ClearTrust SecureControl

Policy Administration Guide

Version 4.2

August 2000

ClearTrust SecureControl, Release 4.5

Securant Technologies, Inc., One Embarcadero Center, 5th Floor, San Francisco, CA 94111

DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. I.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

The reason behind this being stated in this direct manner is past experience in code simply being copied and the attribution removed from it and then being distributed as part of other packages. This implementation was a non-trivial and unpaid effort.

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 otherfunctions.

(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.

About this Guide

Intended Audience

This *Policy Administration Guide* is designed to help security administrators, system administrators, and IT planners understand and use Securant's ClearTrust solution for securing their intranet, extranet, and Internet resources.

Conventions

The following conventions are used in this guide:

Convention	Meaning
`courier text`	Courier font denotes filenames, directory names, pathnames, or commands.
`italic text`	Italic font denotes variables or field values in command strings and the titles of other guides.
`UPPER CASE`	Upper-case denotes environment variables or Oracle commands, including SQL commands.
`[ ]`	Optional information appears in brackets.
`...`	Ellipsis in code listings denote continuation of a file or command.

Related Documents

For more information, see the following guides, available on the Securant ClearTrust installation CD:

- *Installation and Configuration Guide*
- *Developer's Guide*

Your Comments Are Welcome

Please send comments, corrections, and suggestions about this guide to *pubs@securant.com*.

Chapter 1
ClearTrust SecureControl Overview

This chapter introduces ClearTrust SecureControl's Unified Access Management solution. It includes the following sections:

- How ClearTrust SecureControl Provides the Complete Solution
- ClearTrust SecureControl Components
- Component Security
- Embedded Supporting Software Products
- Support for Related Software Products

How ClearTrust SecureControl Provides the Complete Solution

Many organizations today are implementing the Internet at the core of their business models, both internally and externally. Intranets provide mission-critical information throughout an organization, while Extranets make organizations more easily accessible to business partners, customers, and suppliers. As an open, public network, the Internet provides a virtually limitless platform for any organization conducting business in a global marketplace.

As an open, public network, however, the Internet also exposes organizations to risk; it lacks essential security features that companies need to conduct e-business. Thus, organizations involved in e-business require a comprehensive system that lets them define and manage security policy so that they can conduct successful and secure business via the Internet.

Security policy defines a structure for and the rules governing access to information contained in an organization's Intranet or on their Extranet. ClearTrust SecureControl is an integrated, policy-based access management

solution that provides a wide range of tools for organizations to define and manage security policy. Using ClearTrust SecureControl, you can define policies governing:

- **Access Control** - what users can access which resources on a Web server;
- **Authorization** - which functions can a user perform within an application;
- **Auditing** - what user and administrator actions must be audited;
- **Authentication** - how to prove a user's identity;
- **Assessment** - ensures that the security policy is implemented correctly;
- **Single Sign-On** - seamless access across Web servers;
- **Delegated Administration** - which administrators can implement security policy; and
- **Intrusion Detection and Response** - what defines an attack and what policies can be implemented to respond.

Managing security policy for potentially tens or hundreds of thousands of Users—partners, customers, suppliers, and employees—is an administrative challenge. In addition, executing a security policy

organizations with a large number of Users, a poorly defined security policy can leave the entire enterprise vulnerable. Some Users may be denied access to important applications to which they are entitled, while others can be granted access to restricted Applications. ClearTrust SecureControl addresses the potential problems and risks associated with managing security policy for an organization's Extranet, Intranet, and e-business applications.

Comprehensive Security Infrastructure

ClearTrust SecureControl provides a complete security solution for both enterprise Web and Client/Server environment. ClearTrust SecureControl is designed to manage a large number of Users and provides multiple levels of access control for corporate Extranets and Intranets. Using ClearTrust SecureControl, you can manage employees, customers, and suppliers simultaneously in both Windows NT and UNIX environments. In short,

ClearTrust SecureControl offers a unified method for consistently deploying security services for a large number of Users across various platforms and Applications in a simple and cost-effective manner.

ClearTrust SecureControl centralizes security policy management for your Web environment and enhances the management of your existing environment by providing the following key benefits:

- Multiple Forms of Authentication
- Simplified Integration
- Streamlined Administration
- Delegated Policy Administration
- Business Rules
- Web Single Sign-on
- Reliability and Fault Tolerance
- Scalablity
- Native Support for LDAP Directories
- Java and C APIs
- Auditing and Logging
- Administration

Multiple Forms of Authentication

Authentication is a process that verifies the identity of a User who is logging onto a network or computer system. Common authentication mechanisms include passwords, digital certificates, smart cards, and one-time password cards. By supporting multiple authentication modes, ClearTrust SecureControl enables you to create a flexible authentication system tailored to your specific needs.

You can deploy a variety of off-the-shelf authentication mechanisms, and you can also create and implement your own custom authentication mechanisms. ClearTrust SecureControl's pluggable authentication framework allows you to choose the authentication mechanism—or multiple mechanisms—that work best for different environments. ClearTrust SecureControl ships with out-of the-box support for ClearTrust

SecureControl Username-and-password combinations, Windows NT logins, LDAP passwords, digital certificates, and SecurID token cards. ClearTrust SecureControl can also be used with biometrics devices.

ClearTrust SecureControl's support for multiple forms of authentication promotes added security, greater flexibility, and simplified management. For example, you can deploy more secure forms of authentication, such as token cards and digital certificates, to protect especially sensitive resources, and you can require only usernames and passwords for those resources having less stringent security requirements. Support for multiple authentication mechanisms provides maximum flexibility in deployment.

Authorization and Access Control

Authorization and *access control* refer to the system's mechanisms for granting a specific User access to a resource. Access control is a form of authorization and answers the question "can any User access resource X?" Other types of authorization can be more specific, for example, "can User 'Joe' delete a record?" or "can User 'Joe' place an order online?" ClearTrust SecureControl supports granular access control to Web resources as well as fine-grained authorization at the Application Function level.

Simplified Integration

ClearTrust SecureControl is designed to provide a single security solution for existing, heterogeneous, multi-vendor environments, and provides out-of-the-box integration with leading Web technologies. ClearTrust SecureControl is an off-the-shelf solution for deploying a security infrastructure, employing such diverse technologies as LDAP directories, digital certificates, Web Servers, and Application Servers. It substantially lowers integration costs and deployment times associated with implementing secure Web Applications.

Streamlined Administration

Security policy administration can be a labor-intensive task. ClearTrust SecureControl offers a number of features that simplify security policy management for any number of Users. First of all, administration is centralized via a simple, Java-based GUI, the ClearTrust SecureControl Manager. From the ClearTrust SecureControl Manager, you can define security policy based on logical User Groups and Administrative Roles, and

you can manage security policy using your organization's business rules, or policies. You can further enhance security policy administration by using ClearTrust SecureControl's unique and powerful Smart Rules™, which automate much of the security policy administration process.

