (not by DNS entry). In addition to explicitly naming Web Servers, it is possible to explicitly name *Server Trees* (groups of Resources on a Web Server), so that different Administrative Groups can own different parts of the same Web Server.

For information about protecting Resources using Application Functions, Basic Entitlements and SmartRules, see *Runtime Access Control* on page *2-10*. This section contains information about the following:

- Web Servers (including Server Trees, Server Redirection and Mirror Sites)
- Applications (including Application Functions and Web Server mapped documents)
- URIs (including URIs in overlapping applications and Dynamic Content)

Important: Active and Passive Mode

Before using the Entitlements Manager to define protected Resources, you should be aware of whether your ClearTrust environment is configured for *active* or *passive* mode. Access to Resources not explicitly defined as part of an Application will depend on this configuration.

If the system is configured in active mode only those Resources that are part of an Application and associated with an Application Function are protected.

If the system is configured in passive mode every Resource is protected, whether or not it's part of an Application. To provide access in this mode, you must expressly configure each Resource as part of an Application.

From an Administrator's stand-point, passive mode involves more configuration work. You'll have to explicitly create Applications for anything you want your Users to be able to access, or they'll be denied access. On the other hand, if you intend to protect all of your resources passive mode will ensure that this occurs.

In either case, any Resource that's protected will require either a Basic Entitlement or a Smart Rule to determine access, or the access will be denied.

The Authorization Server mode is set in the `Default.conf` file, by the `securecontrol.aserver.authorization_mode` parameter. By default, the parameter is set equal to active. (See the *Installation and Configuration Guide* for information on changing the setting.)

WEB SERVERS

Before you can protect a Resource or Application, you must identify to the system the web server (or web servers) on which it resides. Web servers in the ClearTrust SecureControl system are identified by name, not domain name. When a web server name is created in the system the following information about the web server is associated with it:

Table 2.5 Web Server information

Server Information	Description	Comments
Name	The name by which the web server is known to the ClearTrust SecureControl system	Each web server in the system must have a unique name. The name must match the value of the `securecontrol.plugin.web_server_name` parameter in the web server Plug-in's `Default.conf` file. (The default name in that file is "WebServer").
Hostname	This must match the actual, fully-qualified name of the web server	For example, *hostname.domain.com*, or the web server's IP address.

Table 2.5 Web Server information

Server Information	Description	Comments
Port number	This is the port address on which the web server advertises its http services.	The default is port 80, but this can be changed if the web server is configured with a different port number.
Owner	The Administrative Group that owns this web server.	By default, this is the Administrative Group of the Administrator account that created the web server. A Super User can transfer ownership to another Administrative Group.

Server Trees

Access to a Web Server is controlled by the Administrative Group that owns the server (typically the Administrative Group that created the Web Server). To facilitate delegated administration, it is possible to divide the Resources on a Web Server into Server Trees. Server Trees, and therefore the Resources which they contain, can be owned by different Administrative Groups. Administrators from these Administrative Groups can then create the Applications made up of these Resources, and can control access to these Applications.

Server Redirection

Sometimes an organization may want a ClearTrust SecureControl protected Web Server to redirect a User's browser to another page.

It is possible to configure the ClearTrust SecureControl Web Server Plug-in to redirect a User's browser to different locations in the event of authorization failure. More than one alternate location is supported - ClearTrust SecureControl can return different HTML pages depending on the reason for the failure. For more information on redirecting the User's browser, see the *Installation and Configuration Guide*.

It is also possible to use HTTP to refer the browser to a different page once the referring page has been requested. Refer to the documentation that came with your Web Server to see how to configure it to perform that kind of redirection.

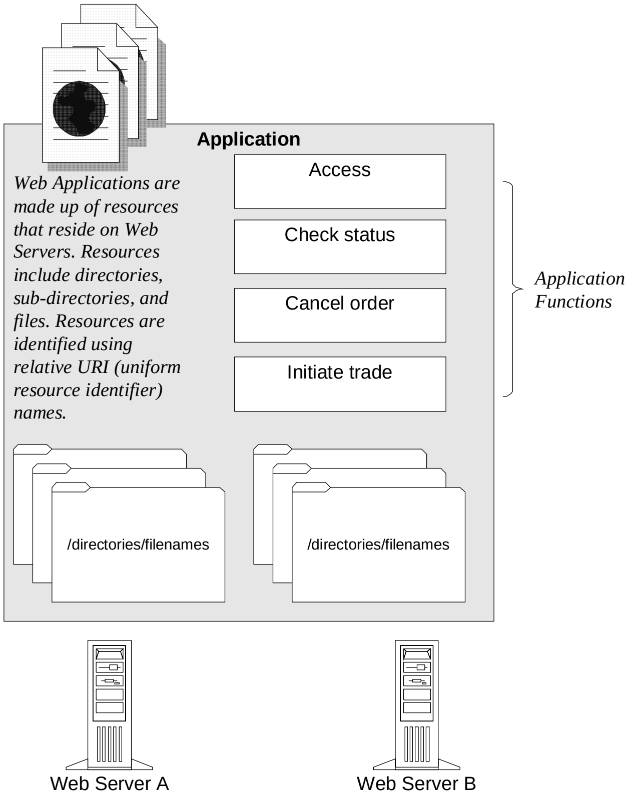
Mirror Sites

If an organization has several load-balanced web servers that are acting as mirror sites (they all serve the same content, and have the same directory structure and files), those servers can all be named the same thing in the Entitlements Manager. In addition to having the same name in the Entitlements Manager, the servers must all have the same name specified in their web server Plug-in's `Default.conf`. URIs will only need to be assigned once for mirrored Resources.

If servers are configured this way it will not be possible to track activity on each individual web server separately in the ClearTrust SecureControl logs. To track activity separately for each server, they must be named differently and URIs assigned on each one.

APPLICATIONS

An Application is a collection of Resources in the ClearTrust SecureControl system that have been explicitly specified and named. Resources included in an Application can include web pages, cgi files, directories, gif or jpg files, databases, and so on.


Application
Access
Check status
Cancel order
Initiate trade
Application Functions
Web Applications are made up of resources that reside on Web Servers. Resources include directories, sub-directories, and files. Resources are identified using relative URI (uniform resource identifier) names.
/directories/filenames
/directories/filenames
Web Server A
Web Server B

Resources in an Application are specified by the Resource's *URI*. Adding URIs to an Application is subject to the following limitations:

- A specific URI can be defined as a member of only one Application at a time. The same URI cannot be added to more than one Application.
- Since a URI can be a directory, URIs in different Applications can overlap.
- A single Application can contain URIs on more than one Web Server, as long as the Administrative Group that owns the Application also owns the all the Web Servers or Server Trees and all the included URIs.

URIs are discussed further later in this section.

Application Functions

Application Functions define access permissions for a specified group of URIs within an Application. ClearTrust SecureControl automatically includes the default Application Function, ACCESS when an Application is created. Unless otherwise configured, ACCESS allows access to all the URIs within an Application. It is possible to define more specific and complex Access Functions using the ClearTrust SecureControl API.

Web Server mapped documents

Web Servers often display a file that is different from the URL requested by the browser. For example, entering `http://www.acme.com/` in a Web browser will usually display the page `index.html`, located in the default web directory for the acme.com domain. To protect pages that can be accessed by more than one URL, be sure to include both URI in the Application. In this example, you'd specifically define both `/` and `/index.html`.

URIs

All Resources on a Web Server that will be added to an Application must be identified by a Universal Resource Identifier (URI). URIs are inclusive - on a system where the `/marketing` directory contains the `/applications` directory, for example, the URI `/marketing/*` contains everything in the `/applications/` directory.

Administrators can only manage URIs in their own Administrative Group. Trying to add another Administrative Group's URI to your Application will generate an error message.

A URI can only belong to one Application at a time, but overlapping URIs can belong to different Applications. A URI can also designate dynamic content.These issues are discussed further in the remainder of this section.

> ***Warning:*** When specifying directories on a web server to be protected, do not use "`/*`" to protect the entire web server. Using a "`/*`" to protect your entire web server will block the SecureControl system itself from accessing the CGIs and forms needed to perform operations such as password changes. To protect all the files on your web server except the SecureControl files, move all the directories except `/securant` into a sub-directory and then protect that sub-directory.

URIs in overlapping applications

A URI can only be part of one Application at a time, but because URIs can overlap it is possible for Resources to belong to more than one Application. When determining if a User has access to a resource, SecureControl will apply the most explicit URI available for that resource.

Figure 2.4: *An example of a Web Server with multiple Applications* on page *2-21* includes the following Applications:

- The "Profit Projections" Application, which contains the URI `/projections/profits/*`
- The "Salaries" Application, which contains the URI `/salaries/*`
- The "Finance Server" Application, which contains `/*`

Both the Profit Projections and Salaries Applications overlap the boundaries of the Finance Server Application. When a User tries to access a Resource that matches more than one Application, which entitlements will be enforced?

Figure 2.4 An example of a Web Server with multiple Applications

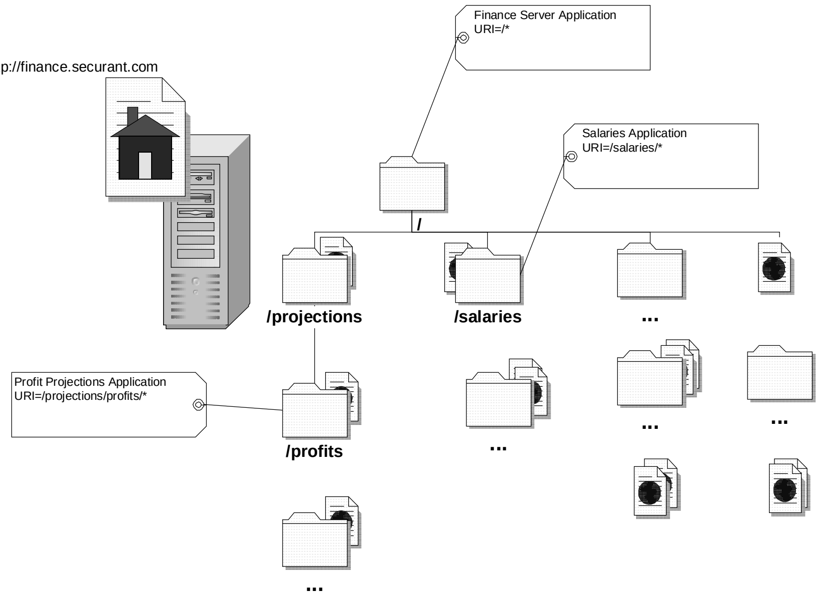

Finance Server Application
URI=/*
http://finance.securant.com
Salaries Application
URI=/salaries/*
/
/projections
/salaries
...
Profit Projections Application
URI=/projections/profits/*
/profits
...
...
...
...

Table 2.6 describes how some access attempts will be handled by the SecureControl system.

Table 2.6 Access to overlapping URIs

Resource	Most Explicit URI	Application Determining Access
`/projections/profits/`	`/projections/profits/*`	Profit Projections
`/projections/spending/`	`/*`	Finance Server
`/salaries/exec.html`	`/salaries/*`	Salaries
`/salaries/slack/bob.gif`	`/salaries/*`	Salaries
`/salaam.html`	`/*`	Finance Server

Dynamic Content

Within ClearTrust SecureControl, server-side programs and scripts are treated like any other Web content. CGI, Active Server Page, or similar files can be designated by a URI and included in an Application. For example, the following are all valid URIs to add to a ClearTrust SecureControl Application:

- `/projections/spending/today.cgi`
- `/projections/sales/db_update.pl`
- `/receivables/aging_report.asp`

Dynamically created URIs, however -- pages using a CGI or any other server-side program that appends data to the URL at submission time (using GET, for instance) - should be designated using a wildcard. For example, the URI to designate a web page such as:

```
http://yourserver.domain.com/budget/today.cgi?day=tuesday
```

is:

```
/budget/today.cgi/*
```

It is also possible to specify automatically generated pages and images that are all in one directory by designating the directory as the URI using a wildcard. For example, if all of the automatically generated content will be in a directory called `/results/daily/`, everything in that directory including the automatically generated content can be designated using the URI `/results/daily/*`

PASSWORDS

The ClearTrust SecureControl Entitlements Manager includes functionality to define and enforce *Password Policies*. Password Policies are associated with Administrative Groups. The policy applied to a User's password depends on the Administrative Groups that the User belongs to. If no Password Policy has been defined for an Administrative Group, the The SecureControl Default Password Policy will be applied.

Important: There must be a Default Password Policy for the system at all times. The existing Default Password Policy cannot be deleted unless you first define another policy as the default. There cannot be more than one Default Password Policy at one time.

Design of a Password Policy requires common sense. Forcing Users to live with an overly strict Password Policy (for example, one that requires overly long passwords or very frequent password changes) may cause them to compromise security (most commonly by writing their passwords down).

This section contains information about the following:

- SecureControl Password Policy Features
- Individual Password Management

SECURECONTROL PASSWORD POLICY FEATURES

SecureControl includes the following Password Policy features:

Length

Passwords that are too short are vulnerable to brute force attacks, but passwords that are too long can be difficult to remember, and may cause problems in some poorly-written programs. SecureControl allows Administrators to specify a minimum and maximum required length for User passwords.

A password shorter than six characters is probably unacceptably weak, but a password longer than 32 characters could also be problematic.

Because the algorithm used by SecureControl for encrypting passwords encrypts all passwords to be the same length, the length of the password is unimportant to the SecureControl system itself.

Non-Alphabetic Characters

Because the most common attacks used by crackers are dictionary attacks, adding a few non-alphanumeric characters to a password can enhance a password’s security greatly (for example, changing “password” to “password-327”). SecureControl password policies can be configured to require at least one non-alphabetic character.

Most common alphanumeric substitutions (the numeral 1 for the letter l, the numeral 3 for the letter E and the numeral 7 for the letter T, among others) have been integrated into cracking tools.

Character Exclusion

If a password is going to be used in more than one environment (particularly if it is going to be used in a UNIX environment), it would be better if it did not contain certain non-alphanumeric characters. Characters such as &, `*`, and `/` can have unpredictable effects when used in strings passed to some common UNIX commands. SecureControl allows you to reject potential passwords that include specified characters.

Dictionary Search

SecureControl will match potential new passwords against a list of words (in the file `words.txt`) and exclude passwords that are on the list. `words.txt` contains several thousand commonly-used words that will likely be included as part of any dictionary attacks on the system. The SecureControl installation also includes empty.txt, to which you can add your own words to be excluded.

Password History

A common way Users deal with strictly-enforced password policies (particularly in system where passwords must be changed frequently) is to come up with two or three “good” passwords and rotate among them. SecureControl checks Users’ potential new passwords against a list of their previous passwords and rejects the new password if it has been used before. This function can be configured to compare the potential new password to the last 0 to 25 passwords.

Password Lifetime

The longer a password exists, the more likely it is to be compromised. SecureControl includes a function to force Users to change their passwords after a specified period of time has passed. When Users’ passwords expire, they will be locked out of any SecureControl-protected Resources until they choose a new, valid password.

Password Expiration

A User’s password can be expired before the Password Lifetime is up via the SecureControl API, or in the Entitlements Manager by setting the User’s password’s expiration date to match the current date or by checking the “Force Password Expiration” checkbox. Among other uses, this forces the User to change his/her password the next time he or she authenticates.

Individual Password Management

Note: The default password (“ch4nge_me”) is automatically set when a new User is created in the SecureControl Entitlements Manager. If the **Force Password Expiration** checkbox is selected (or the `force_password_expiration` parameter is set to *true*), the User will be automatically prompted to change their password the first time they log in. If the **Force Password Expiration** checkbox is de-selected (or the `force_password_expiration` parameter is set to *false*), the default password will be active for the period of time specified for passwords by the User’s Administrative Group’s Password Policy.

SecureControl’s API provides functionality for individual password management in the form of CGIs and Java Servlets.

Web-based Password Change and Reset

Web Users can change their passwords through the SecureControl *Password Change* Web page. This page can be customized to have the same look and feel as the rest of a Web site.

The Password Change Web page asks the User to provide his or her old password and then the new password two times. The old password is checked against the User's expired password to verify accuracy. The User is asked to provide the new password twice to avoid mistyping, and the two *new* passwords are checked against each other to make sure they match. Assuming that the old password provided matches the expired password in the database and that the User's new password has been correctly typed, the new password is then checked for compliance with password policy.

If the password meets the User’s password policy requirements, a success message is returned to the User via the Web page, the password is changed in the database and the password expiry is set according to the predefined password expiry policy. If the password does not meet the format requirements, the User is returned an error Web page and is instructed to provide a compliant password.

Forgotten Passwords

SecureControl provides a secured 'Password Reset' Web page whose access can be limited to help desk attendants. If Users forget their passwords, they can call the help desk to be issued a new password. Using the Password Reset page, the help desk attendant can then issue a new, randomly generated, compliant password (which is unknown to the help desk Administrator) which is automatically sent to the User's email account.

If an organization doesn't want to have passwords being sent via email it is also possible to configure the Password Reset page so that the attendant can read the generated password to the User or leave the password on the User's voicemail.

CLEARTRUST SECURECONTROL ADMINISTRATION TASK SUMMARY

The following list will help System Administrators plan and set up a SecureControl security policy system:

3. **Plan Ahead**—Identify the Resources (Web sites, URIs, Applications) that you want to secure. Identify the kinds of Users that should access those Resources and design logical groupings of Users with common needs to be formed into Groups and Realms.
   - Consider how, if at all, you want to delegate Administration capabilities to others for specific Resources and Users. The Administrators to whom you delegate some or all of the administration for your ClearTrust environment will be the ones who use the Manager tool to create Applications and to identify the Resources that will comprise the Applications.
   - Define conditions for determining access rights to the Resources you want to secure.
   - If you plan to implement SmartRules, you should also define the appropriate User Properties upon which to base access rules.
4. **Set up Delegated Administration**—Define Administrative Groups and Administrative Roles and assign Users to Administrative Groups.
5. **Create Users, Groups, and Realms**—Define User Properties as needed and create Users, Groups, and Realms. Create User accounts for all Users for

whom you want to provide access. (You can also import User information. See Chapter 5, *Integrating Other Directories and ClearTrust*, for more information).

6. **Define Web Servers**—Define Web Servers, and create Server Trees if you want to delegate administration of specific Resources to select Administrative Groups. Create Applications, add Resources to Applications, and change ownership of Applications to meet your needs.
7. **Define Runtime Access Control**—Define Basic Entitlements and SmartRules
8. **Test Access Permissions**—Test the security policies you have defined. The Entitlements Manager includes a "Test" function to simulate Users requesting access to Resources.

CHAPTER 3

THE ENTITLEMENTS MANAGER WEB UI

The Entitlements Manager Web User Interface is a browser-based interface to the ClearTrust SecureControl policy management system. The ClearTrust SecureControl Manager Web interface lets you:

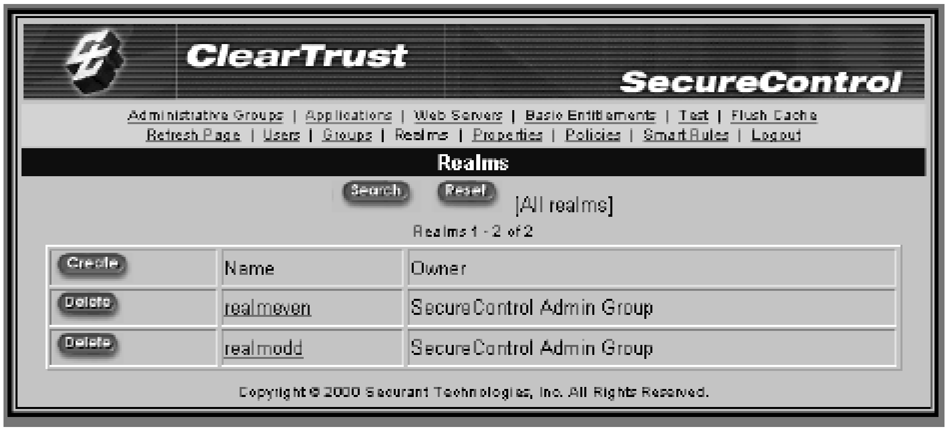
- Create and modify Users, Groups and Realms.
- Manage access to Web Servers, Applications, and other Resources.
- Designate some Users as “Administrative Users,” who can then manage access to Resources for other Users.
- Create and manage User passwords, and password policies.

This chapter provides an overview of the Web UI, as well as instructions on how to log in and step by step instructions for some of the more basic functionality. More detailed instructions on how to perform specific tasks in the Web UI are available in the on-line help. Before using the Web UI, you should familiarize yourself with the basic concepts and terminology described in Chapter 2, *The Entitlements Manager Background Concepts*.

INTERFACE OVERVIEW

MENU ITEMS

As shown in Figure 3.1, the ClearTrust SecureControl Manager has a menu at the top to access different areas of functionality, as well as function buttons and hypertext links to more specific information within each function area.


ClearTrust
SecureControl
Administrative Groups | Applications | Web Servers | Basic Entitlements | Test | Flush Cache
Refresh Page | Users | Groups | Realms | Properties | Policies | SmartRules | Logout
Realms
Search
Reset

[All realms]

Realms 1 - 2 of 2

Create	Name	Owner
Delete	realmeven	SecureControl Admin Group
Delete	realmodd	SecureControl Admin Group

Copyright © 2000 Securant Technologies, Inc. All Rights Reserved.