Delegated Policy Administration

In order to manage security policy for large sites you must delegate the administration of these policies securely. Secure delegated administration ensures that only the right Administrators have the privileges necessary to make certain changes.

ClearTrust SecureControl supports a flexible model in which administration is delegated through Administrative Groups, also referred to as Virtual Business Units (VBUs). Within Administrative Groups, specific Administrative Roles have associated privileges. With ClearTrust SecureControl security built into Administrative Groups, you can scale the workload of User administration across departments, operating companies, and Extranet partners. This type of delegation lowers administration costs, improves responsiveness, and enhances overall site manageability.

Administrative Groups allow your administrative hierarchy to reflect your actual business model. You can establish individual administrative hierarchies that are responsible for managing specific resources and Users. With these Administrative Groups in place, departments can manage the resources specific to their department, while complying with overall security practices and policies established by your organization.

For example, you can create a help desk Administrative Group in which the help desk Administrators are permitted to create new accounts and reset passwords for Users but are not permitted to change access control policies. You can also establish Administrative Groups for partner companies, thereby allowing your partners to administer their own Users. There is also enforced privacy between Administrative Groups so partners can't manage or view other partners' Users or information.

Business Rules

Business rules refer to the policies that define your company's business practices. ClearTrust SecureControl provides an integrated policy administration platform that leverages business rules extensively.

ClearTrust SecureControl was designed to make the task of security policy administration as easy as possible no matter how large the User base. ClearTrust SecureControl provides the tools to manage a large User base intelligently and efficiently. Without adequate management and administrative tools, even the fastest security system will collapse under the weight of a growing User base.

ClearTrust SecureControl's Smart Rules technology allows you to build automated access control policies that reflect actual business requirements. Compared to basic non-automated "role banding" rules that are static in nature, Smart Rules dynamically links access control policies to User data that is subject to change. By implementing security policies based on Smart Rules, you ensure that access control policies are updated automatically as conditions change and are always accurate and scalable to a growing User base.

For example, you can define a Smart Rule based on a User's credit status. That is, the credit status you define determines whether the User is allowed access to a resource. If his or her credit falls below acceptable levels, he or she is automatically denied access to the protected resource. Once the User's credit is restored, he or she is automatically able to access the resource again. ClearTrust SecureControl automates these conditional access decisions so that no administrative intervention is required. Without the automation that ClearTrust SecureControl provides, you would be forced to manage permissions manually—a process that is time-consuming, expensive, and prone to security exposures.

Web Single Sign-on

Single Sign-On makes your website simple and convenient for Users—they need only a single password, which they are asked to provide only once. With ClearTrust SecureControl's Web Single Sign-On feature, Web Users can travel between protected servers on your company's domain without being required to log in and authenticate over and over again. Single Sign-On works across vendors and platforms so even if a User begins his or her Web session on a Netscape UNIX Web Server and moves to a Microsoft IIS server on NT, he or she only has to authenticate once on the first server. Single Sign-On is not only more convenient for Users but translates into substantial administration-based savings as Users place fewer password administration calls to your help desk.

You can set Single Sign-On sessions to prevent idle sessions and to enforce maximum session duration. Single Sign-On identities can also be passed onto Web Application Servers such as the Netscape Application Server, Net Dynamics, and Web Logic Tengah, thereby passing the User's identity transparently to backend Applications.

Scalablity

ClearTrust SecureControl uses a Java/Voyager architecture to ensure maximum scalability both in performance and redundancy. Objectspace's Voyager standard for distributed computing enables distributed software components to run across different servers and operating platforms. This allows ClearTrust SecureControl to be deployed on existing UNIX and Windows NT platforms and to be configured for redundant, highly available performance.

ClearTrust SecureControl is as scalable as the hardware on which it runs; there is no logical limit to the number of Users or resources it can manage. ClearTrust SecureControl was designed and built to scale and support millions of Users performing millions of transactions on a day-to-day basis and features sophisticated load balancing and clustering capabilities that ensure high performance.

Reliability and Fault Tolerance

ClearTrust SecureControl is designed to provide maximum reliability and availability and employs a sophisticated failover architecture to ensure that the security system is always available. ClearTrust SecureControl supports hot failover of multiple components and can be deployed in a clustered configuration. Because ClearTrust SecureControl is written in Java, its components can be deployed simultaneously across both NT and UNIX.

ClearTrust SecureControl improves scalability by allowing the security workload to be spread across multiple ClearTrust SecureControl servers. This load balancing ensures that the security system can scale across multiple machines. ClearTrust SecureControl can load balance across UNIX and NT servers simultaneously so existing hardware and server investments are leveraged.

Native Support for LDAP Directories

ClearTrust SecureControl provides extensive native support for LDAP directories. ClearTrust SecureControl's LDAP support goes far beyond simple User authentication. Through its LDAP support, ClearTrust SecureControl customers can centralize User information in the LDAP directory and leverage that data into access control policies managed by ClearTrust SecureControl. ClearTrust SecureControl provides plug-and-play integration with Netscape and PeerLogic Directory Servers.

ClearTrust SecureControl also supports integration of LDAP directories across the Internet to enable tightly integrated Extranets between trading partners. This allows companies to securely share User administration with trading partners, thereby improving security and lowering costs. ClearTrust SecureControl's native LDAP support lowers administration costs by eliminating the need for the redundant administration of User information.

Java and C APIs

ClearTrust SecureControl's Java and C APIs allow you to integrate your existing IT infrastructure with the ClearTrust SecureControl system so you can make the security services of ClearTrust SecureControl available to your whole enterprise. You can integrate enterprise databases, proprietary directories, and other systems into access control policies using the ClearTrust SecureControl API. For example, you can use the ClearTrust SecureControl API to programmatically load large numbers of Users and make sweeping security policy updates. You can also use the ClearTrust SecureControl API to extend ClearTrust SecureControl security policies to your non-Web Applications.

Auditing and Logging

Auditing refers to the tracking of both User activity and resource usage. With ClearTrust SecureControl's auditing and logging capabilities, you can track a User's activities over time. You can also track the usage of a resource by User to assess the potential vulnerability of that resource.