Figure 3.1 A ClearTrust SecureControl Web UI Window

The Web UI menu areas are as follows (following the menu list from left to right and top to bottom):

1. Administrative Groups - Define Administrative Groups and Administrative Roles; assign privileges to Administrative Roles and populate Administrative Groups with Users.
2. Applications - Define Applications and Application Functions and assign resources to Applications.
3. Web Servers - Create ClearTrust SecureControl-enabled Web Servers and server trees.
4. Basic Entitlements - Specify access privileges for Users, Groups and Realms.
5. Test - Simulate a specified User attempting to access a specified Web Server in order to test your security policies.
6. Flush Cache - Update the ClearTrust SecureControl run-time servers with new data. For example, when you change the privileges of a User you must select Flush Cache from the System menu to update the information cached on the Authorization Servers.
7. Refresh Page - Update the appearance of the page to reflect new data.
8. Users - Create and modify User accounts and information.
9. Groups - Create and modify Groups.
10. Realms - Create and modify Realms.
11. Properties - Define User Properties.
12. Policies - Define Password policies that are associated with Administrative Groups.

13. SmartRules - Define mechanisms for determining access based on the values of a User's User Properties.

14. Logout - End a session (if you want to log in as another Administrative User, you must first log out and then log back in).

For more information about these terms, see Chapter 2, *The Entitlements Manager Background Concepts*.

> ***Note:*** It is not possible to successfully navigate between Web UI screens by using your browser's Forward and Back buttons. If you need to abort a dialog and go back up a level use the **Cancel** button in the lower right corner of the window.

COMMON FEATURES

Most interaction windows in the ClearTrust SecureControl Manager Web GUI have the following common features:

- **Cancel** button - To cancel a dialog and return to the previous window, click on the Cancel button in the lower right of the dialog. (You can navigate between top-level interactions using the menu at the top of the window). It is not possible to go forward and back in an interaction by using your browsers Forward and Back buttons.
- **Create** button - To create a new entry in a shown list (Users, Administrative Groups, and so on), click on the Create button in the upper right of the list window.
- **Delete** button - To delete an item from a list of items (Users, Administrative Groups, and so on), click on the Delete button next to the name of the item in the list. Depending on context, this will either remove the item from a specific list (for example "Users in the current Group") or from the entire system (for example "Users"). You will be asked to confirm removing an item from the system.)
- Error messages - During use of the Manager Web GUI an error screen is sometimes shown. Those screens will give you the option of continuing or logging off. If you get the error screen more than once, logging off and logging back on again will often clear the error. Errors may also occur if the Entitlements Server or the Authorization Server is not available.
- Global memory of settings - In many cases, if an Object has been specified in one interaction (for example, "Create User"), and you move to another interaction (for example, "Create Basic Entitlement"), the Object will be automatically selected for that interaction as well (for example, the Basic Entitlement will be created for the newly created User, unless another User is selected).
- **Next** and **Previous** buttons - To navigate to other pages in a lengthy list, click on the Next and Previous buttons.
- Required fields - If information must be typed in to complete an interaction, that field is marked with an asterisk next to the field name.

- **Search** and **Reset -** To search for individual items or items of a specific type within a list of items, click on the Search button. The search results will also be shown as a list of items. To show the complete list again, click on Reset. See the on-line documentation for more information about searching.
- **Use -** To select an item for use from a list of items, click on the Use button next to the name of the item in the list.

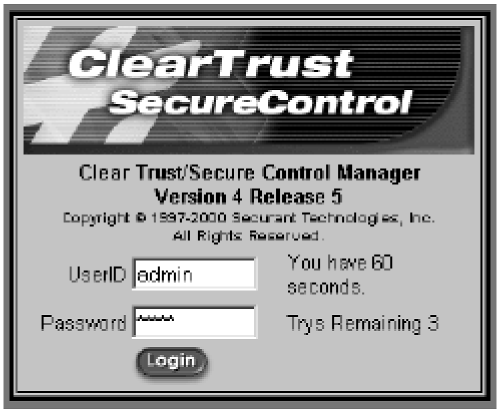
LOGGING IN TO THE CLEARTRUST SECURECONTROL MANAGER

These instructions presume that you’ve installed and configured the ClearTrust SecureControl Manager; see the *Installation and Configuration Guide* for details

To log in to the ClearTrust SecureControl Manager:

1. Access the URL of the ClearTrust SecureControl Manager from your browser as you would any other web page (by typing the URL into the address field or by choosing the page from your bookmarks).

2. In a few seconds, the **Login** dialog displays:



Clear Trust/Secure Control Manager
Version 4 Release 5
Copyright © 1997-2000 Securant Technologies, Inc.
All Rights Reserved.

UserID admin

You have 60 seconds.

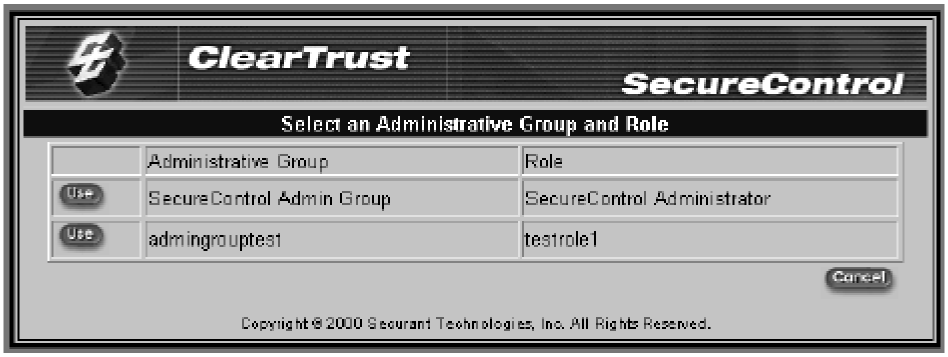
Password *****

Trys Remaining 3

3. Enter your User ID and Password and click the **Login** button to continue.

- If this is the first time you are launching the Manager application, log in using the default administrator account and password that were specified during the install process.

- If you are an Administrator with Administrative Roles in more than one Administrative Group, a dialog displays prompting you for the Administrative Group for this login session:



Select an Administrative Group and Role

	Administrative Group	Role
Use	SecureControl Admin Group	SecureControl Administrator
Use	admingrouptest	testrole1

- If you have not defined any Administrative Groups, you will automatically be logged in as a member of the default ClearTrust SecureControl Administrative Group. In this case, the Administration Role Choice dialog does not appear; the ClearTrust SecureControl Manager window opens directly from the **Login** dialog.

4. If you have Administrative Roles in more than one Administrative Group, select the Administrative Group under which you want to log in. You may have Administrative Roles in more than one Administrative Group, but you can only log in in one group at a time. Any object you create will belong to your current Administrative Group, and passwords for Users you create will have to conform to the password policy for that Administrative Group.

In a few seconds, the ClearTrust SecureControl Manager Web graphical user interface displays.

USING THE WEB GUI: SOME EXAMPLES

The following examples provide a very basic introduction to the following functions in the ClearTrust SecureControl system:

- Creating a User
- Creating a Web Server
- Creating and Adding Resources to an Application
- Creating and Testing Basic Entitlements

While it is possible to protect network resources using only the functions described in this section, administrators of larger networks will benefit from more complex functionality, such as Delegated Administration, grouped Users and Server Trees, that are not described in this section. See Chapter 2, *The Entitlements Manager Background Concepts* and the on-line documentation for more information about these features.

CREATING A USER

A "User" is a unique User ID (UID) in the ClearTrust SecureControl system. While Users are usually individuals, you can also create User accounts for specific job functions within an organization.

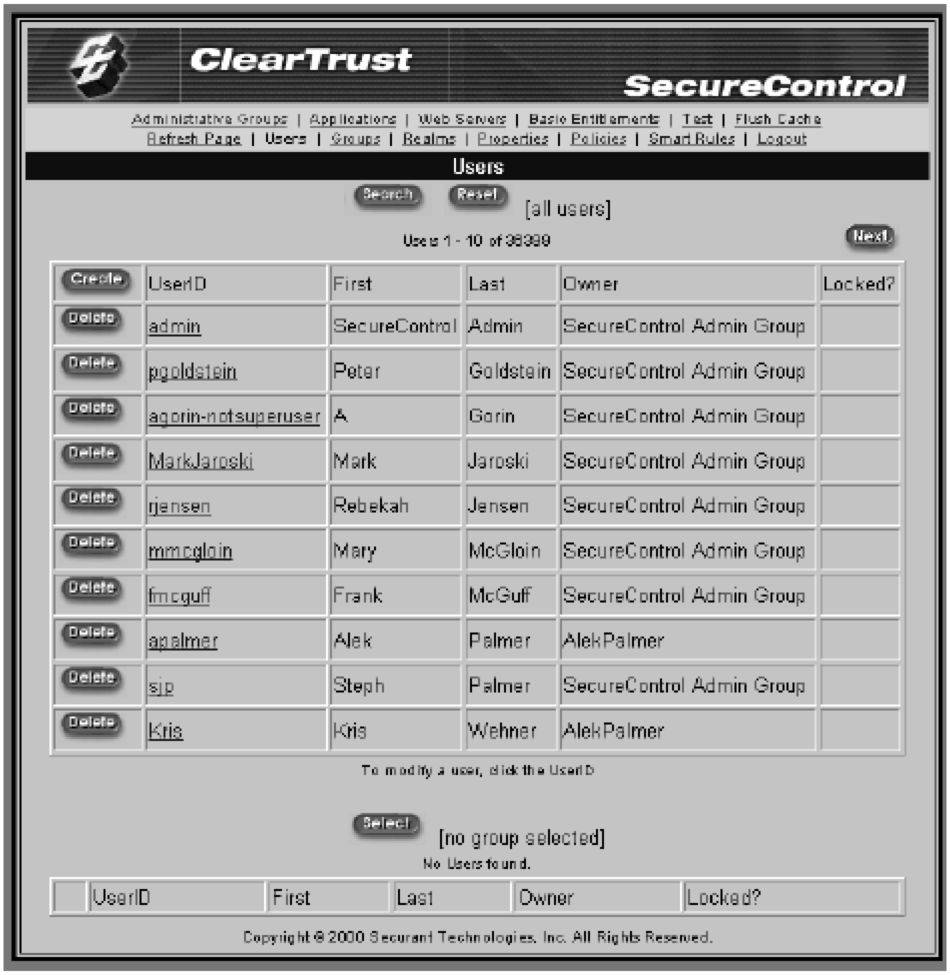
While it is possible to administer a system using only User accounts, ClearTrust allows you to group Users into Groups and Realms for more convenient administration. See Chapter 2, *The Entitlements Manager Background Concepts* and the on-line documentation for more information.

If you are going to control access via SmartRules, you should create the User Properties on which the SmartRules will be based before creating any Users. See Chapter 2, *The Entitlements Manager Background Concepts* and the on-line documentation for more information.

> ***Note:*** Because User IDs may be created for job functions as well as for people, it is possible for a person to have access via more than one User account ("HR" and "Charlie," for example). Keep in mind that Basic Entitlements, SmartRules and User Properties are associated with a User ID, not with an individual.

To create a User Account:

1. In the ClearTrust SecureControl Manager Web GUI window, click on **Users** in the top menu to display the Users interface.


ClearTrust
SecureControl
Administrative Groups | Applications | Web Servers | Basic Entitlements | Test | Flush Cache
Refresh Page | Users | Groups | Realms | Properties | Policies | Smart Rules | Logout
Users
Search
Reset
Next
Create
Delete
Select

[all users]

Users 1 - 10 of 38399

	UserID	First	Last	Owner	Locked?
Delete	admin	SecureControl	Admin	SecureControl Admin Group	
Delete	pgoldstein	Peter	Goldstein	SecureControl Admin Group	
Delete	agorin-notsuperuser	A	Gorin	SecureControl Admin Group	
Delete	MarkJaroski	Mark	Jaroski	SecureControl Admin Group	
Delete	rjensen	Rebekah	Jensen	SecureControl Admin Group	
Delete	mmcgloin	Mary	McGloin	SecureControl Admin Group	
Delete	fmcguff	Frank	McGuff	SecureControl Admin Group	
Delete	apalmer	Alek	Palmer	AlekPalmer	
Delete	sjp	Steph	Palmer	SecureControl Admin Group	
Delete	Kris	Kris	Wehner	AlekPalmer	

To modify a user, click the UserID

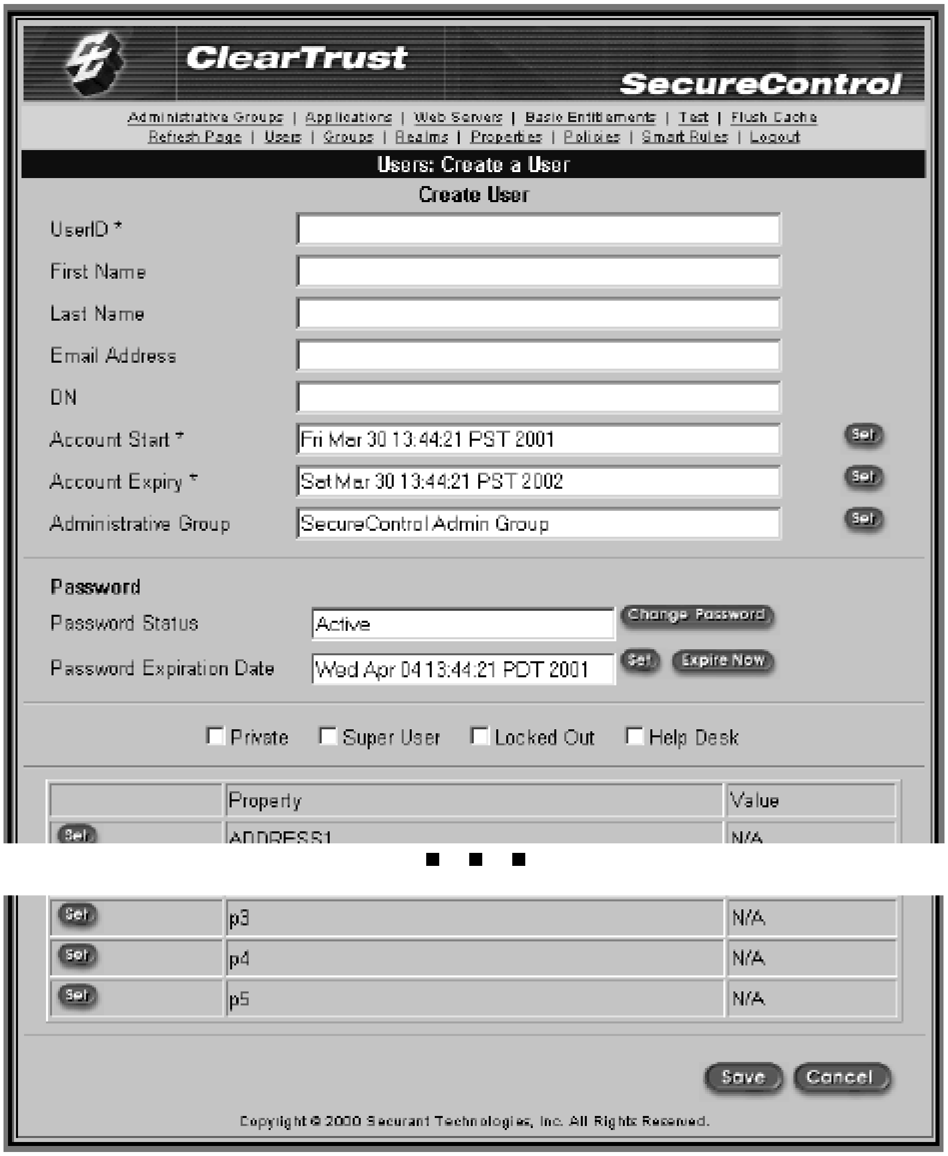
[no group selected]

No Users found.

	UserID	First	Last	Owner	Locked?

Copyright © 2000 Securant Technologies, Inc. All Rights Reserved.

2. Click on the **Create** button at upper left to display the **Create User** dialog box:


ClearTrust
SecureControl
Administrative Groups | Applications | Web Servers | Basic Entitlements | Test | Flush Cache
Refresh Page | Users | Groups | Realms | Properties | Policies | Smart Rules | Logout
Set
Change Password
Expire Now
Save
Cancel

Users: Create a User

Create User

UserID *	
First Name	
Last Name	
Email Address	
DN	
Account Start *	Fri Mar 30 13:44:21 PST 2001
Account Expiry *	Sat Mar 30 13:44:21 PST 2002
Administrative Group	SecureControl Admin Group

Password

Password Status	Active
Password Expiration Date	Wed Apr 04 13:44:21 PDT 2001

□ Private □ Super User □ Locked Out □ Help Desk

	Property	Value
Set	ADDRESS1	N/A

■ ■ ■

	Property	Value
Set	p3	N/A
Set	p4	N/A
Set	p5	N/A

Copyright © 2000 Securant Technologies, Inc. All Rights Reserved.

3. In the **Create User** dialog box, enter a name for the User account (the “UserID”) following the User account naming guidelines or other appropriate convention for your environment (for example, the person’s first initial plus the first seven characters of their last name).

4. Enter values for the other User information as needed for your organization. You can also change any of the default settings. For more specific information about the rest of the information in the **Create User** dialog box, as described Table 3.1.

5. Click **Save** to save the new settings and return to the **Users** interaction, or click **Cancel** to return without changing anything.

Once you have created a User, you can modify the User’s information by clicking on the name of the User, or delete the User by clicking on the **Delete** button next to the User’s name, in the **Users** interaction.

Table 3.1 Fields, Checkboxes and Buttons in the Create User dialog

Field, Checkbox and Button names	Description	Usage note
UserID	Login ID for the User	Required
First Name	User’s first name.	Optional
Last Name	User’s last name	Optional
Email Address	Email address for the User	Optional
DN	Distinguished name (X.500 schema)	Optional
Account Start	Date and time the account becomes active	Default is host machine time when User is saved.
Account Expiry	Date and time the account will expire	Default is 1 year after the Account Start date.
Administrative Group	Administrative Group that owns the User account	Default is the Administrative Group of the Administrator that created the User.
Password status	Indicates whether the password is *active* or has *expired*.	The default password, `ch4nge_me,` is automatically set when you create a new User through the SecureControl Entitlements Manager. If this password is expired (via **Expire Now**) when the User is created, the User will be prompted to choose a new password the first time they log in.
Change password	Click to generate a **Change Password** dialog.	
Password expiration date	When the current password will expire. Click **Set** to set a new expiration date, or **Expire Now** to override the listed date In the **Modify User** dialog, click **Revert** to revert to the listed date after **Expire Now** has been specified.	The default password lifetime is set in the Password Policy associated with the Administrative Group that created the User.
Private	Identifies the User account as private; only the owning Administrative Group will be able to view this User.	Default is public.

Table 3.1 Fields, Checkboxes and Buttons in the Create User dialog

Field, Checkbox and Button names	Description	Usage note
Super User	Super Users can perform any action on any User, Group, Realm, or Application. A User designated as a Super User must be an Administrator.	This checkbox is only enabled if the person creating the account is logged on as a Super User. Assign with caution.
Locked Out	Immediately disables any permissions granted to the User.	Only Super Users can enable this feature.
Super Help Desk	Enables help desk personnel to change or reset passwords across all Administrative Groups	A User identified as Super Help Desk must also be an Administrator.
User Properties	Items of information about each User that have been defined by Administrators instead of being pre-configured by SecureControl.	If User Properties have been created, they will be listed with a **Set** button at the right of the User Property name. Click **Set** to change the User Property for the current User.

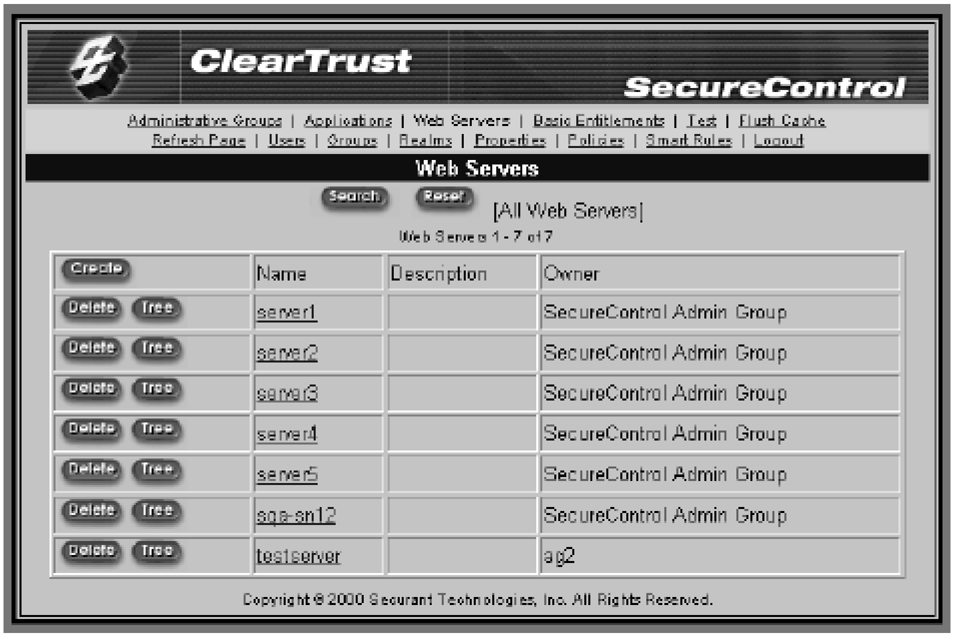
CREATING A WEB SERVER

These instructions presume that you've already installed ClearTrust SecureControl Server and that you have a ClearTrust protected web server—one with the ClearTrust Web Server Plug-in installed and configured—running on your network. (See the *Installation Guide* for additional information.).

While it is possible to administer a network using only web servers to define protected areas, the ClearTrust SecureControl system supports more granular definitions using *Server Trees*. See Chapter 2, *The Entitlements Manager Background Concepts* and the on-line documentation for more information.

To create a Web Server entry:

1. If you are not already in the **Web Servers** interaction, click on **Web Servers** in the ClearTrust SecureControl Web GUI top menu. The **Web Servers** interaction will be displayed.


ClearTrust
SecureControl
Administrative Groups | Applications | Web Servers | Basic Entitlements | Test | Flush Cache
Refresh Page | Users | Groups | Realms | Properties | Policies | Smart Rules | Logout
Search
Reset

Web Servers

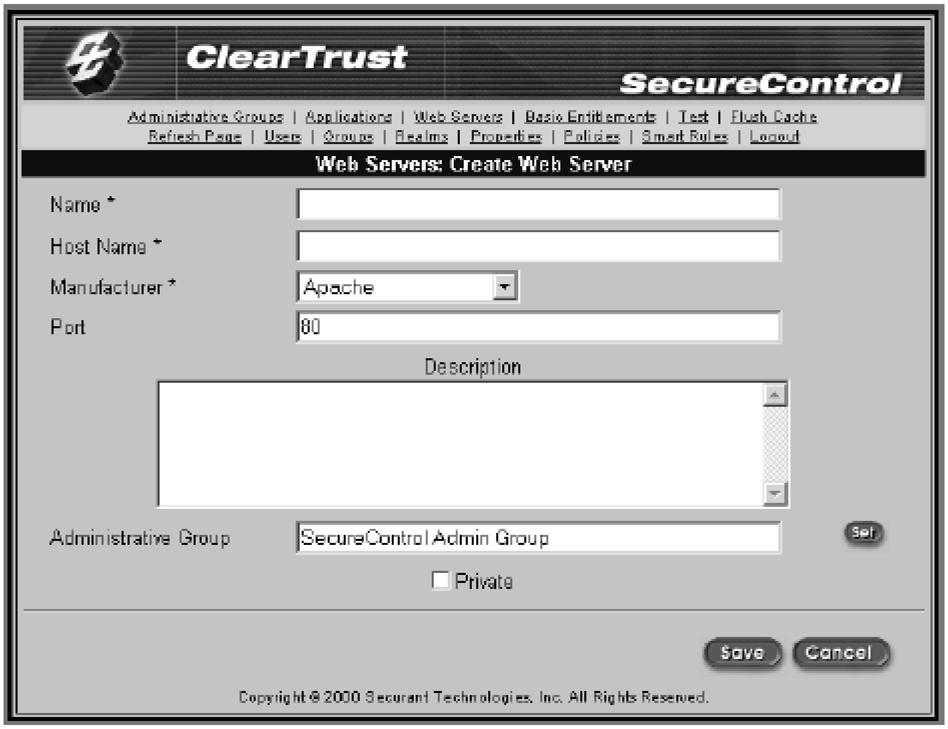
[All Web Servers]

Web Servers 1 - 7 of 7

Create	Name	Description	Owner
Delete Tree	server1		SecureControl Admin Group
Delete Tree	server2		SecureControl Admin Group
Delete Tree	server3		SecureControl Admin Group
Delete Tree	server4		SecureControl Admin Group
Delete Tree	server5		SecureControl Admin Group
Delete Tree	sqa-sn12		SecureControl Admin Group
Delete Tree	testserver		ag2

Copyright © 2000 Securant Technologies, Inc. All Rights Reserved.

2. Click the **Create** button to open the **Create Web Server** dialog:


ClearTrust
SecureControl
Administrative Groups | Applications | Web Servers | Basic Entitlements | Test | Flush Cache
Refresh Page | Users | Groups | Realms | Properties | Policies | Smart Rules | Logout
Set
Save
Cancel

Web Servers: Create Web Server

Name *

Host Name *

Manufacturer * Apache

Port 80

Description

Administrative Group SecureControl Admin Group

□ Private

Copyright © 2000 Securant Technologies, Inc. All Rights Reserved.

3. Specify the name, hostname, port number, Administrative Group (owner), manufacturer, and description of the web server. The manufacturer and description information is for your own information; the name, hostname, port number, and owner are significant pieces of information, as described in the following table:

Table 3.2 Web Server Attributes

Entry	Description	Usage Notes
Name	Name by which the Web Server is known to the ClearTrust SecureControl system	The name must be unique in the context of your ClearTrust environment. It must match the Web Server name parameter in the Web Server Plug-in's `Default.conf` file (`securecontrol.plugin.web_server_name`). The default name in that file is "WebServer" - if you enter something other than that here, be sure you change the information in the `Default.conf` file for the Plug-in to match.
Hostname	Must match the actual fully-qualified name of the Web Server	For example, *hostname.domain.com*, or the IP address
Port number	Must match the port address on which your web server advertises its http services.	The default is typically port 80, but if you've configured your web server with a different port number, enter it here.
Administrative Group	The Administrative Group (within ClearTrust SecureControl) that will own this Web Server.	By default, the Administrative Group that your current login account is an Administrator of will display. If you're logged on as a Super User, you can transfer ownership to another group if necessary.

4. To mark the web server as private, select the **Private** checkbox. A private web server can be seen only by an Administrator in the same Administrative Group as the Administrator who created the web server. Web servers are created as public by default.

5. If you're a Super User and you want to transfer ownership of the web server to an Administrative Group other than the one displayed, click the **Set** button (next to the Administrative Group field) to display the **Select Administrative Group** interaction. Once in the **Select Administrative Group** interaction, click on the **Use** button next to an Administrative Group name to select an Administrative Group from the list and return to the **Web Server** interaction, or click **Cancel** to return without making any changes.

6. Click **Save** to save the information about the web server. The server is now listed in the **Web Servers** interaction.

Once you've setup a web server in the ClearTrust SecureControl Manager, you can later return to the **Web Servers** interaction and change the information about the web server by clicking on its name in the **Web Servers** interaction to display the **Modify Web Server** dialog; you can also delete the web server entirely by clicking on **Delete**.

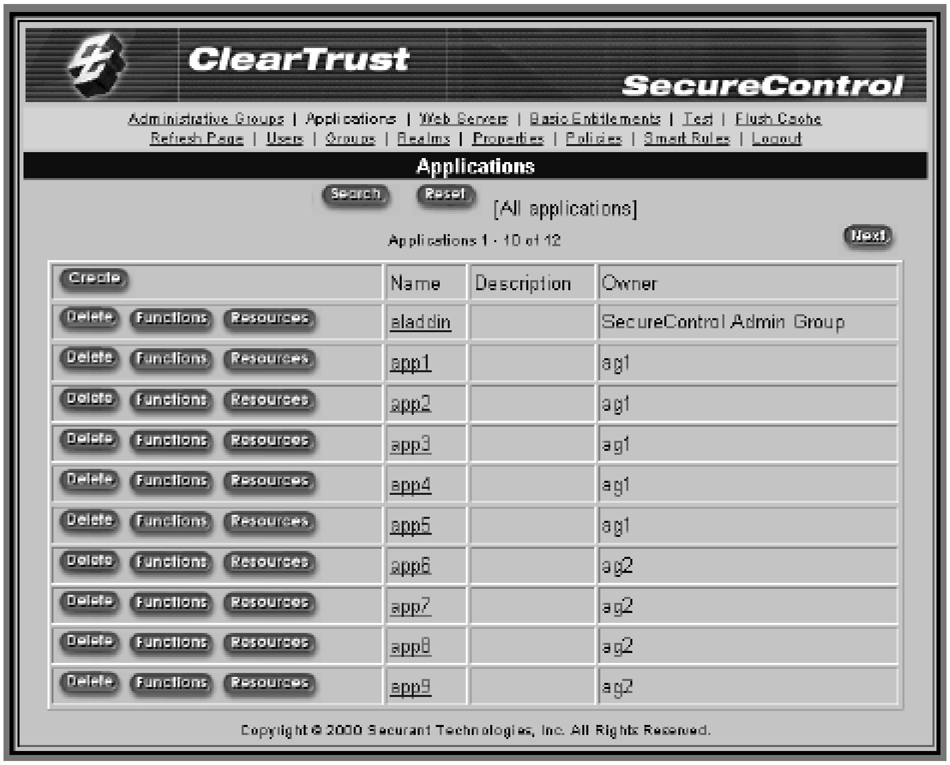
CREATING AND ADDING RESOURCES TO AN APPLICATION

Resources in the ClearTrust SecureControl system are grouped into Applications. To protect Resources, Users are given access or denied access to these Applications.

It is also possible to have more granular levels of access control using Application Functions. See Chapter 2, *The Entitlements Manager Background Concepts* and the on-line documentation for more information.

To create a new Application:

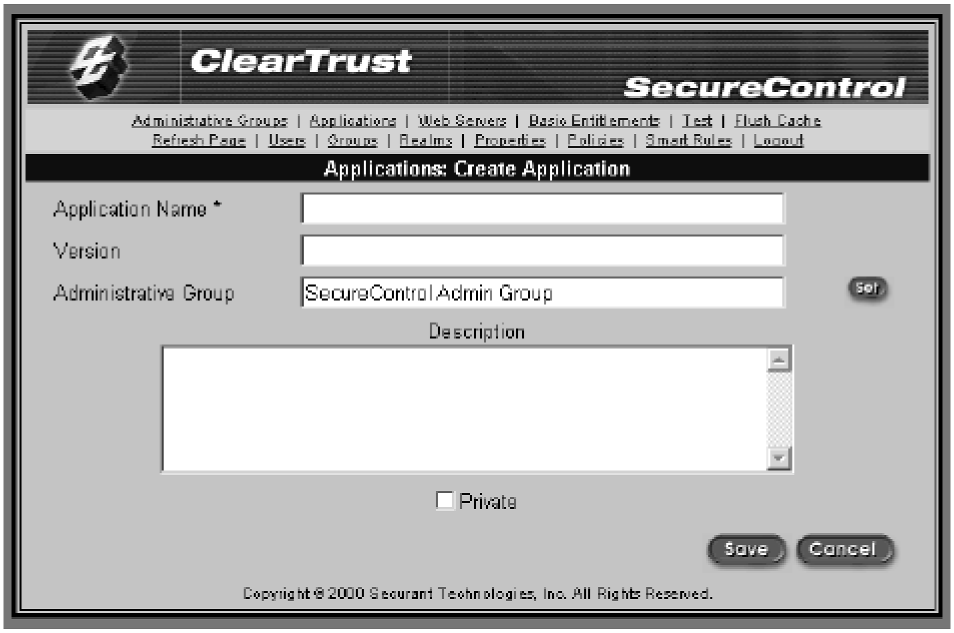
1. If you are not already in the **Applications** interaction, click on **Applications** in the ClearTrust SecureControl Manager Web GUI top menu to open the **Applications** interaction:


ClearTrust
SecureControl
Administrative Groups | Applications | Web Servers | Basic Entitlements | Test | Flush Cache
Refresh Page | Users | Groups | Realms | Properties | Policies | Smart Rules | Logout
Applications
Search
Reset
[All applications]
Applications 1 - 10 of 12
Next

Create	Name	Description	Owner
Delete Functions Resources	aladdin		SecureControl Admin Group
Delete Functions Resources	app1		ag1
Delete Functions Resources	app2		ag1
Delete Functions Resources	app3		ag1
Delete Functions Resources	app4		ag1
Delete Functions Resources	app5		ag1
Delete Functions Resources	app6		ag2
Delete Functions Resources	app7		ag2
Delete Functions Resources	app8		ag2
Delete Functions Resources	app9		ag2

Copyright © 2000 Securant Technologies, Inc. All Rights Reserved.

2. Click the **Create** button to open the **Create an Application** dialog box:


ClearTrust
SecureControl
Administrative Groups | Applications | Web Servers | Basic Entitlements | Test | Flush Cache
Refresh Page | Users | Groups | Realms | Properties | Policies | Smart Rules | Logout
Applications: Create Application
Application Name *
Version
Set
Description
□ Private
Save
Cancel
Copyright © 2000 Securant Technologies, Inc. All Rights Reserved.

Administrative Group: SecureControl Admin Group

3. Enter a meaningful name for the Application in the **Application Name** field. The Application name will be associated with a particular Web Server.

4. Enter a description for the Application, and a version number if appropriate. You can use the **Version** field to enter any additional information that will help describe the application.

5. If you're a Super User and you want to transfer ownership of the Application to an Administrative Group other than the one displayed, you can click the **Set** button (next to the **Administrative Group** field) to display the **Select an Administrative Group** dialog box. Select the name of the Administrative Group from the list by clicking on the **Use** button next to its name (or click on **Cancel** to return to the **Create an Application** dialog box without making any changes).

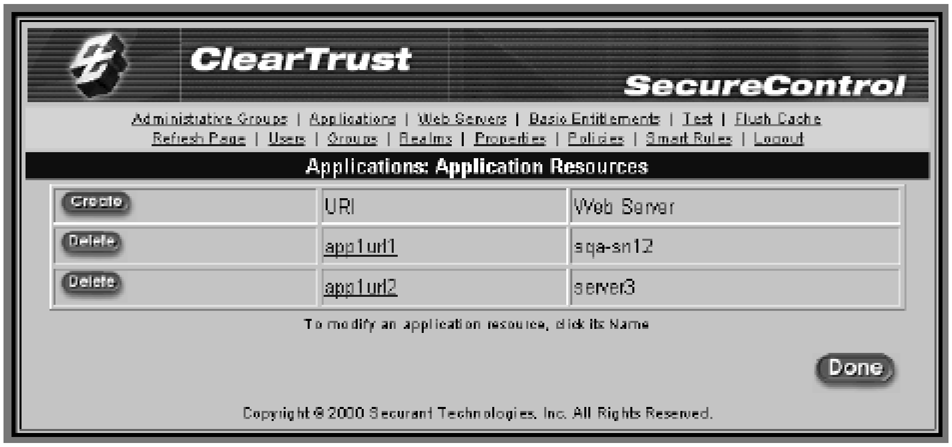
6. If you want to make the Application private, select the **Private** checkbox. A private Application can be seen only by an Administrator in the same Administrative Group as the Administrator that created the Application. Applications are created as public by default.

7. Click the **Save** button to save the Application and return to the Applications interaction. The application is now listed. You can now add resources and functions to the Application as described in *To add resources to an Application:* on page *3-14*. (Or click **Cancel** to return without creating the Application).

To add resources to an Application:

1. If you are not already in the **Application** interaction, click on **Applications** in the ClearTrust SecureControl Manager Web GUI top menu to open the **Applications** interaction.

2. Click on the **Resources** button next to the name of the **Application** to which you wish to add the Resource.The **Application Resources** interaction will be displayed:


ClearTrust
SecureControl
Administrative Groups | Applications | Web Servers | Basic Entitlements | Test | Flush Cache
Refresh Page | Users | Groups | Realms | Properties | Policies | Smart Rules | Logout
Done

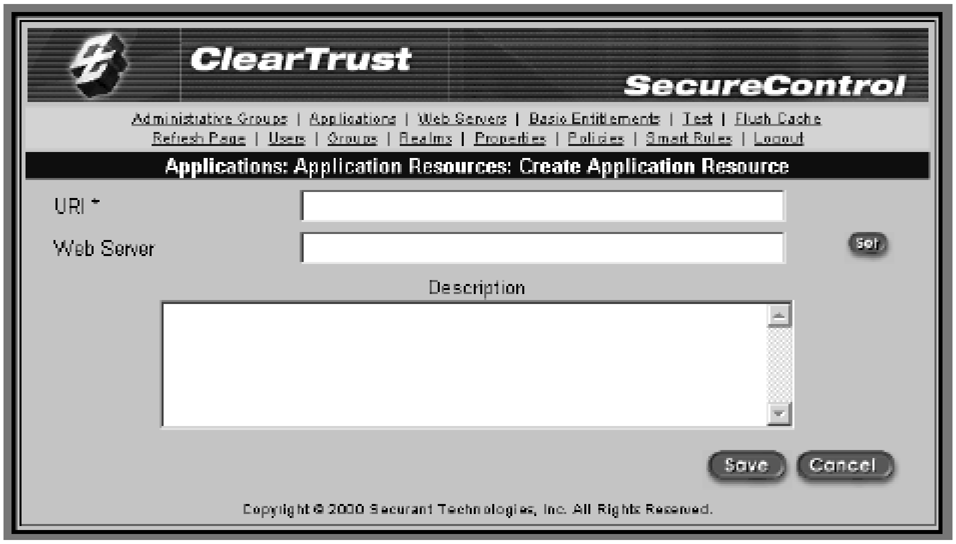
Applications: Application Resources

Create	URI	Web Server
Delete	app1url1	sqa-sn12
Delete	app1url2	server3

To modify an application resource, click its Name

Copyright © 2000 Securant Technologies, Inc. All Rights Reserved.

3. Click on the **Create** button. The **Create Application Resource** interaction will be displayed.


ClearTrust
SecureControl
Administrative Groups | Applications | Web Servers | Basic Entitlements | Test | Flush Cache
Refresh Page | Users | Groups | Realms | Properties | Policies | Smart Rules | Logout
Set
Save
Cancel

Applications: Application Resources: Create Application Resource

URI *

Web Server

Description

Copyright © 2000 Securant Technologies, Inc. All Rights Reserved.

4. Enter the name of the URI in the **URI** field. You can enter the complete URI, or you can enter a wildcard to secure everything under a directory path.

> ***Important:*** When specifying directories on a web server to be protected, exclude the `/securant` directory. Using a “`/*`” to protect your entire web server will block from the securant system from accessing the CGIs and forms needed to perform operations such as password changes. The best solution to protect all the directories on your web server is to move all the directories (except `/securant`) into a sub-directory and then protect that sub-directory.

5. Click **Set** next to the **Web Server** field to specify the web server with which the application resource is associated.

6. Enter a description of the Application Resource as needed.

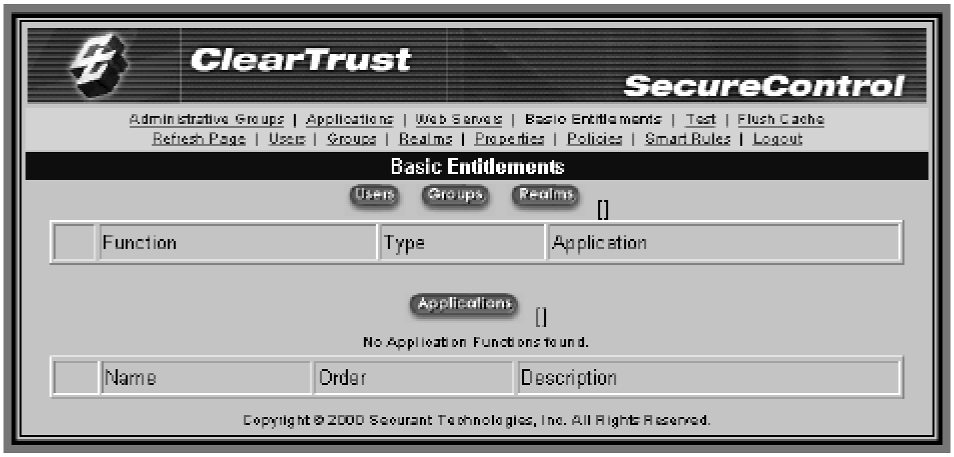
7. Click the **Save** button to save the resource specified as part of the Application. This resource will now be listed as part of the resources for that Application. (Or click **Cancel** to return to the **Applications Resources** interaction without changing anything).
8. Once back in the **Application Resources** interaction, click **Done** to return to the Application interaction.

CREATING AND TESTING BASIC ENTITLEMENTS

There are two ways to protect Resources in the ClearTrust SecureControl system. The first, simpler, way is via Basic Entitlements, which are based on the individual User ID or the User's Group or Realm. The second way is via SmartRules. This section describes Basic Entitlements - for information about SmartRules and more detailed information about Basic Entitlements see Chapter 2, *The Entitlements Manager Background Concepts* and the on-line documentation.