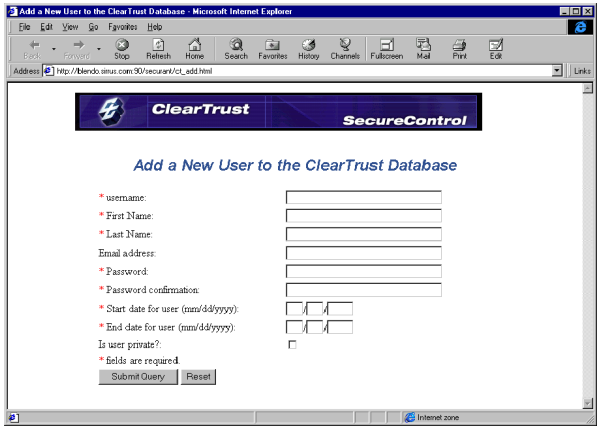
ClearTrust SecureControl provides extensive logging of User and Administrator activity as well as assessment tools to help you model security policy accurately. One major benefit of the ClearTrust SecureControl audit log is that it provides a single point to examine activity for all Users across UNIX and NT servers as well as Netscape, Microsoft,

and Apache Web Servers. ClearTrust SecureControl supports multiple levels of auditing granularity and allows for more comprehensive security audit data than is available from standard Web Server logs. You can view ClearTrust SecureControl audit logs through Microsoft Excel and Crystal Reports.

Administration

ClearTrust SecureControl includes administration client, written in Java, that enables security administrators to create users, establish security policies, and identify the resources that should be secured, among other features. In addition, you can administer security over the Web using the example Administration CGIs or Servlets that ship with the product (see Figure 1-1), or you can develop your own custom administration programs using the ClearTrust SecureControl API. For more information, refer to the *ClearTrust SecureControl Developer's Guide*.

Figure 1-1. Adding a New User via the Web (Using a Sample Administration CGI)



ClearTrust SecureControl Components

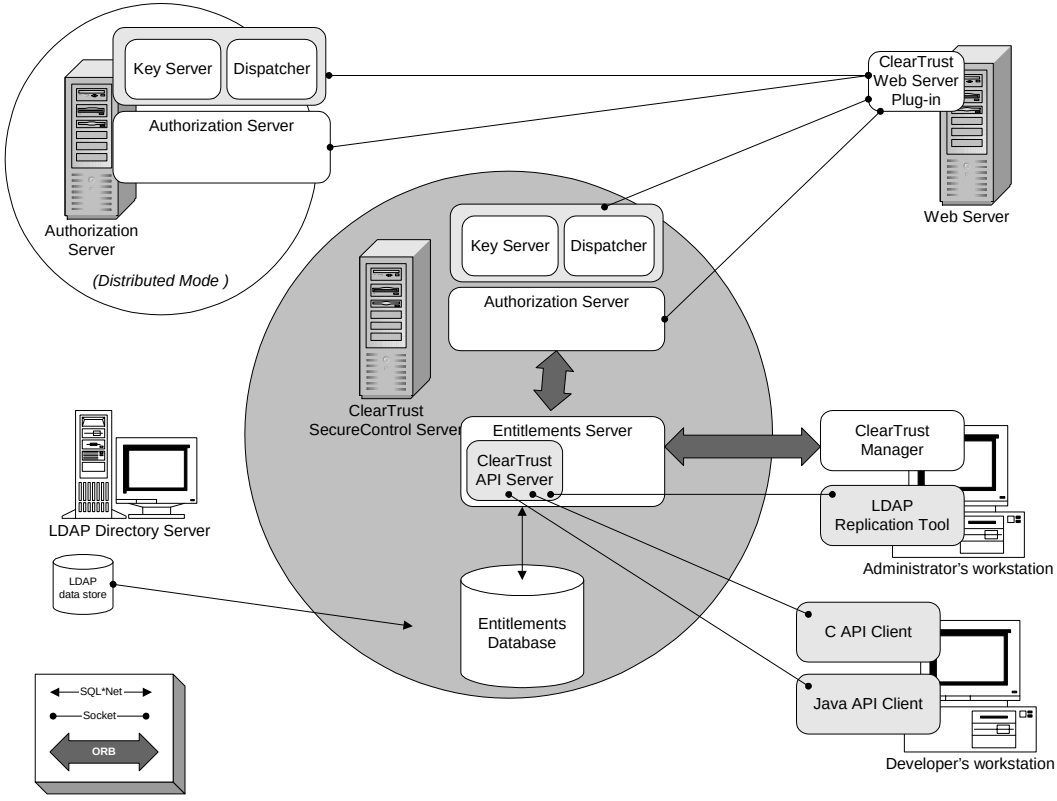
ClearTrust SecureControl is comprised of several key components that interact over TCP/IP networks using a variety of communications mechanisms (sockets, ORB communications, and database protocols; see Figure 1-2 on page 21). The software components encompass both administration and enforcement components:

- Administration components maintain the information in the Entitlements database and provide an interface by which to do so. These components include the SecureControl Manager, the LDAP Replicator Tool, the Java API client, and the C API client library.
- The enforcement or delivery group implements the security policies that an organization defines. These components include the ClearTrust SecureControl Servers (Entitlements, Authorization, and Dispatcher), the Entitlements database, and the ClearTrust Web Server Plug-ins.

Enforcement Components

- The Entitlements Server provides an interface to the database for ClearTrust SecureControl Manager.
- The Entitlements Database stores all of the information about Users, Applications, and their Entitlements. It is SecureControl's persistence mechanism.
- The Authorization Server determines permissions at run time. It interfaces with the Entitlements Database to determine whether a User has permission to access a given resource. The Authorization Server then provides the permission information to the Web Server Plug-ins. The Authorization Server employs extensive caching in order to deliver optimum performance.
- The Server Dispatcher provides information to the ClearTrust SecureControl Web Server Plug-ins about the availability of Authorization Servers. It enables the Plug-ins to choose a new Authorization Server at start-up or in the event of a failure. The Server Dispatcher also monitors the status of the Authorization Servers.
- Single Sign-On Key Server generates and distributes encryption keys to the Web Server Plug-ins. These keys are used by the Plug-ins to encrypt the cookies that ClearTrust SecureControl uses for Single Sign-On functionality. The Single Sign-On Key Server is integrated with the SecureControl Server Dispatcher.
- Web Server Plug-ins enforce ClearTrust SecureControl permissions on the Web Servers into which they are installed. ClearTrust Web Server Plug-ins interface to Netscape Web Servers through the Netscape Server Application Programming Interface (NSAPI); to Microsoft Web Servers through Microsoft's Internet Server API (ISAPI); and to Apache Web Servers through the Apache API (APAPI).

Figure 1-2. ClearTrust SecureControl Component Interaction



Administration Components

- ClearTrust SecureControl API integrates ClearTrust SecureControl functionality into other Applications. The API consists of two components: the API Server and the API Client. The API Server is integrated into the ClearTrust SecureControl Entitlements Server. The API Client is available in two versions: a Java Class library and a C library. The API Client provides an interface for Applications to maintain the information stored in the Entitlements Database.
- ClearTrust SecureControl Manager is a Java client Application used to administer the information about Users, Applications, and Entitlements stored in the Entitlements Database.