To create, modify or delete a Basic Entitlement:

1. If you are not already in the **Basic Entitlements** interaction, click on **Basic Entitlements** in the ClearTrust SecureControl Manager Web GUI top menu to open the **Basic Entitlements** interaction:


ClearTrust
SecureControl
Administrative Groups | Applications | Web Servers | Basic Entitlements | Test | Flush Cache
Refresh Page | Users | Groups | Realms | Properties | Policies | Smart Rules | Logout
Basic Entitlements
Users
Groups
Realms
[]
Applications
[]

	Function	Type	Application

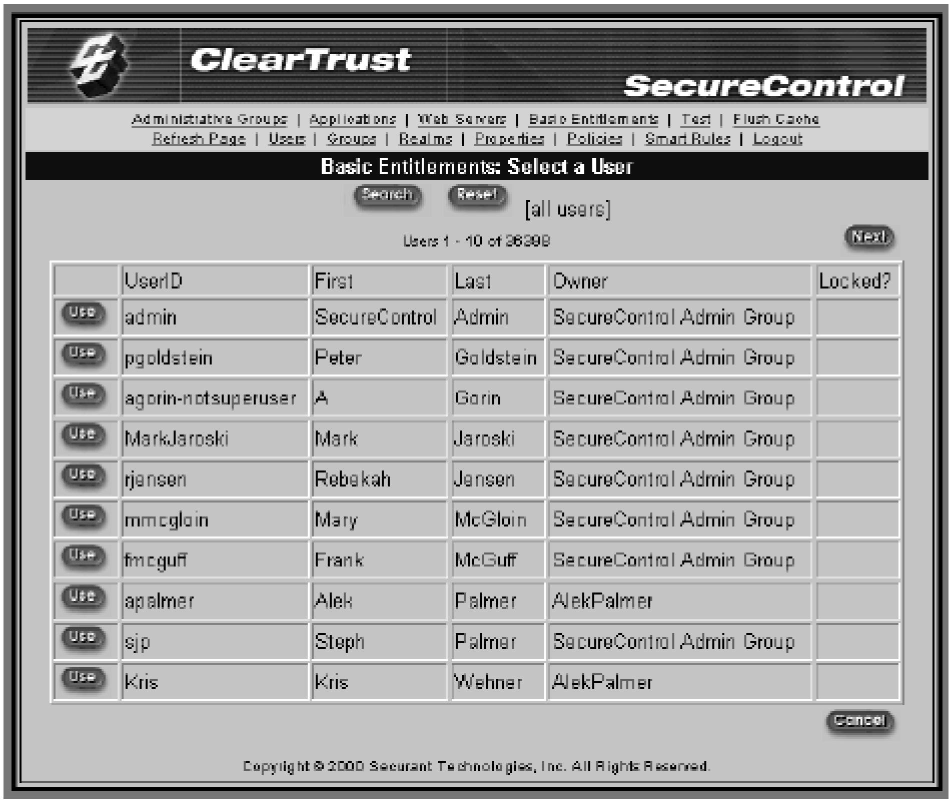
No Application Functions found.

	Name	Order	Description

Copyright © 2000 Securant Technologies, Inc. All Rights Reserved.

2. Click on the **Users** button to select the User for whom you want to create a Basic Entitlement. The **Select A User** dialog will be displayed. (If you have just created a User that User will already be selected - Click on **Users** to select another User, or go on to Step 4).

- It is also possible to create Basic Entitlements for Groups and Realms - See Chapter 2, *The Entitlements Manager Background Concepts* and the on-line documentation for more information.


ClearTrust
SecureControl
Administrative Groups | Applications | Web Servers | Basic Entitlements | Test | Flush Cache
Refresh Page | Users | Groups | Realms | Properties | Policies | Smart Rules | Logout
Search
Reset
Next
Cancel

Basic Entitlements: Select a User

[all users]

Users 1 - 10 of 36398

	UserID	First	Last	Owner	Locked?
Use	admin	SecureControl	Admin	SecureControl Admin Group	
Use	pgoldstein	Peter	Goldstein	SecureControl Admin Group	
Use	agorin-notsuperuser	A	Gorin	SecureControl Admin Group	
Use	MarkJaroski	Mark	Jaroski	SecureControl Admin Group	
Use	rjensen	Rebekah	Jensen	SecureControl Admin Group	
Use	mmcgloin	Mary	McGloin	SecureControl Admin Group	
Use	fmcguff	Frank	McGuff	SecureControl Admin Group	
Use	apalmer	Alek	Palmer	AlekPalmer	
Use	sjp	Steph	Palmer	SecureControl Admin Group	
Use	Kris	Kris	Wehner	AlekPalmer	

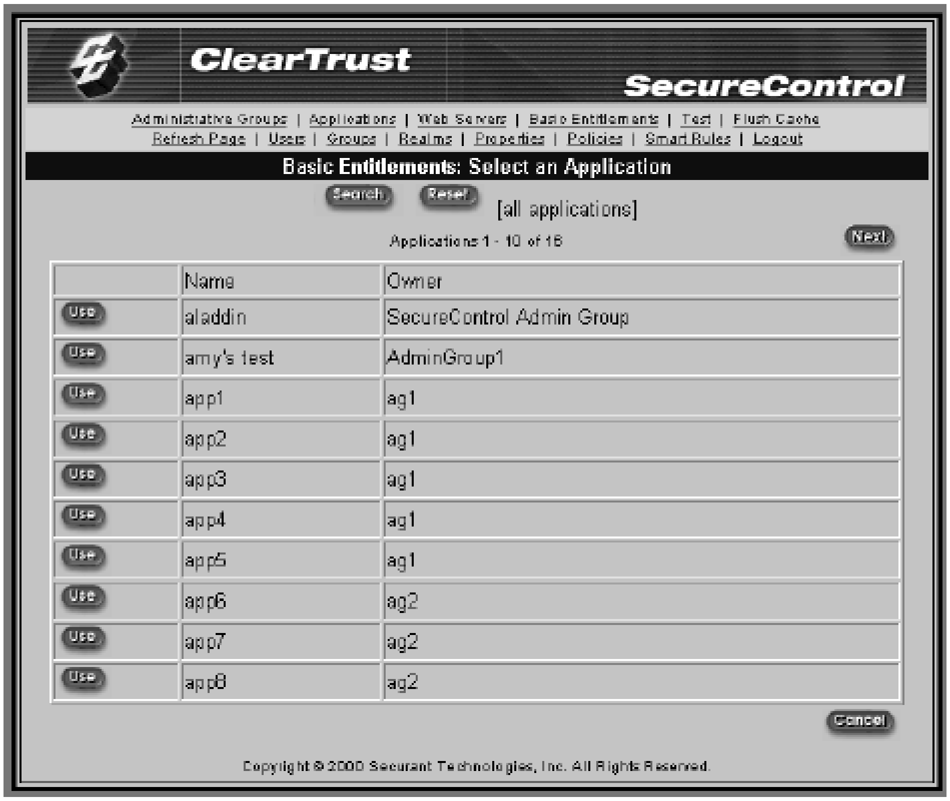
Copyright © 2000 Securant Technologies, Inc. All Rights Reserved.

3. Click on the **Use** button next to the name of the **User** for whom you wish to add Entitlements (or click on **Cancel** to return to the **Basic Entitlements** interaction without making a selection).

- If the list of Users is long and you don't see the name displayed, click on the **Next** button to display more names, or click on the **Search** button to generate a **Search** dialog box. For more information about Searching, see *Searching for Users, Objects and Resources* in the on-line documentation.

Once you have selected a User, the **Basic Entitlements** interaction will be displayed again with the selected User specified. If the User already has Basic Entitlements defined, these will be listed.

4. Click on the **Applications** button to specify an Application to protect or allow. The **Select an Application** interaction will be displayed.


ClearTrust
SecureControl
Administrative Groups | Applications | Web Servers | Basic Entitlements | Test | Flush Cache
Refresh Page | Users | Groups | Realms | Properties | Policies | Smart Rules | Logout
Search
Reset
Next
Cancel

Basic Entitlements: Select an Application

[all applications]

Applications 1 - 10 of 16

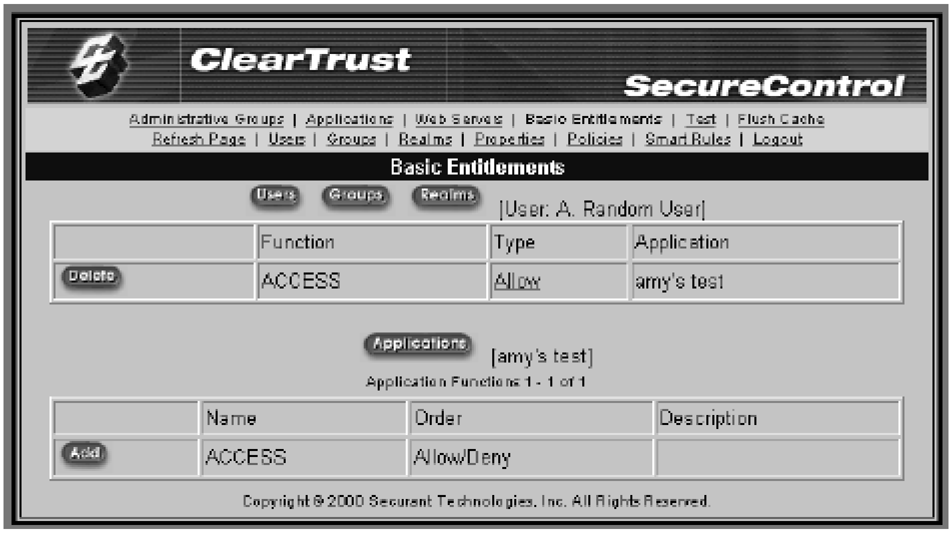
	Name	Owner
Use	aladdin	SecureControl Admin Group
Use	amy's test	AdminGroup1
Use	app1	ag1
Use	app2	ag1
Use	app3	ag1
Use	app4	ag1
Use	app5	ag1
Use	app6	ag2
Use	app7	ag2
Use	app8	ag2

Copyright © 2000 Securant Technologies, Inc. All Rights Reserved.

5. To select an Application from the list, click on the **Use** button next to the Application name.

- If the list of Applications is long and you don't see the name displayed, click on the **Next** button to display more names, or click on the **Search** button to generate a **Search** dialog box. The results of the search will be displayed in a **Select an Application** interaction. To return to the full list of Applications, click **Reset**.

6. Once an Application is selected, the **Basic Entitlements** interaction will now be displayed again, and the Application Functions which are part of the selected Application will be listed. The default Application Function, "ACCESS," allows or denies access to all of the URIs in the Application. (It is possible to create more complex Application Functions using the Runtime API - see the *Developer's Guide* for more information.)


ClearTrust
SecureControl
Administrative Groups | Applications | Web Servers | Basic Entitlements | Test | Flush Cache
Refresh Page | Users | Groups | Realms | Properties | Policies | Smart Rules | Logout
Basic Entitlements
Users
Groups
Realms
Delete
Applications
Add

[User: A. Random User]

	Function	Type	Application
Delete	ACCESS	Allow	amy's test

[amy's test]

Application Functions 1 - 1 of 1

	Name	Order	Description
Add	ACCESS	Allow/Deny	

Copyright © 2000 Securant Technologies, Inc. All Rights Reserved.

Once a User and Application are selected and Application Functions are displayed, there are three ways in which the Basic Entitlements for the User can be modified

- To **add** a Basic Entitlement for the User click on the **Add** button next to the name of the Application Function you wish to add. The Application Function will now appear in the list of Basic Entitlements for the User.
  - If the Application Function is ACCESS, adding it to the User's list of Basic Entitlements will allow or deny the User access to all the URIs in the Application, depending on whether Allow or Deny is shown in the **Type** field for the Application Function.
- To **modify** a Basic Entitlement that already appears in (or has just been added to) the list of Basic Entitlements, click on **Allow** or **Deny** in the **Type** field of the Application list. This link is a toggle - clicking on **Allow** will change it to **Deny**, clicking on **Deny** will change it to **Allow**.
  - The **Type** field in the list of Application Functions for the User specifies whether or not the Application Function will allow or deny access. The **Order** field in the list of Application Functions for the Application is used to process SmartRules, and does not effect Basic Entitlements.
- To **delete** a Basic Entitlement that already appears in the list of Basic Entitlements for that User, click on the **Delete** button next to the name of the Application Function. A confirmation dialog will be shown. Click **OK**. The Basic Entitlement will be removed for that User (the Application Function will not be deleted from the system).

To test a Basic Entitlement:

1. If you are not already in the Test interaction, click on **Test** in the Entitlements Manager Web GUI top menu to open the Test interaction.
2. Click **Set** next to the **User ID** field to open the **Select a User** dialog. Once the dialog is displayed, click **Use** next to the name of the User for whom you wish to test access.

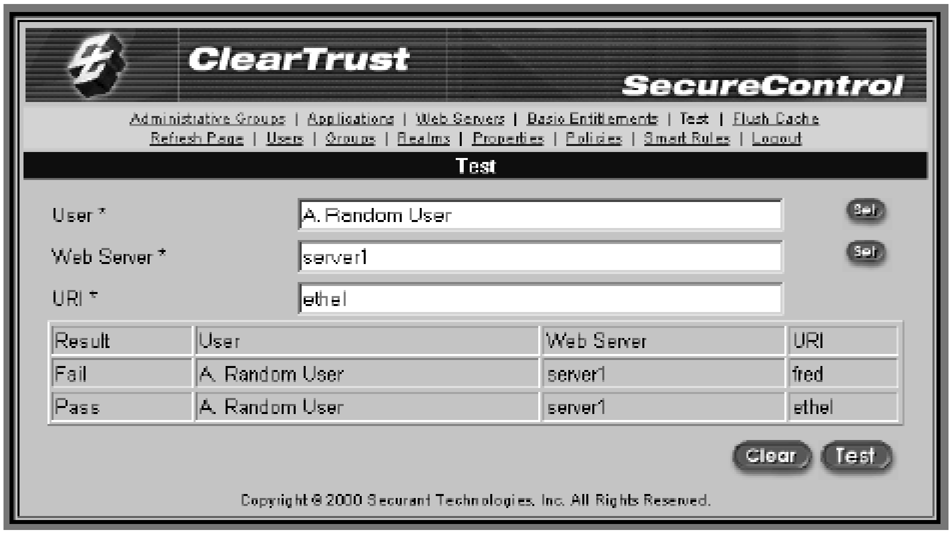
- If the list of Users is long and you don't see the name displayed, click on the **Next** button to display more names, or click on the **Search** button to generate a **Search** dialog box. The results of the search will be displayed in a **Select a User** interaction. To return to the full list of Users, click **Reset**. See the on-line documentation for more information about searching for Users.

3. Click **Set** next to the **Web Server** field to open the **Select a Web Server** dialog. Once the dialog is displayed, click **Use** next to the name of the web server for which you wish to test access.

- If the list of web servers is long and you don't see the name displayed, click on the **Next** button to display more names, or click on the **Search** button to generate a **Search** dialog box. The results of the search will be displayed in a **Select a Web Server** interaction. To return to the full list of Web Servers, click **Reset**. See the on-line documentation for more information about searching for web servers.

4. Enter the URI for which you wish to test access.

5. Click on **Test**. Test Results will appear at the bottom of the screen. (If the list of results gets long, click on **Clear** to clear the list of results).


ClearTrust
SecureControl
Administrative Groups | Applications | Web Servers | Basic Entitlements | Test | Flush Cache
Refresh Page | Users | Groups | Realms | Properties | Policies | Smart Rules | Logout
Set
Set
Clear
Test

Test

User * A. Random User

Web Server * server1

URI * ethel

Result	User	Web Server	URI
Fail	A. Random User	server1	fred
Pass	A. Random User	server1	ethel

Copyright © 2000 Securant Technologies, Inc. All Rights Reserved.

> ***Note:*** It is possible to test access for URIs which are not part of any Application. In this case, the results will depend on whether the system is configured in "Active" (allow access unless explicitly denied) or "Passive" (deny access unless explicitly allowed) mode. See Chapter 2, *The Entitlements Manager Background Concepts* for more information.

CHAPTER

4

THE ENTITLEMENTS MANAGER JAVA CLIENT UI

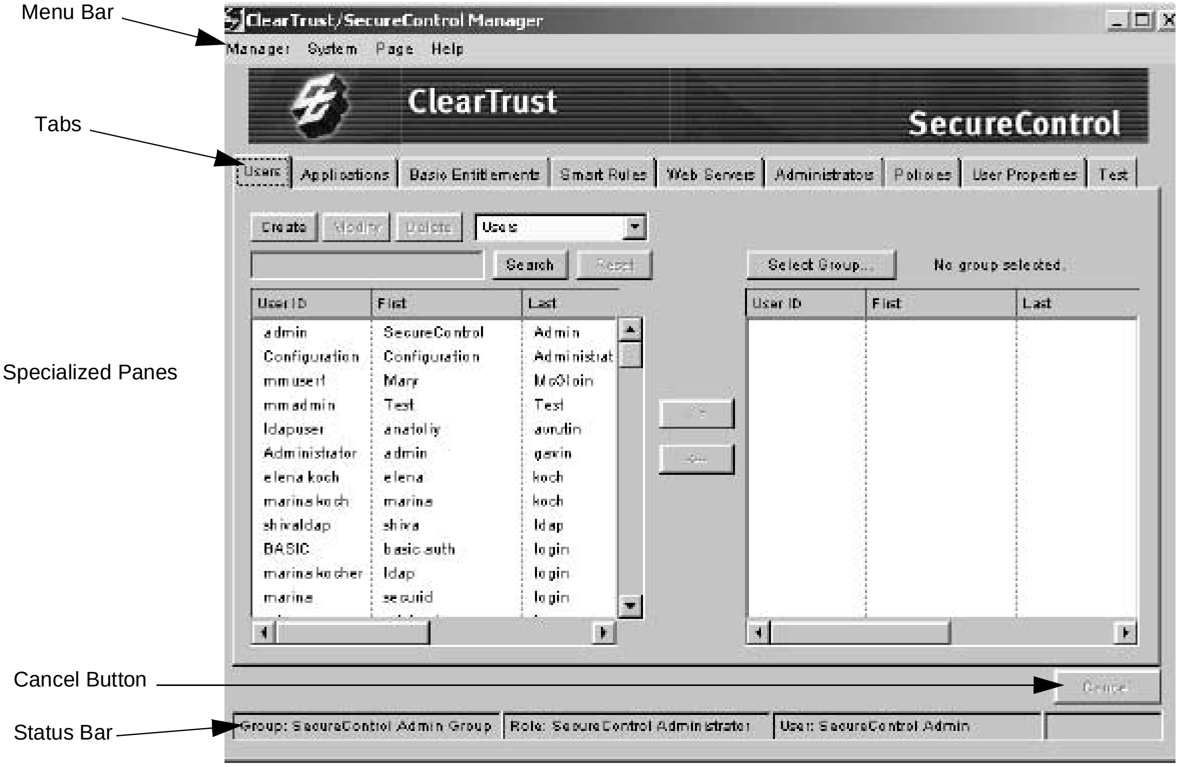
The ClearTrust SecureControl Entitlements Manager Java Client UI is a stand-alone tool for working with the ClearTrust SecureControl entitlements management infrastructure.

An overview of the functions provided by the Entitlements Manager is in Chapter 2, *The Entitlements Manager Background Concepts*. A detailed description of how to perform individual tasks is in the on-line documentation for the Java Client. This chapter provides a general description of the interface, instructions on how to log in, and examples of some specific functions.

OVERVIEW

As shown in Figure 4.1, the ClearTrust SecureControl Manager consists of a menu bar, tabs for each of the functional areas of the Manager, specialized interaction panes for specific functions (different in each tab), and the various buttons that comprise typical windowing system GUIs.

Figure 4.1 ClearTrust SecureControl Manager Window.



User ID	First	Last
admin	SecureControl	Admin
Configuration	Configuration	Administrat
mmuser1	Mary	McGloin
mmadmin	Test	Test
ldapuser	anatoliy	avrutin
Administrator	admin	gavin
elena koch	elena	koch
marina koch	marina	koch
shivaldap	shiva	ldap
BASIC	basic auth	login
marina kocher	ldap	login
marina	securid	login

User ID	First	Last

Group: SecureControl Admin Group | Role: SecureControl Administrator | User: SecureControl Admin

Starting from the upper-left-hand corner of the figure, the interface features are as follows:

1. **Menu Bar -** includes the following:
   - **Manager -** lets you Exit the program entirely, or log off without exiting so you can log in again using another Administrator account.
   - **System -** includes a **Flush Cache** button that can be used to force updates of the ClearTrust SecureControl run-time server's cache after User data has been changed.
   - **Page -** a drop-down list of all the tabs that comprise the Manager; this is an alternative to clicking on the tab directly.
   - **Help -** links to online information about using the Manager.
2. **Tabs -** includes the following:
   - **Users -** functions involving User Properties, Users, Groups and Realms.
   - **Applications -** functions involving Applications and Application Functions.
   - **Basic Entitlements -** functions involving Runtime Access Control via Basic Entitlements.
   - **SmartRules -** functions involving Runtime Access Control via SmartRules.
   - **Web Servers -** functions involving web servers and server trees.
   - **Administrators -** functions involving Administrative Groups and Administrative Roles.

- **Policies-** access to Password policies.
- **User Properties** - define, edit and delete User Properties.
- **Test** - simulate a specified User attempting to access a specified Resource in order to test security policies.

3. **Specialized Panes** - change according to the tab selected, specific to the tab's function.
4. **Status Bar** - shows the Administrative Group, Administrative Role, and User account that is currently logged on.
5. **Cancel** - click the **Cancel** button to cancel all cancellable requests.

For more information about the functions listed, see Chapter 2, *The Entitlements Manager Background Concepts*.

LOGGING IN TO THE CLEARTRUST SECURECONTROL MANAGER

These instructions presume that you've installed and configured the ClearTrust SecureControl Manager; see the *Installation Guide* and the *Configuration and Implementation Guide* for more information.

Before starting the Entitlements Manager, you must have started the Entitlements Server. See the *Installation Guide* for more information.

> ***Warning:*** ClearTrust SecureControl installs with one default administrator account that you can use for initial login. This default account is `admin`, with the password of `admin`. Be sure to disable this account once you've created new accounts for actual administrators, or change the password to one that's secure to prevent unauthorized Users from accessing the system.

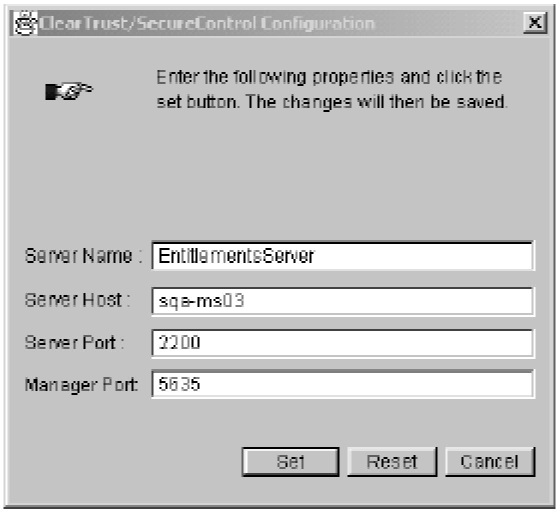
To log in to the ClearTrust SecureControl Manager:

1. From the Windows **Start** menu, select the following menu items: **Programs > Securant > ClearTrust SecureControl > Start All ClearTrust Services**.

   If this is first time you are launching the ClearTrust Manager software, you must first identify the server you wish to manage:

   a. In the Windows Start menu, select the following: **Programs > Securant > ClearTrust SecureControl > Entitlements Manager 4.6.1 > Configure**

Entitlements Manager. The ClearTrust SecureControl Configuration window is displayed:



Enter the following properties and click the set button. The changes will then be saved.

Server Name : EntitlementsServer

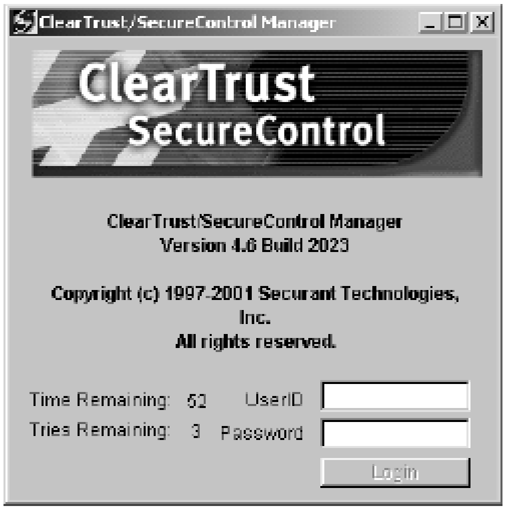
Server Host : sqa-ms03

Server Port : 2200

Manager Port 5635

b. In the Server Host field, enter the hostname (or the IP address) of the server that is running the Entitlements server. You can leave all the other fields unchanged. Once you are done, click on the **Set** button to save the new information.

2. To launch the Manager, then select the following in the Windows Start menu: **Programs > Securant > ClearTrust SecureControl > Entitlements Manager 4.6.1 > Entitlements Manager**.



ClearTrust/SecureControl Manager
Version 4.6 Build 2023

Copyright (c) 1997-2001 Securant Technologies, Inc.
All rights reserved.

Time Remaining: 52

Tries Remaining: 3

3. Once the Manager login screen is displayed, you will have 60 seconds to enter your User ID and Password and click the **Login** button to continue.

- The first time you launch the Manager application, you should login using the default administrator account (`admin`) and password (also `admin`).

4. If you have Administrative Roles in more than one Administrative Group, a Select Administrative Group dialog will be displayed after the login dialog. Select the Administrative Group you wish to belong to for this login session.

- You may have Administrative Roles in more than one Administrative Group, but you can only log in in one group at a time. Any object you create will belong to your current Administrative Group, and passwords for Users you create will have to conform to the password policy for that Administrative Group.
- If you are logging in as “admin” and have not added any Administrative Roles to that User ID, you will automatically be logged in as an Administrator of the default ClearTrust SecureControl Administrative Group. In this case, the Administration Role Choice dialog does not appear; the ClearTrust SecureControl Manager window opens directly from the **Login** dialog.

In a few seconds, the ClearTrust SecureControl Manager graphical user interface displays. The Entitlements Manager interface is now ready to use.

USING THE JAVA CLIENT: SOME EXAMPLES

The following examples provide a very basic introduction to the following functions in the ClearTrust SecureControl system:

- Creating a User
- Creating a Web Server
- Creating and Adding Resources to an Application
- Creating and Testing Basic Entitlements

While it is possible to protect network resources using only the functions described in the section, administrators of larger networks will benefit from more complex functionality such as Delegated Administration and Server Trees. See Chapter 2, *The Entitlements Manager Background Concepts* and the on-line documentation for more information.

CREATING A USER

A “User” is a unique User ID (UID) in the ClearTrust SecureControl system. While Users are usually individuals, you can also create User accounts for specific job functions within an organization.

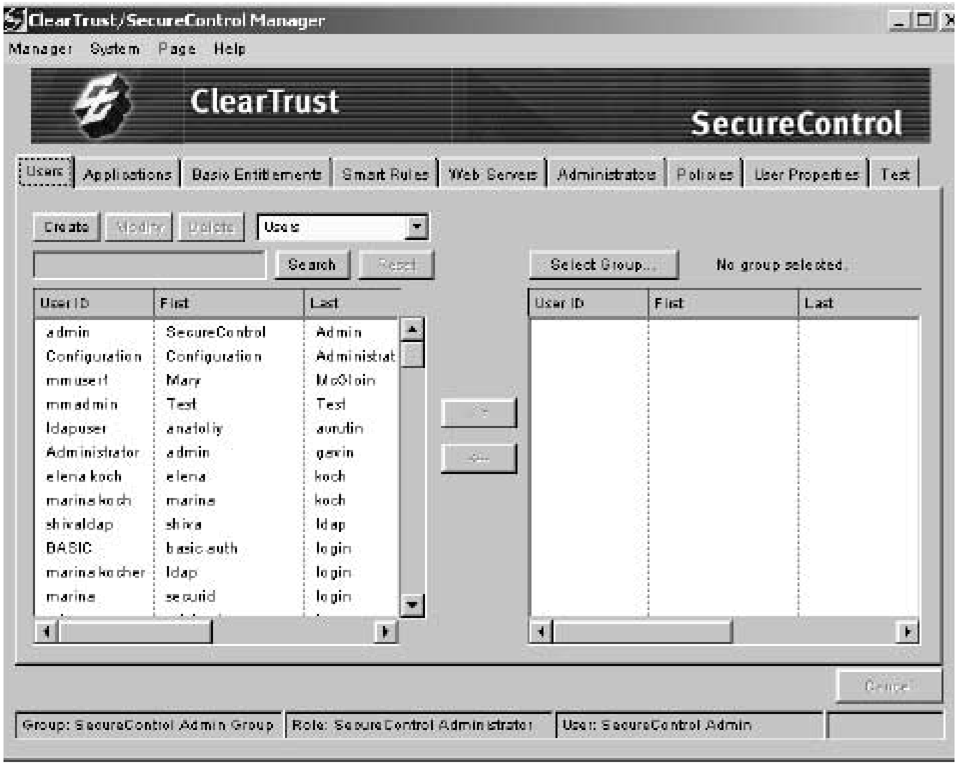
While it is possible to administer a system using only User accounts, ClearTrust allows you to group Users into Groups and Realms for more convenient administration. See Chapter 2, *The Entitlements Manager Background Concepts* and the on-line documentation for more information.

If you are going to control access via SmartRules, you should create the User Properties on which the SmartRules will be based before creating any Users. See Chapter 2, *The Entitlements Manager Background Concepts* and the on-line documentation for more information.

> ***Note:*** Because User IDs may be created for job functions as well as for people, it is possible for a person to have access via more than one User account ("HR" and "Charlie," for example). Keep in mind that Basic Entitlements, SmartRules and User Properties are associated with a User ID, not with an individual.

To create a User:

1. In the ClearTrust SecureControl Manager window, click on the **Users** tab to bring the Users tab pane to the front of the display:



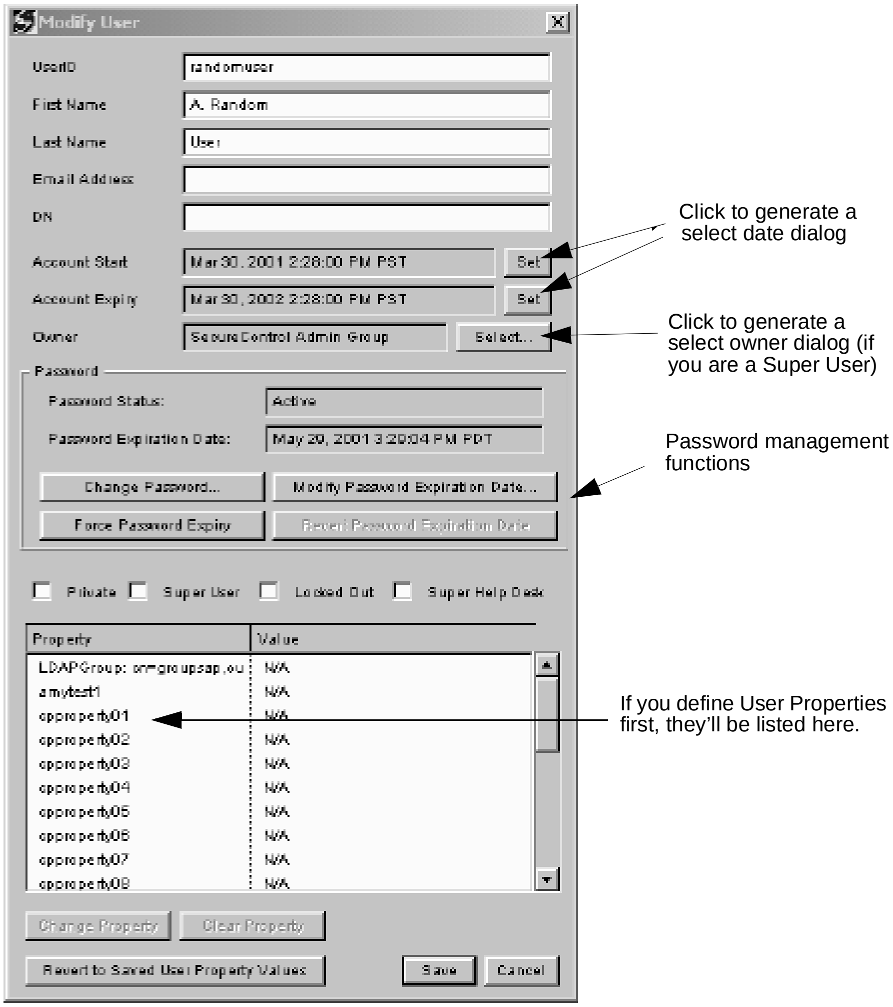
User ID	First	Last
admin	SecureControl	Admin
Configuration	Configuration	Administrat
mmuser1	Mary	McGloin
mmadmin	Test	Test
ldapuser	anatoliy	aurutin
Administrator	admin	gavin
elena koch	elena	koch
marina koch	marina	koch
shivaldap	shiva	ldap
BASIC	basic auth	login
marina kocher	ldap	login
marine	securid	login

User ID	First	Last

Group: SecureControl Admin Group | Role: SecureControl Administrator | User: SecureControl Admin

2. Select **Users** on the pull-down list near the upper-middle of the tab pane, if it is not already visible.

3. Click on the **Create** button to display the **Create User** dialog box:



Modify User

UserID: randomuser

First Name: A. Random

Last Name: User

Email Address:

DN:

Account Start: Mar 30, 2001 2:28:00 PM PST

Account Expiry: Mar 30, 2002 2:28:00 PM PST

Owner: SecureControl Admin Group

Password

Password Status: Active

Password Expiration Date: May 29, 2001 3:29:04 PM PDT

□ Private □ Super User □ Locked Out □ Super Help Desk

Property	Value
LDAPGroup: cn=groupsap,ou	N/A
amytest1	N/A
approperty01	N/A
approperty02	N/A
approperty03	N/A
approperty04	N/A
approperty05	N/A
approperty06	N/A
approperty07	N/A
approperty08	N/A

Set
Set
Select...
Change Password...
Modify Password Expiration Date...
Force Password Expiry
Revert Password Expiration Date
Change Property
Clear Property
Revert to Saved User Property Values
Save
Cancel

Click to generate a select date dialog

Click to generate a select owner dialog (if you are a Super User)

Password management functions

If you define User Properties first, they'll be listed here.

4. Enter a name for the User account in the **UserID** field following the User account naming guidelines or other appropriate convention for your environment (for example, first initial plus first seven characters of last name).

5. Enter values for all the other User information as needed for your organization. You can also change any of the default settings. (Click **Set** next to a greyed field to change the value in it, or just type into a white field. To change a User Property select the User Property and click **Change Property**).

Table 4.1 Fields, Checkboxes and Buttons in the Create User dialog

Field, Checkbox and Button names	Description	Usage note
UserID	Login ID for the User	Required
First Name	User's first name.	Optional
Last Name	User's last name	Optional
Email Address	Email address for the User	Optional

Table 4.1 Fields, Checkboxes and Buttons in the Create User dialog

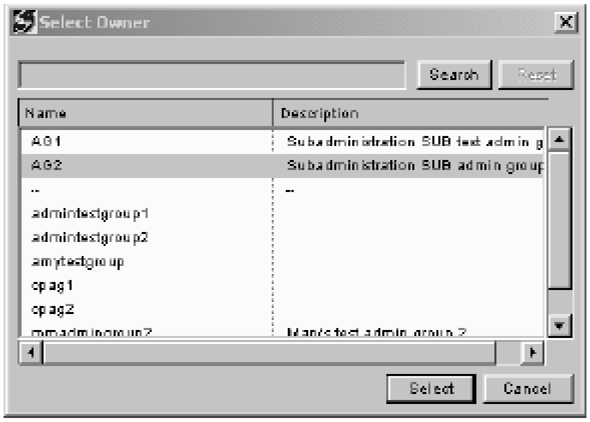
Field, Checkbox and Button names	Description	Usage note
DN	Distinguished name (X.500 schema)	Optional
Account Start	Date and time the account becomes active Default is the host machine time when User is saved.	Click **Set** to generate a dialog to choose the date. Click the **Now** button to use the current date and time of the host computer.
Account Expiry	Date and time the account will expire Default is 1 year after the Account Start date.	Click **Set** to generate a dialog to choose the date. Click the **Now** button to use the current date and time of the host computer.
Owner	Administrative Group that owns the User account	Default is the Administrative Group of the Administrator that created the User. If you are a Super User, click **Select** to display a dialog to select the owner.
Password Status	Indicates whether the password is *active* or has *expired*.	
Password Expiration Date	The password lifetime is set in the Password Policy associated with the Administrative Group that created the User.	
Change Password		Click to generate a **Change Password** dialog.
Modify Password Expiration Date		Click to generated a dialog to select the date.
Revert Password Expiration Date	Reverts the date to the previous value after **Force Password Expiry** has been used.	
Force Password Expiry		The default password, `ch4nge_me,` is automatically set when you create a new User through the SecureControl Entitlements Manager. If this password is expired when the User is created, the User will be prompted to choose a new password the first time they log in.

Table 4.1 Fields, Checkboxes and Buttons in the Create User dialog

Field, Checkbox and Button names	Description	Usage note
Private	Identifies the User account as private; only the owning Administrative Group will be able to view this User. The default is public.	
Super User	Super Users can perform any action on any User, Group, Realm, or Application. A User designated as a Super User must be an Administrator.	This checkbox is only enabled if the person creating the account is logged on as a Super User. Assign with caution.
Locked Out	Immediately disables any permissions granted to the User.	Only Super Users can enable this feature.
Super Help Desk	Enables help desk personnel to change or reset passwords across all Administrative Groups	A User identified as Super Help Desk must also be Administrators
Change Property	Displays a Modify User Property dialog box that enables you to change the value of a User Property.	Click on a User Property to highlight its name, and then click on Change Property to display the **Change Property Value** dialog box.
Clear Property		Highlight the User Property name in the list and click on the Clear Property button to erase the value displayed.
Revert to Saved User Property Values		Click to revert User Properties to the previously saved values for the User.

6. If you're a Super User and you want to transfer ownership of this User account to an Administrative Group other than the one displayed, click the **Select** button (next to the Owner field) to display the **Select Owner** dialog box and

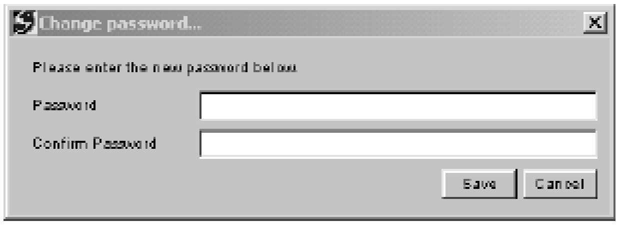
select the Administrative Group to which you want to transfer ownership of this User.



Name	Description
AG1	Subadministration SUB test admin g
AG2	Subadministration SUB admin group
--	--
admintestgroup1	
admintestgroup2	
amytestgroup	
cpag1	
cpag2	
mmadmingroup2	Mary's test admin group 2

- Select the new Administrative Group and click **Select** to transfer ownership to the selected Administrative Group.

7. To create a new password for the User, click the **Set Password** button to display the **Change Password** dialog box:



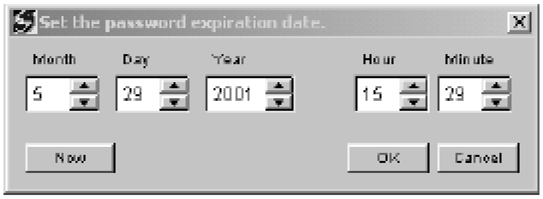
   a. Enter the Password.

      - The password must conform to the Password Policy for the Administrative Group of the Administrator creating the User.

   b. Re-enter the password in the **Confirm Password** field.

   c. Click **Save** to save the password and return to the **Users** tab.

8. You can also select the **Modify Password Expiration** button to display the **Set Password Expiration** dialog. In this dialog, you can reset this individual User's password expiration to a specific date or select **Now** to immediately expire the password.The User will be prompted to choose a new password the next time they log in.



Month: 5
Day: 29
Year: 2001
Hour: 15
Minute: 29

9. Select the **Force Password Expiration** button to override the password lifetime for an individual User. When you select this button, the password expiration date will be displayed in red to indicate that the Administrative Group's default password expiration date has been overridden.

- Select the **Revert Password Expiration** button to revert back to the original password expiration.
- If the password is set to expire when the User is created (via the Password Policies for the User's Administrative Group), the User will be able to log in with the default password the first time they log in to the system, but will then be immediately prompted to change their password. In this case, the **Revert Password** button will be greyed out.

10. Mark the User as Private, Super User, or Super Help Desk (or all three) by selecting the appropriate checkboxes. See Table 4.1 for additional information about these choices.

11. Once you've finished specifying all the information for the User, click **Save** to save the User's information in the SecureControl database.

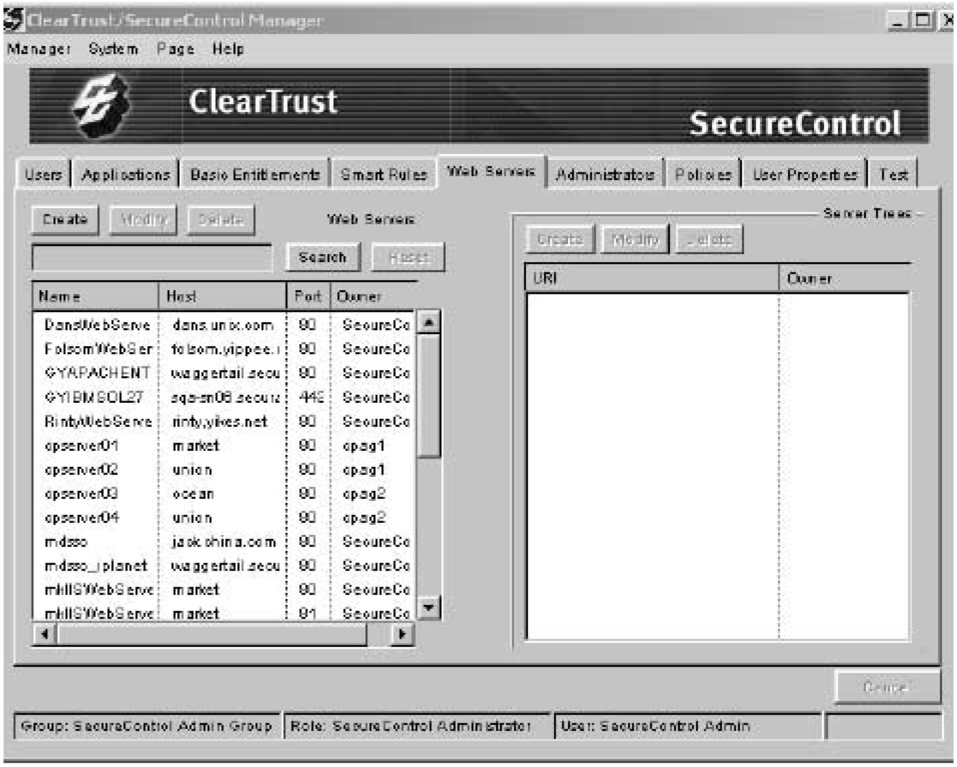
CREATING A WEB SERVER

These instructions presume that you've already installed ClearTrust SecureControl Server and that you have a ClearTrust protected Web Server—one with the ClearTrust Web Server Plug-in installed and configured—running on your network. (See the *Installation Guide* for additional information.).