- The LDAP Replicator Tool replicates data from a Netscape or PeerLogic Directory Server into the Entitlements Database. This tool consists of two components: the Manager and the Agent. You use the LDAP Manager to configure the replication information; that is, how to connect to the Directory Servers, and how often to replicate, how to map LDAP attributes to ClearTrust SecureControl User Properties, and to define replication filters. The Agent carries out the replication.

Component Security

Creating a truly secure ClearTrust SecureControl system requires more than just protecting Web Servers. The communication between the different components must be secure, and sensitive information stored in the file system must also be protected. This section describes the different areas that need protection and the steps necessary to shield the system from attack. It also provides information on password storage and transmission across the network; it includes following sections:

- Inter-Component Security
- Oracle and Sybase Database Security
- Operating System Security
- Single Sign-On Cookie Security

Inter-Component Security

Inter-component security must prevent individuals from stealing information as it is passed over the network and ensure that someone cannot impersonate a ClearTrust SecureControl component and then steal information. Encryption prevents the “sniffing” of information as it is passed over the network, while authentication technology ensures data is only sent between trusted ClearTrust SecureControl processes.

Many ClearTrust SecureControl components communicate with one another across the network. Much of this communication is sensitive and must be secured from prying eyes. To protect the system from network eavesdroppers, ClearTrust SecureControl uses Secure Sockets Layer (SSL). The particular SSL modes vary from one component to another, but in all cases ClearTrust SecureControl uses 128-bit or better encryption for all messages sent across the network.

Inter-Component Encryption All data sent between ClearTrust SecureControl components is encrypted using Secure Sockets Layer encryption technology. Before transmission over the network, the data is encrypted. The particular SSL modes vary from one component to another, but in all cases ClearTrust SecureControl uses 128-bit or better encryption for all messages sent across the network. Within the SSL framework, encryption secures communications between the following components:

- Web Server Plug-in and Authorization Server
- Web Server Plug-in and Server Dispatcher
- Server Dispatcher and Authorization Server
- All ORB communications

Browser to Server Encryption For the Single Sign-On (SSO) system to work correctly, a *browser cookie* must be created by the Web Server Plug-In and sent to the browser. Because the cookie contains information about the User, ClearTrust encrypts the cookie before sending. All ClearTrust SecureControl protected Web Servers need to decode this cookie, which means they must all share the same key used to encode the cookie. The Server Dispatcher distributes the encryption key to all Web Server Plug-ins, ensuring the cookies are decodable and secure.

Note that the cookie encryption for SSO doesn't require SSL; SSL is used to encrypt Web site data, such as HTML files or CGI program output, or form input data, such as credit card numbers. The cookie encryption is specific to ClearTrust and is a separate process.

Plug-In to Server Dispatcher Authentication Before a Web Server Plug-in retrieves a new cookie encryption key from the Server Dispatcher, it must prove to the Dispatcher that it is a trusted ClearTrust SecureControl component. If this were not done, anyone could contact the Dispatcher and download the encryption key, allowing them to decode Browser Cookies and steal important User information. Each Plug-In is configured with a key generated by the *keygen* utility included with ClearTrust SecureControl. This key is passed to the Server Dispatcher when the Plug-In needs to retrieve a new cookie encryption key, authenticating the Plug-In to the Dispatcher. For details about using the *keygen* utility, see the *ClearTrust SecureControl Installation and Configuration Guide*.

User Passwords Each User in the ClearTrust SecureControl database may have a password. Other forms of authentication are available, but the default authentication mode is password checking from the ClearTrust SecureControl database. Whenever a password is passed over the network or stored on disk there is a risk that password may be stolen. In order to reduce the likelihood of password theft, ClearTrust SecureControl uses three different mechanisms:

- Passwords are converted into a form that makes the original password unrecoverable.
- Oracle or Sybase database security is used to prevent access to the ClearTrust SecureControl database.
- Operating system file permissions are used to prevent access to sensitive files.

Hashing Hashing converts a human-readable password into a string of 32 seemingly random characters. But these characters are not random: the same password always converts into the same 32 characters. Furthermore, the process can not be run in reverse: given a 32 character hash there is no way to retrieve the human-readable password. All passwords stored in the database are stored hashed.

Oracle and Sybase Database Security

Access to the database is tightly controlled. Only three database accounts are created during installation; the names and passwords for these accounts are stored in the `Default.conf` configuration file. Securant reommends that you don't create any additional database accounts, and that you change default passwords for any and all user accounts created by the database vendor's installation routine. For example, Sybase administrator (sa) has no password at installation, and Oracle uses default accounts for sys and system. You should change these immediately at installation.

Operating System Security

File permissions on the ClearTrust SecureControl directory tree should be very tightly controlled. Only grant access to the few individuals or Groups that absolutely need it; administrators alone should have access to the *Default.conf* configuration file. Set file permissions on the **"**Securant**"** directory tree as follows:

Windows NT: Domain Admins and System have Full Control; Revoke Everyone's access. All files and directories within the tree should be given the above permissions.

Solaris: Revoke all "Group" and "other" access by issuing the following command from the directory above the "Securant" directory:

```
chmod –R go-rwx securant
```

Single Sign-On Cookie Security

SecureControl also uses a browser cookie to provide Single Sign-On (SSO) functionality.

Server Side Protection To prevent anyone from intercepting and using the cookie, ClearTrust SecureControl encrypts the cookie with either 128-bit triple DES encryption or 128-bit Blowfish. The strength of this secret-key (symmetric) encryption is further enhanced by the ClearTrust SecureControl crypto-server which rotates the keys on a continually and configurable basis and communicates only across SSL secured channels to trusted and authenticated ClearTrust SecureControl Plug-ins. The SSL encryption prevents a malicious User from obtaining the public key in the first place and the key rotation makes the public key only usable for a limited period of time. Also, Web User passwords are never passed in the clear but rather are hashed using MD5 and only hashed passwords are stored in the ClearTrust SecureControl Entitlements database.

Client Side Protection The ClearTrust SecureControl cookie is protected on the client in these ways:

- The cookie is a session cookie (rather than a persistent cookie), so it's stored in browser memory only and not on disk, so malicious Users can't retrieve it for later use.
- The cookie contains IP address-specific information that is checked to see whether it is coming from the IP address that it was created for, preventing a malicious User from stealing the cookie and using it from another computer.
- The cookie has time-out settings that render it unusable after a determined period of inactivity, so if Users leave their computers while logged on, other Users won't be able to assume their sessions and access protected resources.

- The cookie has a maximum lifetime setting that forces a re-authentication when the time threshold is exceeded. The time out settings, both for maximum lifetime and inactivity, are set on a per Web Server basis. Different Web Servers can have different time outs and time out settings apply globally to a particular Web Server.

In addition to all these security aspects, you can also configure your Web Servers to run with SSL encryption turned on so that cookies are encrypted (along with all other communications) over the wire, between Web browser and Web Server.

Embedded Supporting Software Products

The following products are embedded in the ClearTrust SecureControl runtime system. Securant supports these components as part of the ClearTrust SecureControl environment; they are provided for use through license of ClearTrust SecureControl as part of the ClearTrust SecureControl deployment.

- Oracle WorkGroup Server or Sybase Adaptive Server Enterprise
- Objectspace Voyager v3.1
- WebLogic JDBC Kona for Oracle v.3.1
- Phaos SSL v1.1.1
- OpenSSL
- Sun Java Runtime Environment

The following subsections describe these products in more detail.

Oracle WorkGroup Server or Sybase Adaptive Server Enterprise

ClearTrust SecureControl supports WorkGroup Server v. 7.3.4 and Sybase Adaptive Server Enterprise v. 11.9.2. These Applications implement the ClearTrust SecureControl Entitlements Database, storing all ClearTrust SecureControl data, such as:

- Users
- Applications
- Entitlements
- Smart Rules
- Sub-Administration Policy

For more information on Oracle, visit http://www.oracle.com. For more information on Sybase, visit http://www.sybase.com.

Objectspace Voyager v3.1

The Objectspace Voyager standard is used for communications between ClearTrust SecureControl Manager and the ClearTrust SecureControl Entitlements Server, as well as between the Entitlements Server and Authorization Servers.

For more information, visit http://www.objectspace.com.

WebLogic JDBC Kona for Oracle v.3.1

The WebLogic JDBC Kona is used to provide connectivity to the Oracle database from the ClearTrust SecureControl Entitlements Server and ClearTrust SecureControl Authorization Servers.

For more information: http://Weblogic.beasys.com/index.htm.

SFL (Standard Function Library)

ClearTrust SecureControl incorporates functions from the iMatix SFL from iMatix Corporation. The iMatix SFL (Standard Function Library) is a portable function library for C/C++ programs. The SFL is written in ANSI C and has been ported to MS-DOS, Windows OS/2, several UNIX systems, including Linux, and Digital Open VMS. The SFL provides about 450 functions that cover the following areas: compression, encryption, and encoding; datatype conversion and formatting; dates, times, and calendars; directory and environment access; users and process groups; inverted bitmap indices; symbol tables; error message files; configuration files; string manipulation and searching; file access; Internet socket access; Internet programming (MIME, CGI); SMTP (email access); Server (batch) programming; and Program tracing.

For more information: http://www.imatix.com.

Phaos SSLava v.1.1.1

Phaos SSLava is used to encrypt the communications sent and received by the ClearTrust SecureControl Authorization Server, the ClearTrust SecureControl API Server, and the ClearTrust SecureControl Java API Client. The algorithms used are RC4/SHA, and the key length is 128-bit.

For more information: http://www.phaos.com.

OpenSSL

ClearTrust SecureControl was developed using encryption tools from the OpenSSL project. The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and open source toolkit implementing SSL and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library. OpenSSL is based on the SSLeay library. The OpenSSL toolkit is licensed under an Apache-style license.

For more information, go to http://www.openssl.org

Sun Java Runtime Environment

ClearTrust SecureControl Entitlements Server, Authorization Server, Server Dispatcher, and Java API Client run on the Sun Java Runtime Environment 1.1.7, the Java runtime virtual machine.

For more information, go to http://java.sun.com.

Support for Related Software Products

This section describes ClearTrust SecureControl's support for the following related software products:

- Web Servers
- LDAP Directories
- Certificate Authorities
- Authentication Servers
- Firewalls
- Application Servers and CGI Applications

Web Servers

The ClearTrust SecureControl Web Server Plug-in communicates with the Web Server through its API interface (NSAPI for Netscape Servers and ISAPI for Microsoft). Once installed, the Web Server Plug-in controls various stages of the Web Server's processes. For each request the Web

Server receives, the Plug-in checks if the requested resource is protected. If the resource is protected, the Plug-in authenticates the User and makes sure he or she has appropriate permissions.

- If the User has authenticated properly and has been granted has access permission to the resource by a ClearTrust SecureControl Administrator, the Plug-in allows the Web Server to return the requested resource.
- If the User fails to authenticate, or has not been granted permission to access the resource, the Plug-in forces the Web Server to return an appropriate message to the User.

LDAP Directories

The ClearTrust SecureControl LDAP Replicator Tool replicates and synchronizes User data stored in multiple LDAP Servers with the User data stored in the ClearTrust SecureControl Entitlements Database. The LDAP Replicator Tool currently supports the Netscape and PeerLogic Directory Servers and the LDIF file format. It utilizes the Directory Server's replication interface to duplicate any changes made to data in the Directory Server in the Entitlements Database.

Certificate Authorities

ClearTrust SecureControl does not interface directly with a Certificate Authority (CA). Instead, it leverages the Web Server's own certificate authentication code.

Authentication Servers

ClearTrust SecureControl supports multiple types of authentication, including SecurID (Security Dynamics token based system), NT logins, LDAP, and username/password. In addition, the ClearTrust SecureControl Web Server Plug-in can be extended to use other authentication schemes including Kerberos and custom built Authentication Servers.

Firewalls

ClearTrust SecureControl complements firewalls by providing authentication and access control to the resources that are accessed. ClearTrust SecureControl can be deployed on either side of a firewall, and

components can interoperate across a firewall. See the *Installation and Configuration Guide* for more information on running ClearTrust SecureControl across a firewall.

Application Servers and CGI Applications

ClearTrust SecureControl can be used to authenticate and authorize Users that wish to access dynamic content created by CGI programs and Application Servers such as NetDynamics, WebObjects, NAS, WebLogic, Bluestone, and Haht. In addition, features within these Applications can be protected by ClearTrust SecureControl through use of the ClearTrust SecureControl API. Refer to “Securing Resources” on page 71, for more information.

Chapter 2
ClearTrust SecureControl Data Model

To effectively use ClearTrust SecureControl, you must first understand how the system organizes the resources it protects. This chapter discusses how ClearTrust SecureControl provides a model for organizing and protecting resources by using access control functions. It includes the following sections:

- Overview of the ClearTrust SecureControl Data Model
- ClearTrust SecureControl Access Control Architecture
- ClearTrust SecureControl Administrative Architecture

Overview of the ClearTrust SecureControl Data Model

The ClearTrust SecureControl solution is built on a foundation of two distinct data architectures that let security administrators both define resource accessibility and administer security policy.

The ClearTrust SecureControl Data Model is comprised of the ClearTrust SecureControl Access Control Architecture and the ClearTrust SecureControl Administration Architecture.