While it is possible to administer a network using only Web Servers to define protected areas, the ClearTrust SecureControl system supports more granular definitions using *Server Trees*. See Chapter 2, *The Entitlements Manager Background Concepts*, and the on-line documentation for more information.

To create a Web Server entry:

1. Click **Web Servers** in the ClearTrust SecureControl Manager window to open the **Web Servers** tab:



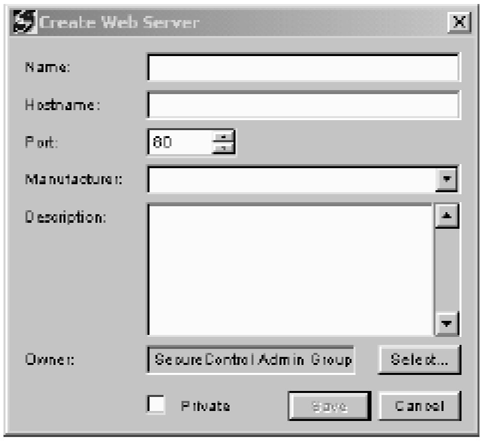
Name	Host	Port	Owner
DansWebServe	dans.unix.com	80	SecureCo
FolsomWebSer	folsom.yippee.i	80	SecureCo
GYAPACHENT	waggertail.secu	80	SecureCo
GYIBMSOL27	sqa-sn08.securi	443	SecureCo
RintyWebServe	rinty.yikes.net	80	SecureCo
opserver01	market	80	opag1
opserver02	union	80	opag1
opserver03	ocean	80	opag2
opserver04	union	80	opag2
mdsso	jack.china.com	80	SecureCo
mdsso_iplanet	waggertail.secu	80	SecureCo
mkIISWebServe	market	80	SecureCo
mkIISWebServe	market	81	SecureCo

Group: SecureControl Admin Group

Role: SecureControl Administrator

User: SecureControl Admin

2. Click the **Create** button above the Web Servers pane in the Web Servers tab to open the **Create Web Server** dialog:



Port: 80

Owner: SecureControl Admin Group

3. Specify the name, hostname, port number, manufacturer, and description of the Web Server. The manufacturer and description information is for your own

information; the name, hostname, port number, and owner are significant pieces of information, as described in the following table:

Table 4.2 Web Server information

Entry	Description	Usage Note
Name	Name by which the Web Server is known to the ClearTrust SecureControl system	Must be a unique name for the web server (unique in the context of your ClearTrust environment). Theoretically, this name can be anything, but it must match the Web Server name parameter in the Web Server Plug-in's `Default.conf` file (`securecontrol.plugin.web_server_name`). The default name in that file is "WebServer;" if you enter something other than that here, be sure you change the Default.conf file for the Plug-in.
Hostname	Must match the actual fully-qualified name of the Web Server	For example, *hostname.domain.com*. You can enter the IP address if you prefer
Port number	Must match the port address on which your Web Server advertises its http services.	Default is typically port 80, but if you've configured your web server with a different port number, enter it here.
Owner	Administrative Group (within ClearTrust SecureControl) that will own this Web Server.	By default, the Administrative Group that your current login account is an Administrator of will display. If you're logged on as a Super User, you can transfer ownership to another Administrative Group.

4. Mark the web server as private by selecting the **Private** checkbox. A private web server can be seen and manipulated only by an Administrator with the same Administrative Role as the Administrator who created the web server. Web servers are created as public by default.

5. Click **Save** to save information about the web server. The server is now listed in the **Web Servers** pane on the **Web Servers** tab.

Once you've setup a web server in the ClearTrust SecureControl Manager, you can later return to the **Web Servers** tab and change the information about the web server; you can also delete the web server entirely.

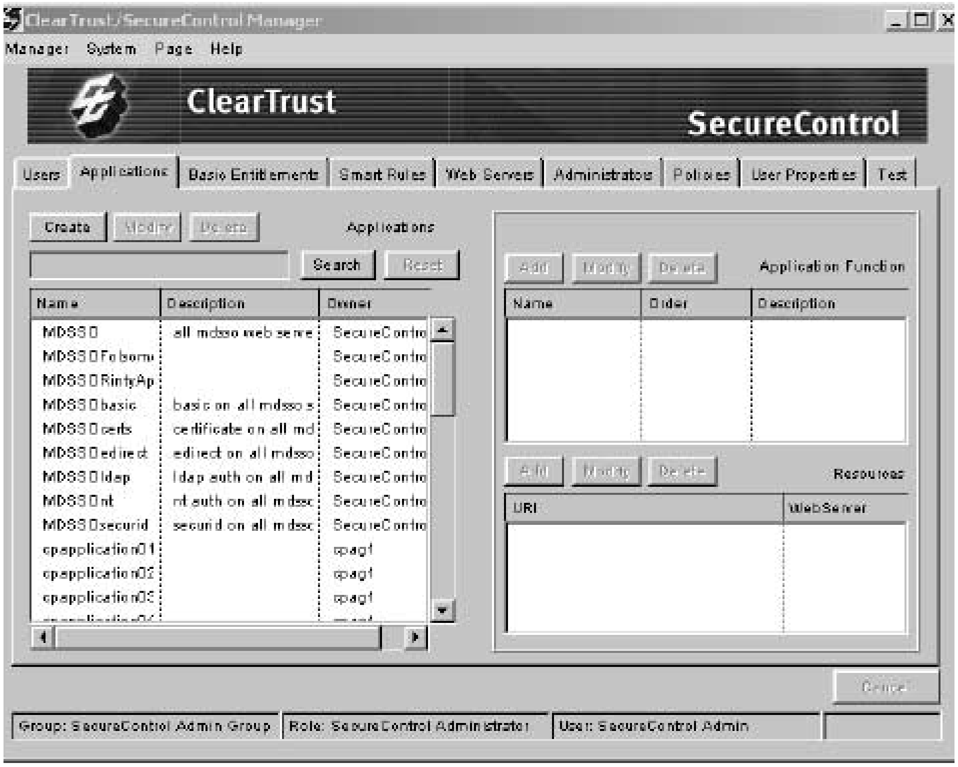
CREATING AND ADDING RESOURCES TO AN APPLICATION

Resources in the ClearTrust SecureControl system are grouped into Applications. To protect a Resource, Users are given access or denied access to these Applications.

It is also possible to have more granular levels of access control using Application Functions. See Chapter 2, *The Entitlements Manager Background Concepts* and the on-line documentation for more information.

To create a new Application:

1. Click **Applications** in the ClearTrust SecureControl Manager window to open the **Applications** tab:



Name	Description	Owner
MDSSO	all mdsso web serve	SecureContro
MDSSOFoborm		SecureContro
MDSSORintyAp		SecureContro
MDSSObasic	basic on all mdsso s	SecureContro
MDSSOcerts	certificate on all md	SecureContro
MDSSOedirect	edirect on all mdsso	SecureContro
MDSSOldap	ldap auth on all md	SecureContro
MDSSOnt	nt auth on all mdssc	SecureContro
MDSSOsecurid	securid on all mdssc	SecureContro
cpapplication01		cpag1
cpapplication02		cpag1
cpapplication03		cpag1

Name	Order	Description

URI	WebServer

Group: SecureControl Admin Group | Role: SecureControl Administrator | User: SecureControl Admin

2. Click the **Create** button above the **Applications** panel in the **Applications** tab to open the **Create an Application** dialog box.

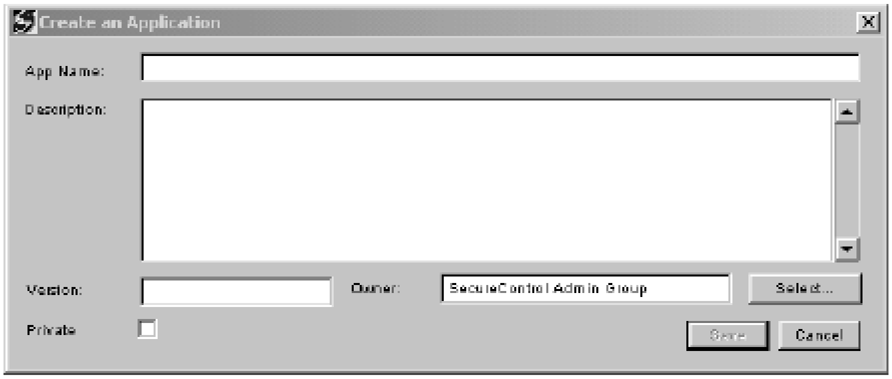
a. Enter a meaningful name for the Application in the **App Name** field.

b. Enter a description for the Application, and a version number if appropriate. You can use the Version field to enter any additional information that will help describe the application.

- If you're a Super User and you want to transfer ownership of the Application to an Administrative Group other than the one displayed, click the **Select** button (next to the Owner field) to display the **Select Owner** dialog box. Select the name of the Administrative Group from the list by clicking on its name and then click the **Select** button to transfer ownership of the Application and redisplay the **Create an Application** dialog box.

c. You can also select the **Private** checkbox if you want to make the Application private: A private Application can be seen and manipulated only by an Administrator with the same Administrative Role as the

Administrator that created the Application. Applications are created as public by default.



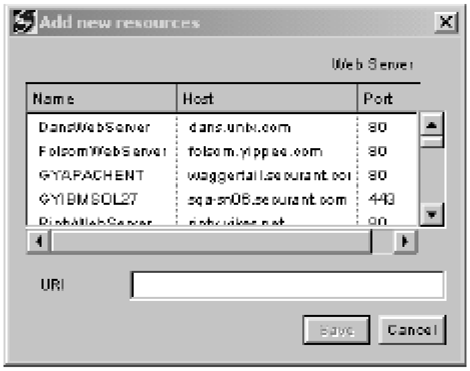
Owner: SecureControl Admin Group

Private □

d. Click the **Save** button to save the Application. The Application is now listed in the **Applications** pane on the **Applications** tab. You can add Resources to the Application as described in the following section.

To add Resources to an Application:

1. If you are not already in the **Applications** tab, open the tab by clicking on **Applications** in the Tab menu.
2. Select the Application to which you wish to add Resources by clicking on its name in the Applications pane.
3. Click the **Add** button above the **Resources** pane on the **Applications** tab to display the **Add new resources** dialog box.



Web Server

Name	Host	Port
DansWebServer	dans.unix.com	80
FolsomWebServer	folsom.yippee.com	80
GYAPACHENT	waggertail.securant.co	80
GYIBMSOL27	sqa-sn06.securant.com	443
[illegible]	[illegible]	[illegible]

4. Highlight the name of the web server that contains the Resource you'll be securing.
5. Enter the name of the URI in the URI field. You can enter the complete URI or you can enter a wildcard to secure everything under directory path.
6. Click the **Save** button to save the resource specified as part of the Application. The **Applications** tab re-displays, and you'll see this Resource listed in the **Resources** pane of the **Applications** tab.

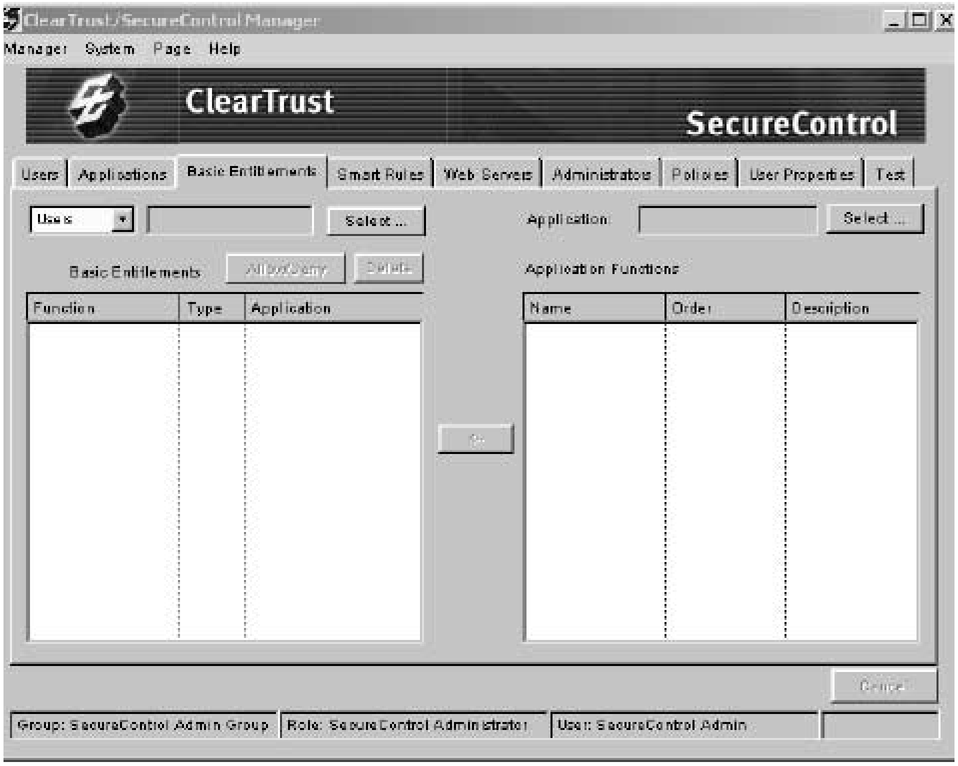
Warning: When specifying directories on a web server to be protected, exclude the `/securant` directory, particularly the directories containing the CGIs and forms. Using a “`/*`” to protect your entire web server will block from accessing the CGIs and forms needed to perform operations such as password changes. The best solution to protect all the directories on your web server is to move all the directories (except `/securant`) in to a sub-directory and then protect that sub-directory.

CREATING AND TESTING BASIC ENTITLEMENTS

There are two ways to protect Resources in the ClearTrust SecureControl system. The first, simpler, way is via Basic Entitlements, which are based on the individual User ID or the User’s Group or Realm. The second way is via SmartRules. This section describes Basic Entitlements - for information about SmartRules and more detailed information about Basic Entitlements see Chapter 2, *The Entitlements Manager Background Concepts* and the on-line documentation.

To define Basic Entitlements:

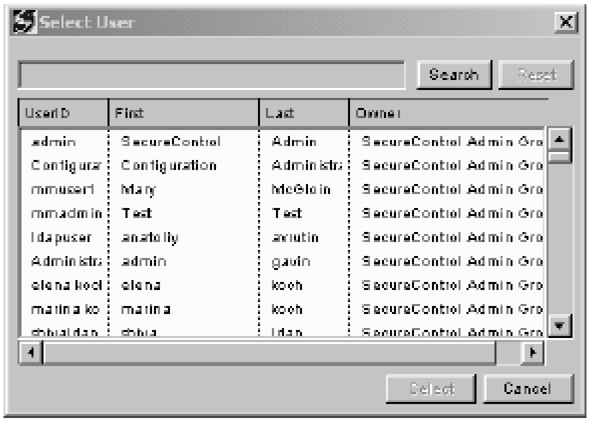
1. Click **Basic Entitlements** in the ClearTrust SecureControl Manager window to open the **Basic Entitlements** tab:



Group: SecureControl Admin Group | Role: SecureControl Administrator | User: SecureControl Admin

2. If Users is not already selected, select **Users** from the pull-down list box in the upper left corner of the tab.

3. Click the **Select** button above the Basic Entitlements pane to open the **Select User** dialog:

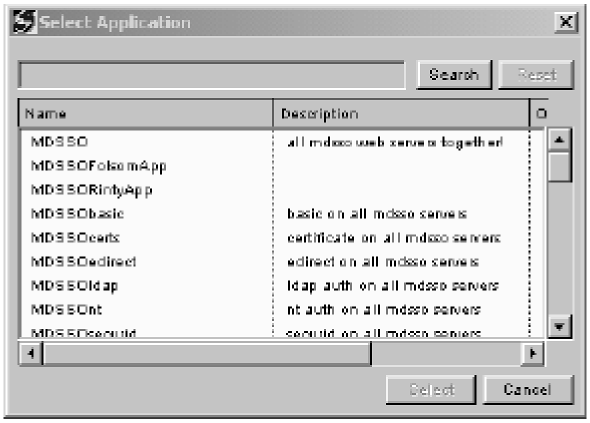


UserID	First	Last	Owner
admin	SecureControl	Admin	SecureControl Admin Gro
Configurat	Configuration	Administra	SecureControl Admin Gro
mmuser1	Mary	McGloin	SecureControl Admin Gro
mmadmin	Test	Test	SecureControl Admin Gro
ldapuser	anatoliy	avrutin	SecureControl Admin Gro
Administra	admin	gavin	SecureControl Admin Gro
elena koch	elena	koch	SecureControl Admin Gro
marina ko	marina	koch	SecureControl Admin Gro
shbualdan	shbua	ldan	SecureControl Admin Gro

a. Click on the name of the User to whom you want to assign a Basic Entitlement.

b. Once the name is selected, click **Select** to confirm your selection and return to the **Basic Entitlements** tab pane. The User's existing Basic Entitlements will be displayed.

4. Select the Application you want to protect by clicking the **Select** button next to the **Application** field. The **Select Application** dialog displays:



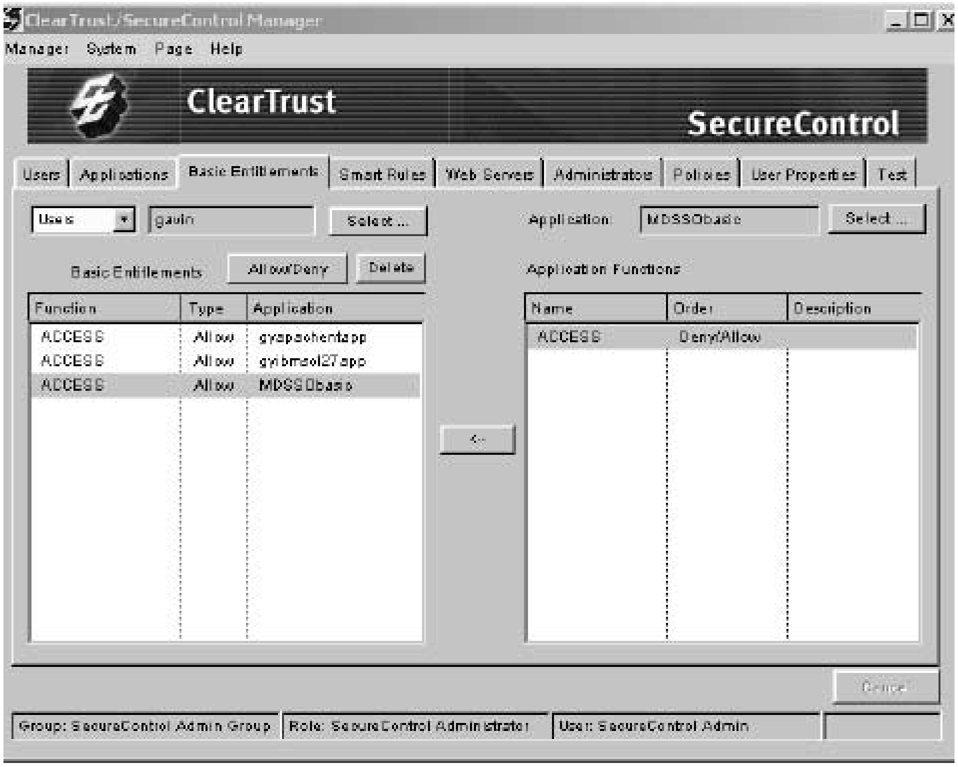
Name	Description	O
MDSSO	all mdsso web servers together!	
MDSSOFolsomApp		
MDSSORintyApp		
MDSSObasic	basic on all mdsso servers	
MDSSOcerts	certificate on all mdsso servers	
MDSSOedirect	edirect on all mdsso servers	
MDSSOldap	ldap auth on all mdsso servers	
MDSSOnt	nt auth on all mdsso servers	
MDSSOsecuid	securid on all mdsso servers	

5. Click on the name of the Application in the list and then click the **Select** button to confirm your selection and redisplay the **Basic Entitlements** tab. The Application you selected is now displayed. The Application Functions associated with that Application are listed in the **Application Functions** pane.

- The default Application Function, ACCESS, is created automatically when an Application is created. Adding it to a list of Basic Entitlements will allow or deny access to all the URIs in the Application (depending on whether Allow or Deny is shown in the **Type** field).

6. Copy the Application Functions you want to include as part of the Basic Entitlement from the **Application Functions** pane to the **Basic Entitlements** pane by clicking on an Application Function to highlight its name and then clicking on the left arrow button (**<--**).

Once the Application Function is listed in the **Basic Entitlements** pane, select the name of the Application Function you wish to use for the Basic Entitlement. The **Allow/Deny** button and the **Delete** button will become active:


ClearTrust/SecureControl Manager
Manager System Page Help
ClearTrust
SecureControl
Users Applications Basic Entitlements Smart Rules Web Servers Administrators Policies User Properties Test
Select ...
Allow/Deny
Delete
<--
Select ...
Close

Users: gavin

Application: MDSSObasic

Basic Entitlements

Function	Type	Application
ACCESS	Allow	gyapachentapp
ACCESS	Allow	gyibmaol27app
ACCESS	Allow	MDSSObasic

Application Functions

Name	Order	Description
ACCESS	Deny/Allow	

Group: SecureControl Admin Group | Role: SecureControl Administrator | User: SecureControl Admin

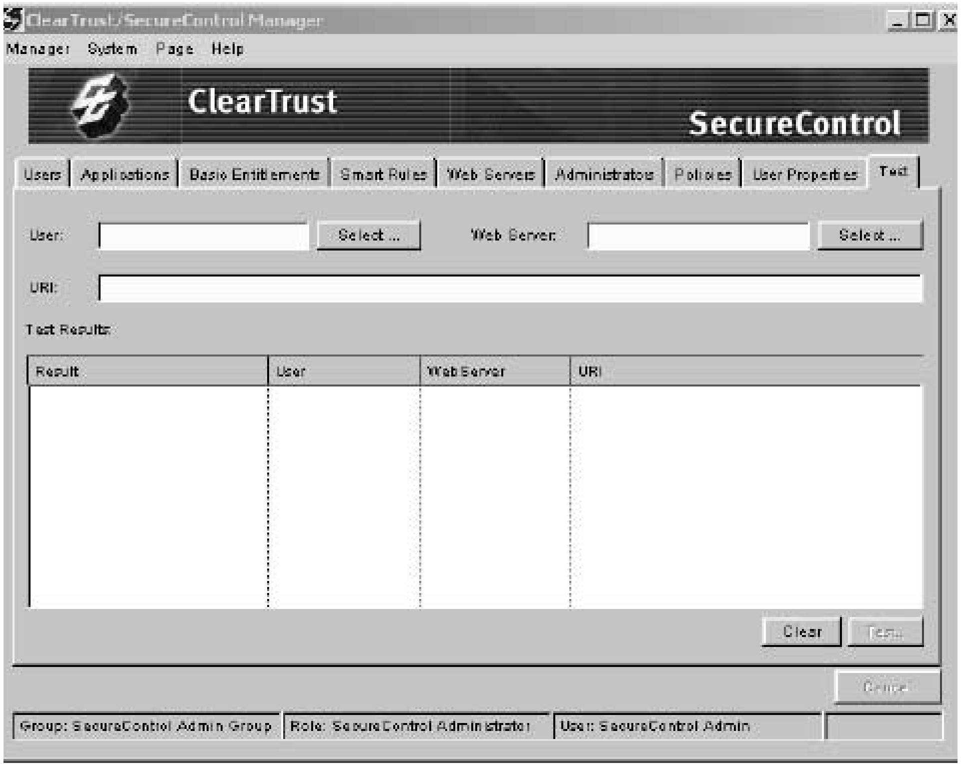
7. Click the **Allow/Deny** button to toggle the access type to Allow or Deny.

- The value in the **Order** field in the list of Application Functions for the Application is used to process SmartRules, and does not effect Basic Entitlements.

You have now created a Basic Entitlement that allows or denies the specified User, Group, or Realm access to the specified Application.

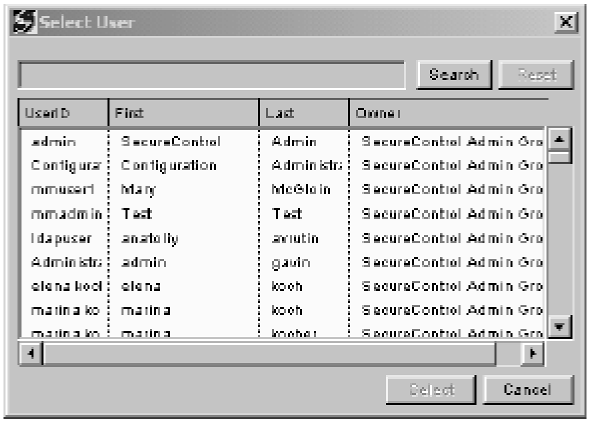
To test a Basic Entitlement:

1. Click on the **Test** tab to open the **Test** interaction:


ClearTrust/SecureControl Manager
Manager System Page Help
ClearTrust
SecureControl
Users Applications Basic Entitlements Smart Rules Web Servers Administrators Policies User Properties Test
User:
Select ...
Web Server:
Select ...
URI:
Test Results:
Result User Web Server URI
Clear
Test
Close

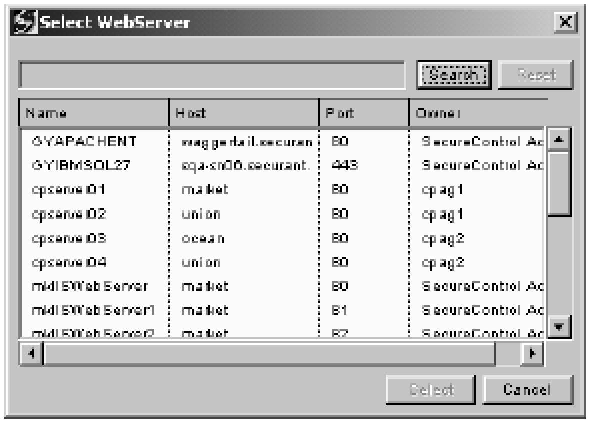
Group: SecureControl Admin Group | Role: SecureControl Administrator | User: SecureControl Admin

2. Click the **Select...** button next to the **User** field to open the **Select User** dialog. Select the User ID of the User for whom to test access, and click the **Select** button:



UserID	First	Last	Owner
admin	SecureControl	Admin	SecureControl Admin Gro
Configurat	Configuration	Administr	SecureControl Admin Gro
mmuser1	Mary	McGloin	SecureControl Admin Gro
mmadmin	Test	Test	SecureControl Admin Gro
ldapuser	anatoliy	avrutin	SecureControl Admin Gro
Administr	admin	gavin	SecureControl Admin Gro
elena koch	elena	koch	SecureControl Admin Gro
marina ko	marina	koch	SecureControl Admin Gro
marina ko	marina	kocher	SecureControl Admin Gro

3. Click the **Select...** button next to the **Web Server** field to open the **Select Web Server** dialog. Select the name of the web server for the URI to which you want to test access, and click the **Select** button:



Name	Host	Port	Owner
GYAPACHENT	maggerdail.securan	80	SecureControl Ac
GYIBMSOL27	sqa-sn06.securant.	443	SecureControl Ac
cpserver01	market	80	cpag1
cpserver02	union	80	cpag1
cpserver03	ocean	80	cpag2
cpserver04	union	80	cpag2
midl5WebServer	market	80	SecureControl Ac
midl5WebServer1	market	81	SecureControl Ac
midl5WebServer2	market	82	SecureControl Ac

4. Enter the URI to test access to in the **URI** field.

5. Click **Test** to perform the test.

6. If the list of test results becomes too long, click **Clear** to clear the test results pane.

CHAPTER

5

INTEGRATING OTHER DIRECTORIES AND CLEARTRUST

The ClearTrust SecureControl solution enables enterprises to leverage the information stored in existing LDAP (lightweight directory access protocol) or ActiveDirectory directories by populating the ClearTrust Entitlements database with User account information from external directories by using the SecureControl Directory Replication Manager. This tool comprises two software components:

- The SecureControl Directory Replicator, a background software process that handles interaction with external directory services (also called LDAP Agent)
- The SecureControl Replication Manager, the graphical user interface that Administrators use to configure, schedule, and manage replication

You can configure regularly scheduled, on-going replication with a wide range of access directory products. This chapter explains how to configure directories for replication and how to use the ClearTrust SecureControl Replication Manager.

> ***Note:*** It is also possible to customize your Web Server Plug-in environment so that Users authenticate to LDAP directories (see *The ClearTrust SecureControl Installation Guide* for more information).

This chapter contains the following sections:

- Configuring Directories for Replication
- Using the ClearTrust SecureControl Replication Manager

CONFIGURING DIRECTORIES FOR REPLICATION

This section tell you how to configure specific directory services for Replication. The following directory servers are supported:

- Microsoft ActiveDirectory
- Netscape Directory Server 2.x
- Netscape Directory Server 3.x
- Netscape Directory Server 4.x (iPlanet)
- PeerLogic i500 8A.2
- PeerLogic i500 8A.3 (no configuration necessary)
- LDIF Files (no configuration necessary)

MICROSOFT ACTIVEDIRECTORY

ActiveDirectory should be properly configured automatically during installation of Windows 2000 Server. Follow Microsoft’s on-screen instructions after booting up the server. In order for ClearTrust’s Directory Replicator to work properly, you will need to create an NTFS partition and configure the server as a domain controller. See Microsoft’s documentation for more information. (For more information about replicating Microsoft ActiveDirectory, see *Specific Information for ActiveDirectory Replication* on page *5-15*).

NETSCAPE DIRECTORY

To replicate from a Netscape Directory Server, the Server must be configured as a replication supplier. If the Netscape Directory Server from which you are going to replicate has not already been configured to be a replication supplier, you must perform the configuration:

1. Use the Netscape Admin Server to go to the Server’s administration console.
2. Select the Directory Server that you want to use as the supplier.
3. From the Navigation bar, click **Replication**.
4. Click the **Configure this Server** link on the left side of the page.
5. In the **Supplier Server Replication Settings** section:
   a. Select the directory in which you want the change log to be stored.
   b. Enter **`cn=changelog`** for the changelog suffix.
   c. set the `max changelog records` and the `max changelog age`.
6. Click **OK**.
7. Click **Apply** in the header to apply your changes.
8. Restart the Directory Server to apply the above changes.

PEERLOGIC-ICL I500 8A.2 DIRECTORY

To replicate from a PeerLogic-ICL i500 8A.2Directory Server, you must make the changelogs format (in the `attributes.cfg` file) consistent with the LDAP Replicator Tool format.

To modify the changelogs:

1. Shut down the PeerLogic-ICL i500 8A.2 Directory Server.
2. Insert the following modifications to `attributes.cfg` in the correct numerical order in the `i500ldap` directory:

```
2.16.840.1.113730.3.1.5
NAME 'changeNumber'
DESC 'a number which uniquely identifies a change made to a directory
      entry'
SYNTAX 'INTEGER'
EQUALITY integerMatch
ORDERING integerOrderingMatch
)


(2.16.840.1.113730.3.1.6
     NAME 'targetDN'
     DESC 'the DN of the entry which was modified'
     EQUALITY distinguishedNameMatch
     SYNTAX 'DN'
)


  (2.16.840.1.113730.3.1.7
     NAME 'changeType'
     DESC 'the type of change made to an entry'
     EQUALITY caseIgnoreMatch
     SYNTAX 'DirectoryString'
  )


  ( 2.16.840.1.113730.3.1.8
     NAME 'changes'
     DESC 'a set of changes to apply to an entry'
     SYNTAX 'OctetString'
  )


  (2.16.840.1.113730.3.1.9
    NAME 'newRDN'
    DESC 'the new RDN of an entry which is the target of a modrdn
operation'
    EQUALITY distinguishedNameMatch
    SYNTAX 'DN'
  )


  (2.16.840.1.113730.3.1.10
    NAME 'deleteOldRDN'
    DESC 'a flag which indicates if the old RDN should be retained as
an attribute of the entry'
    EQUALITY booleanMatch
    SYNTAX 'BOOLEAN'
  )


  (2.16.840.1.113730.3.1.11
    NAME 'newSuperior'
    DESC 'the new parent of an entry which is the target of a moddn
operation'
    EQUALITY distinguishedNameMatch
    SYNTAX 'DN'
  )
```

3. Restart the PeerLogic-ICL i500 Directory Server. The changelogs are now readable by the Directory Replicator Tool.

USING THE CLEARTRUST SECURECONTROL REPLICATION MANAGER

This section tells you how to use ClearTrust SecureControl Replication Manager.

> ***Warning:*** All existing directory entries should be imported before any replication occurs to ensure correct behavior. When replicating from Microsoft ActiveDirectory, the initial import should be performed using the Replicate Now function as opposed to Import, to avoid duplicating changes during the next scheduled replication.

> ***Note:*** Be sure to start the Replication Agent before attempting to start the Replication Manager. See the *Installation Guide* for more information.

This section contains the following sub-sections:

- Starting the Replication Manager
- Buttons and Fields in the Replication Manager
- Creating and Modifying Replication Tasks
- Tabs in the Task Configuration Interaction

STARTING THE REPLICATION MANAGER

To start the Replication Manager:

- In Windows NT: **Start > Programs > Securant > Securecontrol > Replication Manager**
- In Unix: execute the file `LDAPManager.exe` file
- In Solaris and HP-UX: execute the file `LDAPManager.bin`

BUTTONS AND FIELDS IN THE REPLICATION MANAGER

- **Schedule** - schedule tasks for replication according to selected intervals. It changes to "Unschedule" if a selected task is already scheduled
- **Stop** - abort a currently executing task
- **Import** - import all of the existing Users and Groups in the LDAP database into the ClearTrust SecureControl database
- **Unimport** - remove all the Users and Groups that were previously imported from the ClearTrust SecureControl database

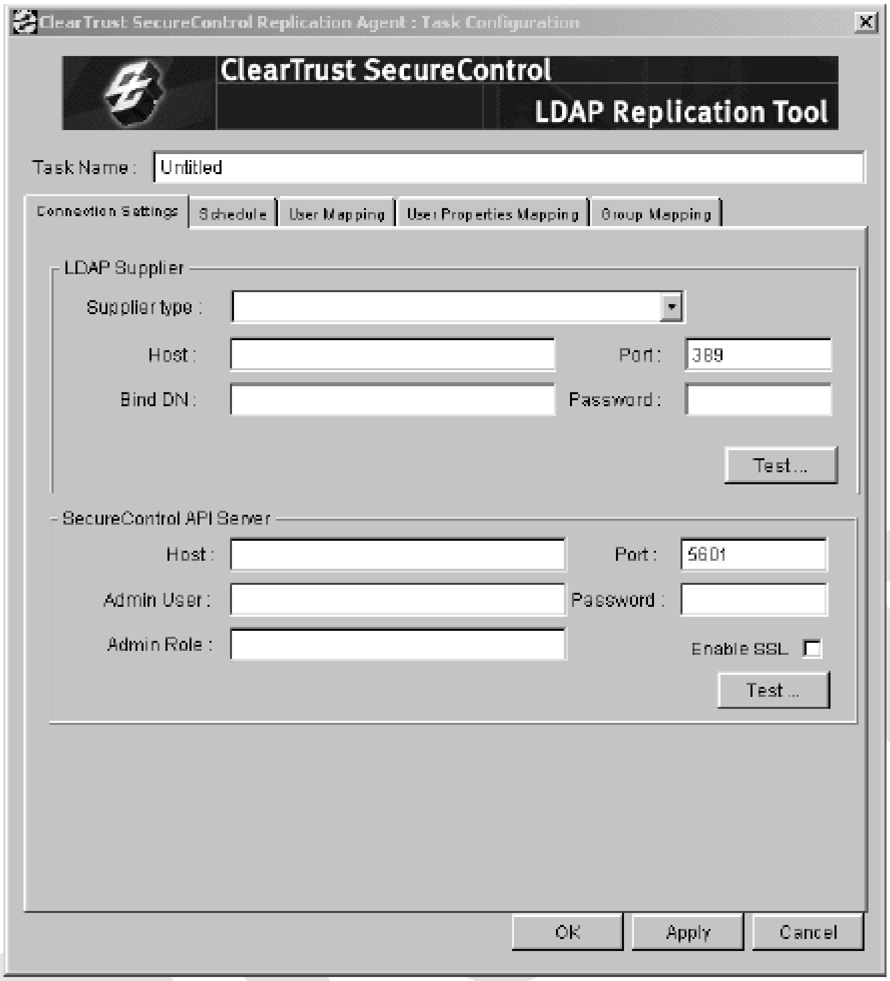
- **Replicate Now -** override the scheduled replication time and perform replication immediately
- **Reset Last Change Log # -** reset the change log # to zero
- **Task Name -** list of the names of the tasks you have created
- **Next Run -** the scheduled time for the next replication
- **Current State -** the current state of the selected task
- **Last Change Log # -** the number of the last change log entry replicated (not available in ActiveDirectory and LDIF)
- **View Log -** view the change log. You can click on the up and down arrows to select the number of lines you would like the system to display.
- **New -** add a new task
- **Copy -** copy a task. Select the name of the task from the list in the Task Name field. After you select the task, click **Copy** and specify the name for the newly created task.
- **Remove -** remove a task. Select the name of the task from the list in the Task Name field. After you select the task, click **Remove**.
- **Properties -** view and edit the properties of a task. Select the name of the task in the Task Name field and click the Properties button,

CREATING AND MODIFYING REPLICATION TASKS

To replicate User data from an external database into ClearTrust SecureControl, you must first define a replication task.

To define a replication task:

1. Click **New** to open the New Task Configuration window. This window contains five tab panels: **Connection Settings**, **Schedule**, **User Mapping**, **User Properties Mapping**, and **Group Mapping**.


ClearTrust SecureControl Replication Agent : Task Configuration

ClearTrust SecureControl
LDAP Replication Tool

Task Name : Untitled

LDAP Supplier
Supplier type :
Host :
Port : 389
Bind DN :
Password :

SecureControl API Server
Host :
Port : 5601
Admin User :
Password :
Admin Role :
Enable SSL □

2. Enter a name for the new task in the **Task Name** field.

   Important: The task name should contain only characters that can be used in file names (i.e. alphanumeric, - and _). It should not contain slashes, periods, commas or ampersands (&).

3. Navigate among the tabs to configure task. Specific information about the tabs is in *Tabs in the Task Configuration Interaction* on page *5-6*.

When you click **Apply** on this panel, the changes you have made to a task are saved. When you click **OK**, all the changes are saved and the **Task Configuration** panel closes. If you have just created the task, its name now appears in the Task Name pane.

Once a task is created, you can also modify the task using the same Task Configuration panel.

TABS IN THE TASK CONFIGURATION INTERACTION

The following are tabs in the **Task Configuration** interaction:

- Connection Settings

- Schedule
- User Mapping
- User Property Mapping
- Group Mapping

Connection Settings

To configure connection settings:

1. Click **Connection Settings** in the **Task Configuration** window to open the **Connection Settings** tab.
2. Enter the following information in the **Supplier** panel:
   - **Supplier Type -** the type of external directory.
   - **Host -** the hostname of the machine where the external directory server is running.
   - **Port -** the port the external directory server is listening on.
   - **Bind DN -** the Distinguished Name (DN) of the external directory entry that has permission to access the change log in the external directory Server. This can be the unrestricted User *cn=Directory Manager* in the default Directory Server installation or an entry with the appropriate ACL assigned to it. See your web server's administrator guide for details.

     Note: When using Microsoft's ActiveDirectory, the account used to bind to the directory must have the `SE_SYNC_AGENT_NAME` privilege.
   - **Password -** the password for the Bind DN.
3. Click the **Test** button in the **Supplier** pane to check that the information you supplied is valid. If you have any problems, double-check your Supplier Server configuration to make sure the settings you entered are correct. This must be configured properly for the replication to take place.
4. Supply the following information in the **ClearTrust SecureControl API Server** panel.
   - **Host** - the host where the ClearTrust SecureControl API server resides.
   - **Port** - the port the ClearTrust SecureControl API server listens on.
   - **Admin User** - the User ID of the ClearTrust SecureControl Administrator with the appropriate administrative permissions to do the replication.