The ClearTrust SecureControl Access Control Architecture provides a framework for determining which Users, or consumers, have access to protected resources. The ClearTrust SecureControl Administration Architecture provides a framework for securing access to the supporting database.

Figure 2-1 illustrates the ClearTrust SecureControl Data Model Architecture.

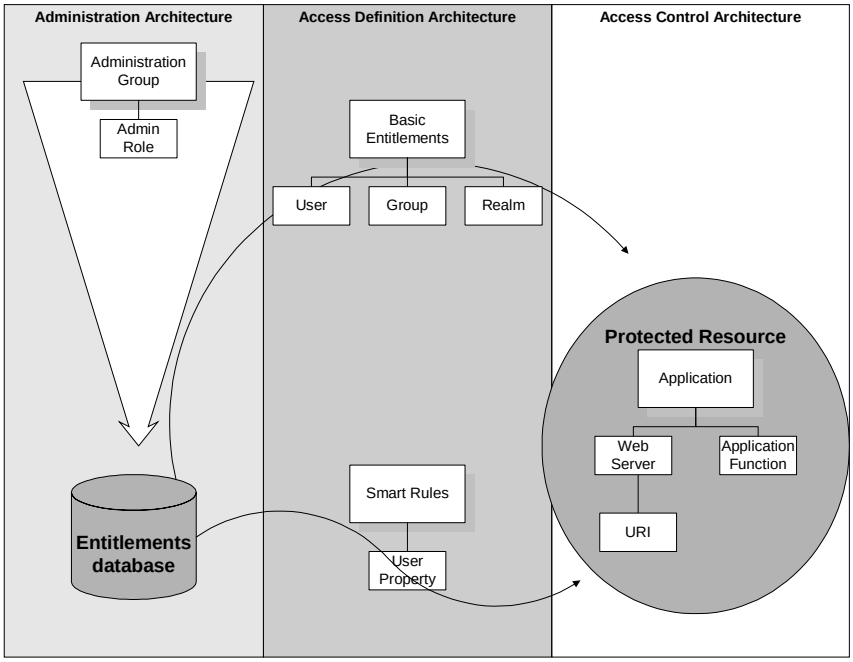


Figure 2-1. ClearTrust SecureControl Data Model

ClearTrust SecureControl Access Control Architecture

The ClearTrust SecureControl Access Control Architecture is divided into three components that constitute the basic building blocks of an access policy:

- Resource Consumer Architecture
- Access Definition Architecture
- Resource Definition Architecture

Resource Consumer Architecture

A resource consumer is an individual that accesses or manipulates a ClearTrust SecureControl defined resource. Thus, a resource consumer could be an employee that needs to retrieve sensitive documents, or a customer who wishes to modify his or her account information, or a supplier that needs to view or update factory floor data. Through the Access

Definition Architecture, you define the security policy that either grants or denies a resource consumer access privileges to a ClearTrust SecureControl resource.

The ClearTrust SecureControl Resource Consumer Architecture further branches out to the Consumer Architecture and the concept of Consumer Objects, Consumer Attributes, and Containers, Realms, and Groups. These are all discussed on the following pages.

Users and User Properties

The ClearTrust SecureControl Consumer Architecture is divided into a **consumer object model** and a **consumer attribute model**. A consumer object is referred to as a *User*. Users are the individuals that access ClearTrust SecureControl-secured Web-based resources via their Web browser or non-Web-based resources by way of a custom Application in an enterprise client/server environment.

A User has both fixed attributes and extensible attributes. Fixed attributes include User ID, first name, last name, and password, for example. Extensible attributes, which are referred to as *User Properties*, are attributes that you define specifically for your organization or for a department within an organization. For example, you may want to define a User Property called Account Status or Job Description. You only have to define a User Property once and it is automatically defined for each User in the database. Of course, you still have to input the value of the User Property for each individual User.

Example: A software company, Megasoft, has developed an Application allowing client companies to view their account information. Each company may have several points of contact that are allowed to access the account database. A ClearTrust SecureControl Administrator defines a User for each of the points of contact, adds each User to a Group that represents the client company, adds the Group to the Customer Realm, and defines a User Property Definition (Service Contract) of type Integer, which means the value can be equal to, less than, or greater than any integer you specify. Then the Administrator sets the Service Contract User Property value for each User.

You can also group Users together into *Groups* and Groups into *Realms* for simplified management. Groups and Realms are discussed below.

Groups and Realms

For organizations with hundreds or thousands of Users, administering security policy on an individual basis is both labor- and time-intensive. ClearTrust SecureControl lets you group Users together into Groups to simplify administration. A User can belong to any number of Groups. Any action applied to a Group, such as granting or denying access to a resource, is automatically applied to every User in that Group.

When you delete a Group, Users are no longer belong to that Group or have the security policy defined for that Group. When you delete a Group, however, you do not delete the individual Users in that Group. You must delete Users individually to remove the information from the ClearTrust SecureControl database and make them unavailable to the Administrator.

A Realm is a collection of Groups. As with Groups, when you apply an administrative action to a Realm is automatically applied to all the Groups within it and to all the Users in those Groups. A Group can belong to any number of Realms but a Realm cannot belong to another Realm. When you delete a Realm, however, you do not delete the individual Groups in that Realm. You must delete Groups individually.

Permission Overrides

Figure 2-2 illustrates the relationship among Users, Groups, and Realms.

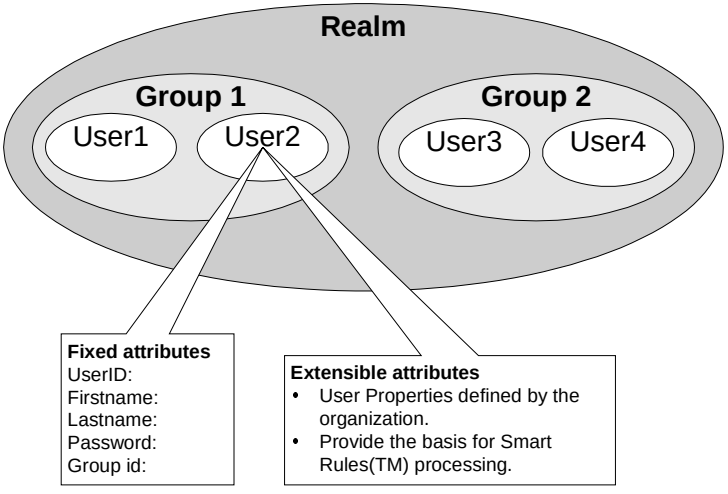


Figure 2-2. Realms Contain Groups; Groups Contain Users

ClearTrust SecureControl allows you to apply access permissions at the User, Group, and Realm levels. While this provides for simplified management in some cases, it can also lead to the possible conflict of permissions to a resource. For example, a conflict arises if User Andy has been granted access to the accounting resource but the Group he is a member of has been denied access to the same accounting resource. ClearTrust SecureControl handles these potential conflicts through the hierarchy of these three levels.