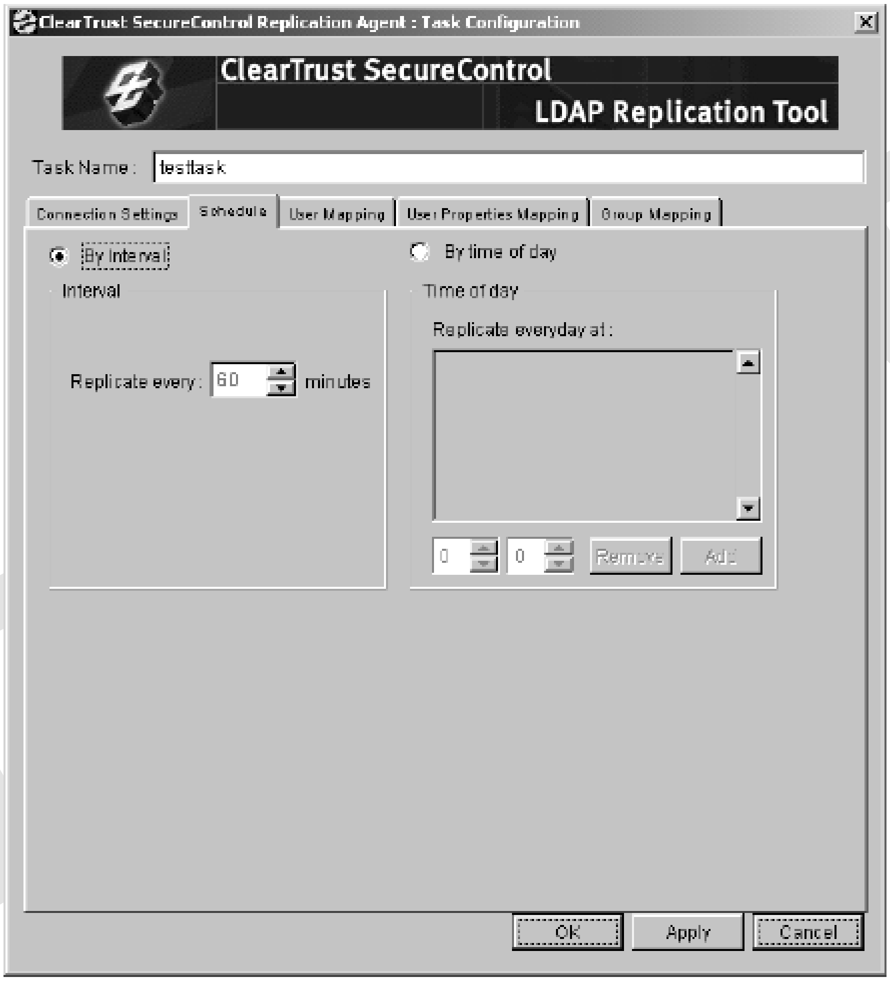
     Note: All Users to be replicated will be in the same Administrative Group as this Administrative User.
   - **Password -** the Administrative User's password.
   - **Admin Role -** the Administrative Role of the Administrative User.
   - **Enable SSL -** whether or not the API server has been configured to require the use of SSL. The software components in the environment must either all be configured for SSL or none of them should be. Check the SSL setting of the `default.conf` files for all components (ClearTrust SecureControl servers, Web Server Plug-in, and the Web Server itself) if you're not sure.

5. Click the **Test** button in the **ClearTrust API Server Information** pane to test the information. A window appears displaying the results of the connection. If errors occur, double-check your ClearTrust SecureControl API Server configuration to make sure the settings you entered are correct. Connection Settings are now complete.

Schedule

To configure schedule settings:

1. Click **Schedule** in the window to open the **Schedule** tab.



Task Name : testtask

● By Interval

○ By time of day

Replicate every : 60 minutes

0 0

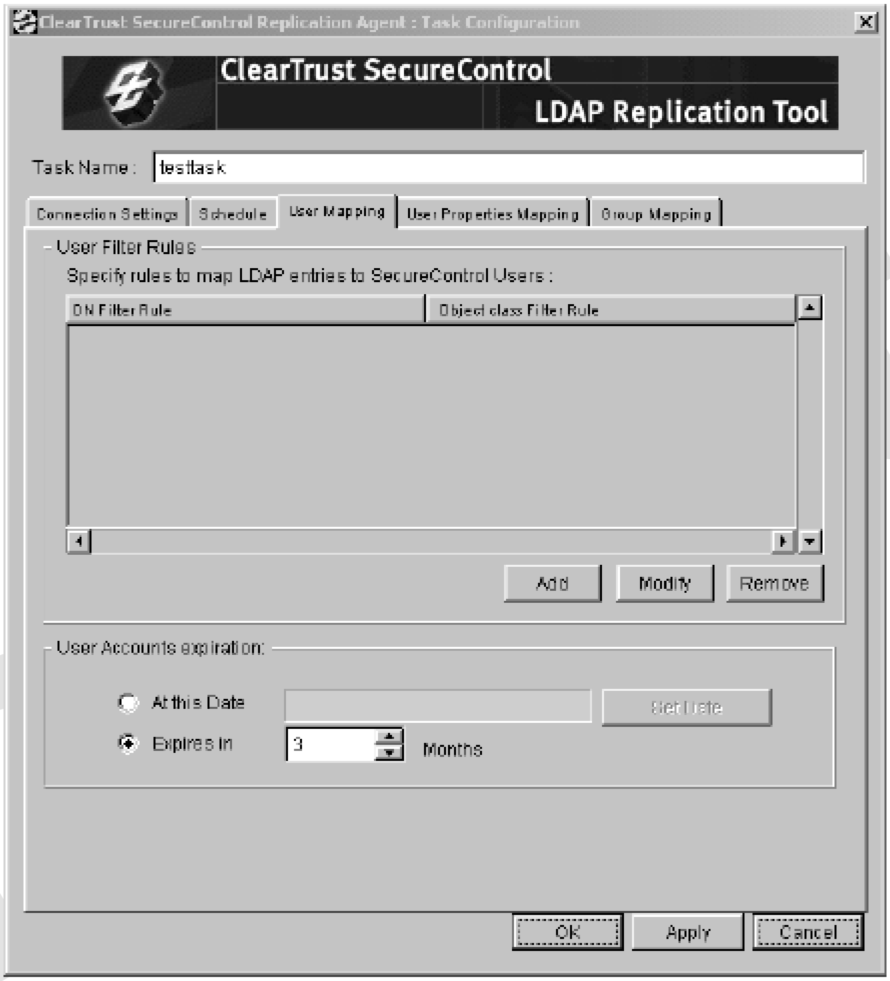
2. To configure how you want the directory replication scheduled, click on either **By Interval** or **By Time of Day**.

- **By Interval -** replicate at minute intervals throughout the day by selecting the number of minutes in the **Replicate every** field.
- **By Time of Day -** replicate at particular times each day by selecting the times in 24-hour format.

User Mapping

To configure rules that map external directory entries to SecureControl Users:

1. Click **User Mapping** in the **Task Configuration** window to open the **User Mapping** tab.



ClearTrust SecureControl Replication Agent : Task Configuration

Task Name : testtask

User Filter Rules

Specify rules to map LDAP entries to SecureControl Users :

DN Filter Rule	Object class Filter Rule

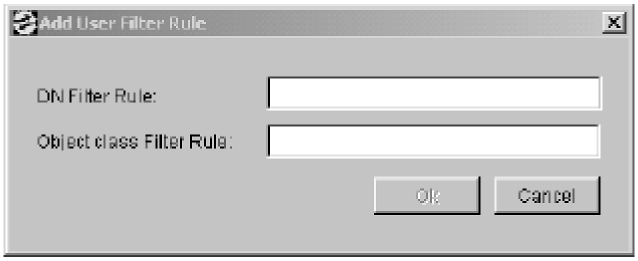
User Accounts expiration:

○ At this Date

● Expires in 3 Months

2. Choose DN Filter Rule and/or Objectclass Filter Rule from the pull-down list. You can specify either or both for User mapping.
   - If you specify a DN filter, only the entries under that DN will be replicated. If you specify an Objectclass filter, only entries of that Objectclass will be replicated. DN and Objectclass rules within a single filter are linked as *Boolean ANDs* - entries must meet all requirements to be replicated. When multiple filters are created they are linked together logically as *Boolean ORs* - entries that meet any one of the sets of requirements will be replicated. You must map the appropriate fields in the external directory that will be used to populate the required fields for each entry in ClearTrust SecureControl

3. Click **Add** to create a new rule. You can also highlight a rule and click on **Modify** to alter it, highlight a rule and click **Remove** to delete it.



4. Check either **At this Date** and **Set Date** to specify the User account expiration date. Or check **Expires in** and choose a number from the pull-down menu to designate the number of months before User accounts will expire.

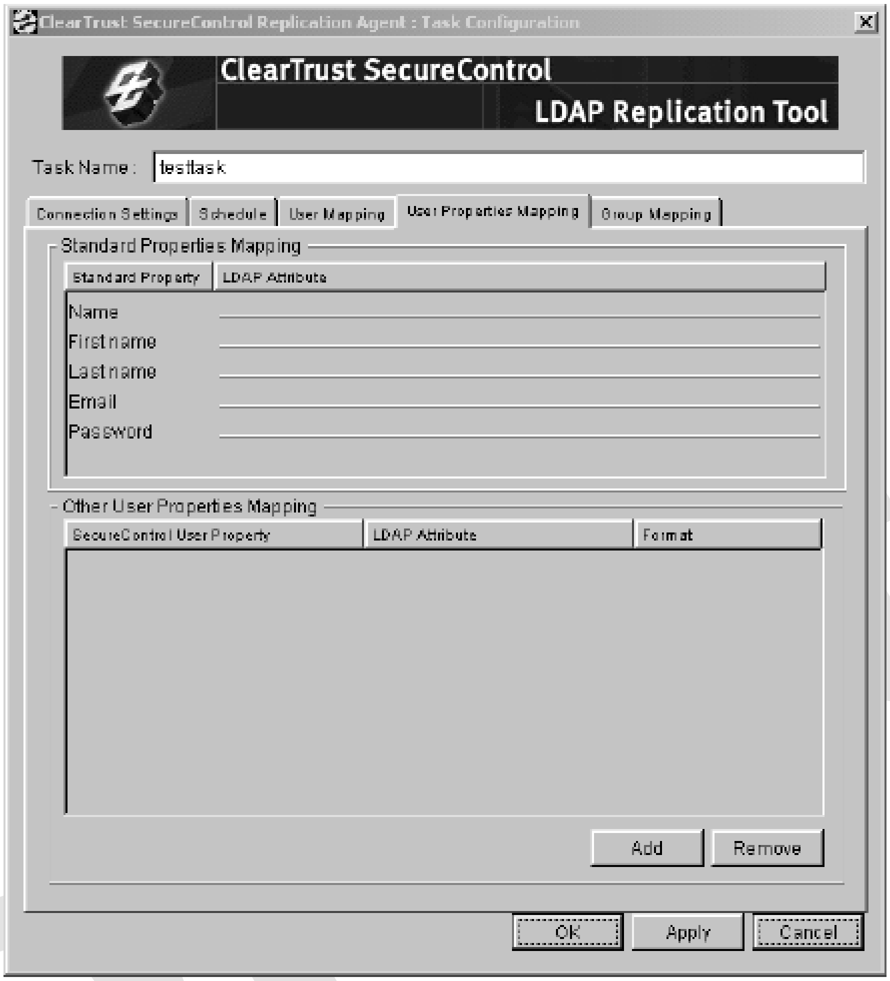
> ***Note:*** You must be very specific when entering Filter Rules for Users and Groups (as discussed later) to avoid conflicts. The Filter Rules for Users and Groups must be distinct or entries will be mapped incorrectly.

User Property Mapping

> ***Note:*** User Properties must be defined prior to replication.

To map additional external directory attributes to ClearTrust SecureControl User Properties:

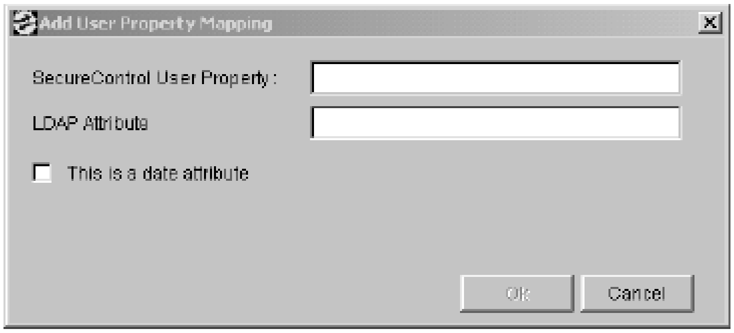
1. Click **User Properties Mapping** in the **Task Configuration** window to open the **Properties Mapping** tab. This displays the **Standard Properties Mapping** field that contains Standard Property information and external directory Attribute information.



Task Name : testtask

2. Type in the external directory Attribute to be mapped to standard SecureControl User Properties

3. Use the **Add** and **Remove** buttons to map or remove additional attributes stored in external directories to User Properties in your ClearTrust SecureControl database. Clicking **Add** displays the **Add User Property Mapping** window.



□ This is a date attribute

4. Enter the name of the SecureControl User Property to which you would like to map the external attribute.

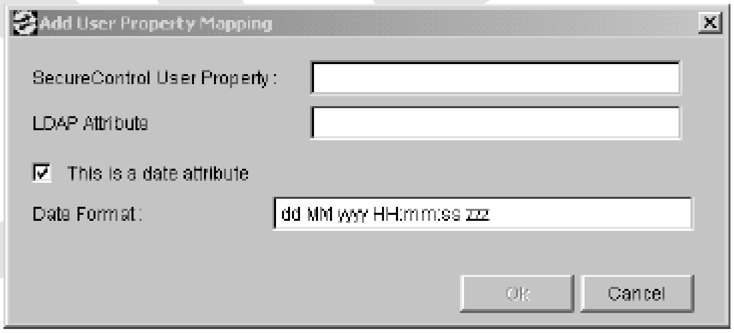
5. Enter the name of the external Attribute you would like to map. If no attribute is specified, the system uses the default. Default mappings are in Figure 5.1:

Table 5.1 Default User Property and User Flag Mappings

	Entitlements Database	External Directory Attribute
User Properties	User Name	uid
	First Name	givenname
	Last Name	sn
	Email	mail
	Password	userpassword
User Flags	public	ispublic
	superuser	issuper
	helpdesk	ishelpdesk

Note: Most external directories do not store passwords in clear text and therefore this property cannot be replicated. As a result, passwords should be mapped to a non-existent external attribute.

6. If the property is a date, click the **This is a date attribute** checkbox in the **Add User Property Mapping** dialog to display the date format field. You can replace the default date format using the formatting conventions in Table 5.2.



Add User Property Mapping

SecureControl User Property :

LDAP Attribute

☑ This is a date attribute

Date Format : dd MM yyyy HH:mm:ss zzz

The default date format uses two digits or characters for all values except for the year, which is four digits, and the time-zone, which is three characters or digits.

Table 5.2 Date Formatting Conventions

Symbol	Meaning	Datatype	Example
G	era designator	text	AD
y	year	digit	1996

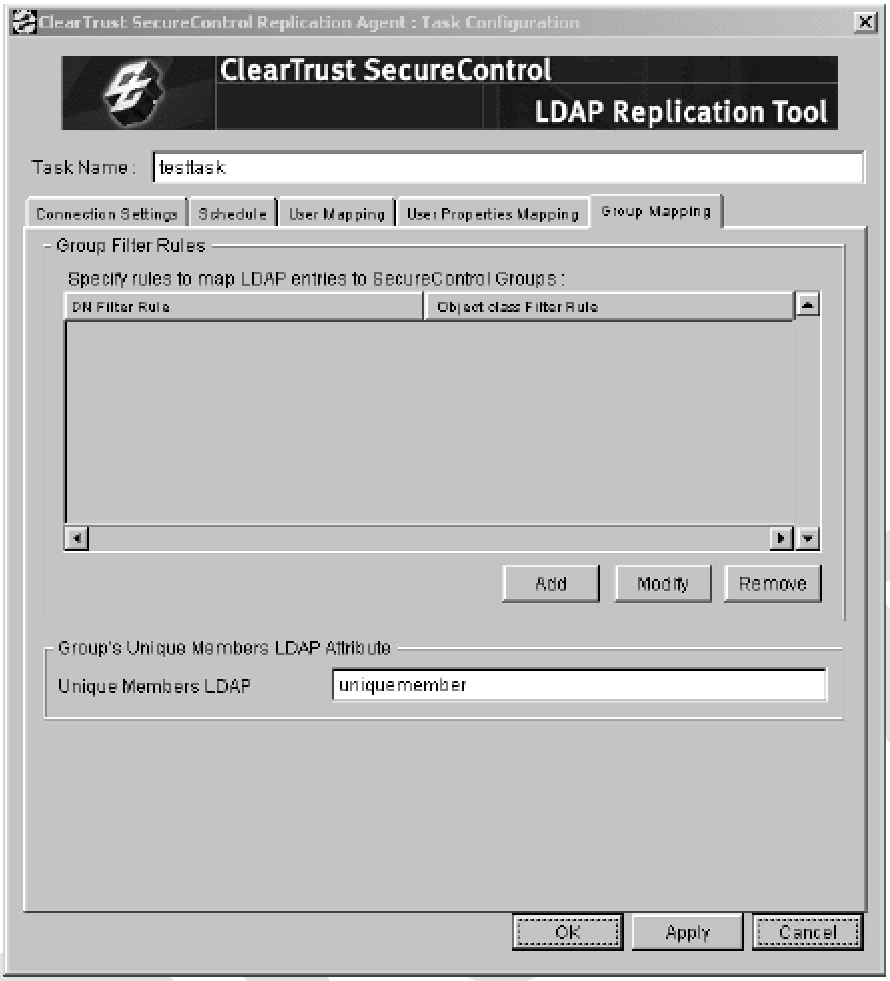
Table 5.2 Date Formatting Conventions

Symbol	Meaning	Datatype	Example
M	month	text or digit Use MM for the number of the month, use any other number of Ms for text.	July and 07
d	day	digit	10
h	hour in am/pm (1-12)	digit	12
H	hour in 24-hour day (0-23)	digit	0
m	minute in hour	digit	30
s	second in minute	digit	55
S	millisecond	digit	978
E	day in week	text	Tuesday
D	day in year	digit	189
F	day of week in month	digit	2 (2nd Wed in July)
w	week in year	digit	27
W	week in month	digit	2
a	am/pm market	text	PM
k	hour in day (1-24)	digit	24
K	hour in am/pm (0-11)	digit	0
z	time zone	text	Pacific Standard Time
‘	escape for text	delimiter	
‘’	single quote	literal	

Group Mapping

To specify rules to map external directory entries to SecureControl Groups:

1. Click on **Group Mapping** in the **Task Configuration** window to open the **Group Mapping** tab. The **Group Mapping** tab displays the Group Filter Rules that you need to specify to map external directory entries to SecureControl Groups. These rules are defined as DN Filter Rules or Objectclass Filter Rules. You can specify one or both filter rules for group mapping.



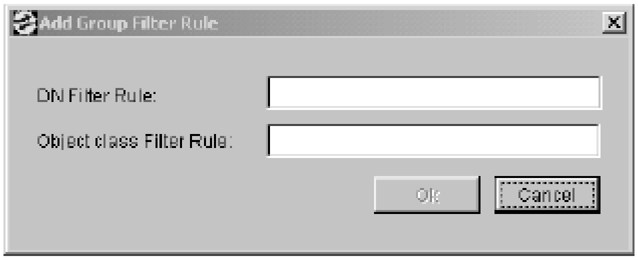
Task Name : testtask

Unique Members LDAP uniquemember

- If you specify a DN filter, only the entries under that DN will be replicated. When you specify an Objectclass filter, only entries of that Objectclass will be replicated. DN and Objectclass rules within a single filter are linked as *Boolean ANDs* - entries must meet all requirements to be replicated. When multiple filters are created they are linked together logically as *Boolean ORs* - entries that meet any one of the sets of requirements will be replicated. You must map the appropriate fields in the external directory that will be used to populate the required fields for each entry in ClearTrust SecureControl.

Note: You must be very specific when entering DN Filter Rules for Users and Groups to avoid conflicts. The DN Filter Rules for Users and Groups must be distinct or entries will be mapped incorrectly.

2. Click **Add** to generate the **Add Group Filter Rule** dialog.



3. Enter the rule and click **OK** to close the dialog.
4. In the Group's Unique Members Attribute pane, enter the group's unique member attribute in the external directory that will be used to identify members (Users) in each Group in SecureControl.

You can also highlight a rule and click on **Modify** to alter a rule. Or you can highlight a rule and click **Remove** to delete it

SPECIFIC INFORMATION FOR ACTIVEDIRECTORY REPLICATION

The following tips may be useful when replicating Microsoft's ActiveDirectory:

Before Replication:

- When replicating from Microsoft ActiveDirectory, the initial import should be performed using the Replicate Now function as opposed to Import, to avoid duplicating changes during the next scheduled replication.

Task Configuration:

- You can use the ADSI Edit tool included in the Win2k support tools to browse through a directory directly. This may be useful in determining correct property mappings.
- When mapping the User Property "Name" (as in login name), use the LDAP Attribute `sAMAccountName`
- The directory structure in ActiveDirectory is different from other vendors. In ActiveDirectory the directory prefix is specified in two parts (for example, `dc=securant`, `dc=com`), while in Netscape or iPlanet the directory prefix is a single string (for example `o=securant.com`).
- You must specify the full DN of the User, for example: "cn=Administrator,cn=users,dc=engtest,dc=securant,dc=com"
- Multiple DNs must be within the same partition. Otherwise, only one base DN can be specified per replication task.

Troubleshooting:

- If ClearTrust returns an "Unknown User" error when trying to replicate a User listed in an ActiveDirectory directory, change the permissions on the directory to allow anonymous reads/searches of the User tree. Alternatively, you can set the `uid` attribute to **`dn`**, which will allow ClearTrust to use the DN field to locate the User rather than performing a search.

- If User entries are ignored (not replicated), the credentials specified during the replication task may not be sufficient to perform the replication task. In order to perform replication the replication agent creates a property dirsync_object_guid of type string (if it does not already exist).To do so, the agent must be able to create User Property definitions.