- Access permissions at the User level have priority over permissions at the Group and Realm level.
- Permissions at the Group level override permissions in the Realm level.

In this case, Andy does have access permission to the accounting resource since he was granted access at the User level. In short, the more specific the permission is, the more powerful the privilege. For more information about access policy, refer to Chapter 6.

Access Definition Architecture

The ClearTrust SecureControl Access Definition Architecture provides two ways to assign consumers access privileges to a protected resource: Basic Entitlements and Smart Rules.

Basic Entitlements

Basic Entitlements are similar to Access Control Lists (ACLs) and allow you to explicitly allow or deny access to a specific resource. You can define Basic Entitlements at the User, Group, or Realm level. If you assign Basic Entitlements at the Group or Realm level, they apply to all objects contained at that level. If a Group is given access rights to a resource through a Basic Entitlement, all the Users contained within the Group have access rights to the resource as well.

Like traditional ACLs, Basic Entitlements are an adequate but not truly flexible approach to defining access privileges. The limitation with these static approaches is that you have to manually assign and administer policy, making management more challenging and labor-intensive than with an automated methods. For organizations that want to automate security policy

management, ClearTrust SecureControl provides Smart Rules, a rules-driven method of defining access privileges. Smart Rules are described on the following pages.

Figure 2-3 illustrates the ClearTrust SecureControl Basic Entitlements access control, which explicitly specifies rights at the realm, group, or user level.

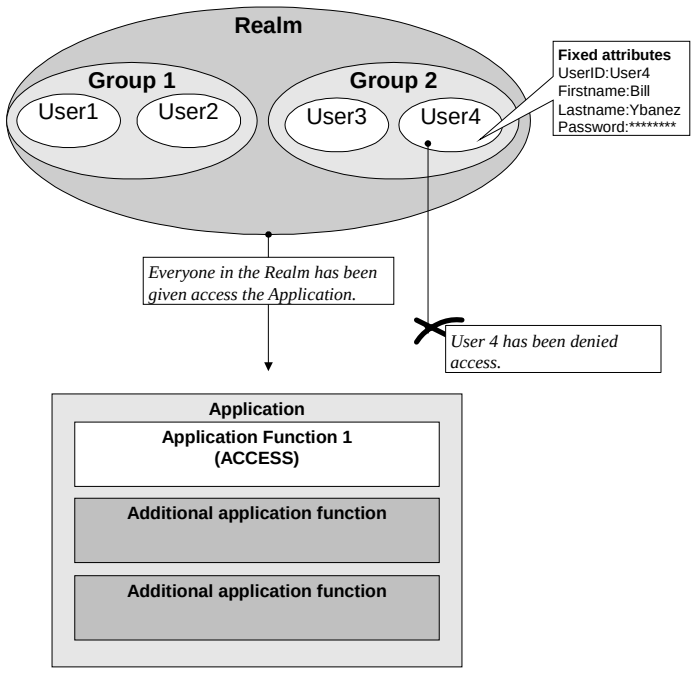


Figure 2-3. ClearTrust SecureControl Basic Entitlements

Smart Rules

ClearTrust SecureControl Smart Rules allow you to define accessibility rules for a resource rather than for a User. The accessibility rules are based on specific User Properties so that the Users allowed access to a resource may change from time to time but the criteria for accessing the resource remains the same. For example, you could grant access to a resource to Users if their account balance is at least $10,000 and their account is in good standing. The unique and powerful advantage of Smart Rules is that is either one of these User Properties changes, Smart Rules automatically adjusts access privileges accordingly. If a User's account balance drops below $10,000, for example, Smart Rules denies access.

Figure 2-4 illustrates the concept of Smart Rules.

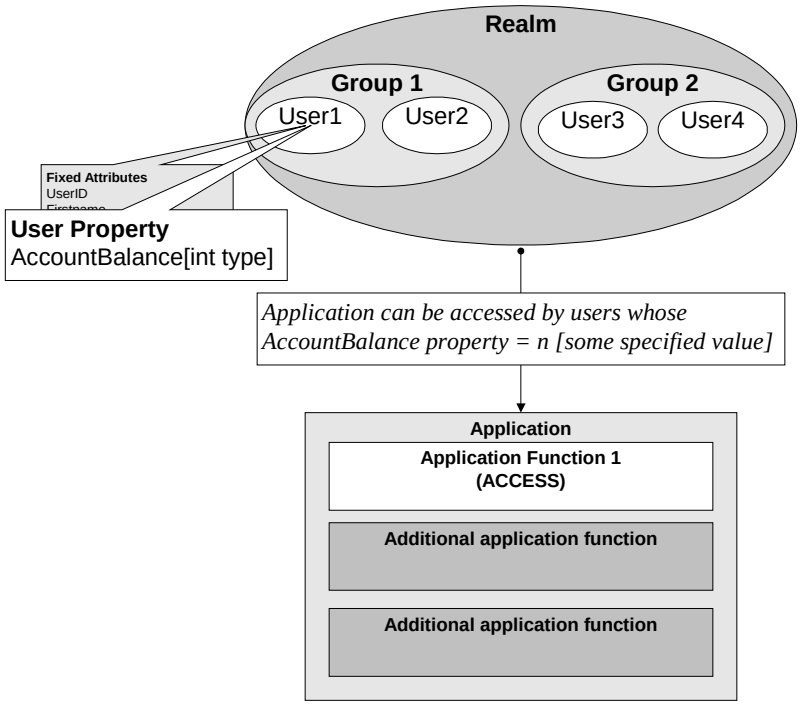


Figure 2-4. Smart Rule Access Control

With Smart Rules, you can create a powerful, flexible, and easy-to-understand security policy. As mentioned, Smart Rules are expressions that you create to define accessibility rules for a resource based on specific User Properties. These accessibility rules are ALLOW, DENY, and REQUIRE and User Properties, as you know, are definable values such as age, residence, account balance, job title, or credit status, of the User. The full expression then, includes one of these rules followed by a User Property. For example, to grant access to a resource to a User with an account in good standing, the Smart Rules expression looks like this:

ALLOW if Credit = Good

You can use your own organization's business rules to create customized Smart Rules expressions. You simply define a User Property and then create a rule that includes the specific value or criteria that Users need to meet in order for access to a resource. You can also combine the rules to create more sophisticated Smart Rules expressions.

ALLOW and DENY conditions are "OR'ed". That is, a user may be granted or denied access to a resource if one of the conditions is met. With REQUIRE conditions, Smart Rules can be grouped together to form compound accessibility definitions. REQUIRE conditions are "AND'ed" are used when there are compound properties that need to be met to satisfy the condition.

Smart Rules can be strung together to form complex expressions with one of three possible results:

- ALLOW—Gives the User access to the resource without any further rule processing, if the rule is satisfied.
- DENY—Denies the User access without any further rule processing if the rule criteria is met.
- REQUIRE—If the rule is satisfied, continues to the next rule to determine accessibility; however, if the rule isn't satisfied, denies the User access. If all the REQUIRE rules are satisfied, User access is granted.

Since ALLOW and DENY are mutually exclusive rules, ClearTrust SecureControl provides a mechanism to allow you to specify whether ALLOW or DENY takes precedence. This tells ClearTrust SecureControl which conditions to process first. Refer to Chapter 6 for a more thorough discussion of how to define and use Basic Entitlements and Smart Rules.

Resource Definition Architecture

The Resource Consumer Architecture and the Access Definition Architecture gave a brief overview of how ClearTrust SecureControl defines Users, Groups, Realms, and User Properties as well as the different ways you can define access privileges for these Users. This section discusses the ClearTrust SecureControl concept of resources, Applications, and Application Functions so that you can define what resources you want

to secure. The same way ClearTrust SecureControl allows you to group Users together for simplified management, it also allows you to group resources together. These concepts are discussed on the following pages.

Figure 2-5 illustrates how resources, Applications, and Application Functions interact in the ClearTrust SecureControl Unified Access Management (UAM) system.

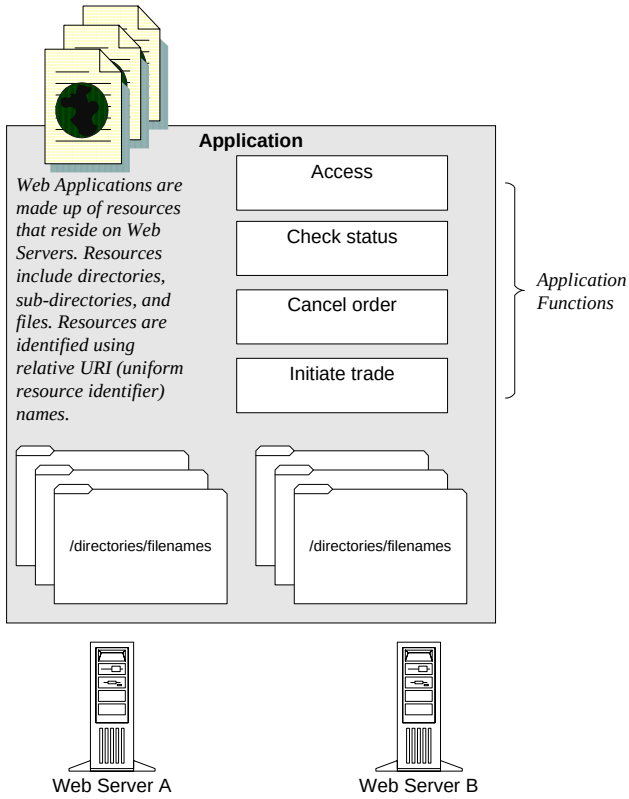


Figure 2-5. Applications, Resources, and Application Functions

Applications

As mentioned, ClearTrust SecureControl uses the term resources for any files, directories, or other information that you want to protect or secure. You can group or organize related resources together into Applications for simplified management and for unique identification within ClearTrust

SecureControl. For example, you can group all of your Human Resources administration pages into an Application called HRAPPS in order to grant access privileges only to HR personnel.

Uniform Resource Identifiers (URIs)

In ClearTrust SecureControl, a Web-based Application is comprised of *Uniform Resource Identifiers* (URIs). The URI of a Web-based Application is associated with and owned by a ClearTrust SecureControl-defined Web Server. The Web Server name identifies the location of a resource and the location of the ClearTrust SecureControl-enabled Web Server. ClearTrust SecureControl applies the name of the Web Server in the ClearTrust SecureControl database to the actual Web Server. The URI and its associated Web server are considered a *Uniform Resource Locator* (URL). Thus, when a ClearTrust SecureControl-enabled Web Server receives a request for a standard Web URL, the resource tested for access permissions is a combination of the URL's URI and the name of the ClearTrust SecureControl-enabled Web Server.

Application Functions

When you create an Application, the ClearTrust SecureControl Manager assigns it the default Application Function, ACCESS. ACCESS is a top-level Application Function but you can also create other levels of Application Functions for each Application to determine what a User can do or what tasks they can perform once they have accessed an Application. Thus, Application Functions provide granular transaction authorization.

Within each Application, you can define any number of Functions. For example, in the HRAPPS Application, Application Functions might include tasks like "Provide Employment Verification" or "Job Postings". You may only want certain HR personnel to have access to employee records to use when outsiders call to confirm employment so you would deny access of the Application Function, "Provide Employee Verification", to certain employees. And it may be up to only one employee to manage recruitment so you could grant access to the Application Function, "Job Postings", only to that User. Thus, for each Application Function you define, you assign access privileges.

The security policies you define for Application Functions are not used by the Web Server Plug-in, however, but are used by your Application and are queried using the ClearTrust SecureControl API. The ACCESS Application Function of the referenced Application determines accessibility to the requested URL.

Example: Megasoft's customer account Application has varying functionality depending on the client's service contract. Consequently, Megasoft wants all their customers to be able to access the Application but they want their system to return an interface supporting only the level of functionality that matches the client's service contract. To do this, a ClearTrust SecureControl Administrator creates an Application: CustomerAccountApplication. Next, the Administrator defines the URI of the Application, `/customeraccountapp.cgi`, and a Web Server object that owns the Application: CustomerWebServer. The Administrator then defines Application Functions representing the various interfaces to the CustomerAccountApplication. The Administrator associates either a Smart Rule or a Basic Entitlement with the ACCESS Application Function and each additionally-defined Application Function.

When a User requests the CustomerAccountApplication, the ClearTrust SecureControl-enabled Web Server processes the ACCESS function to determine accessibility to the Application. Once a User is granted access, Megasoft's Application uses the ClearTrust SecureControl API to query the different application functions determining the respective functions the User may access.

Resources and Resource-Naming Conventions

Web-Based Resources

ClearTrust SecureControl manages access privileges to a wide range of Web-based resources or Universal Resource Identifiers (URIs). These resources may be Web pages or Directory Trees of Web pages that contain HTML or CGI. ClearTrust SecureControl lets you group together these Web-based resources to provide access control at multiple levels of granularity.

ClearTrust SecureControl provides a natural directory-based naming scheme for identifying individual Web-based resources. This naming scheme can be added explicitly to the Application. ClearTrust SecureControl uses a variation of the standard URL naming scheme used in the World Wide Web to identify these resources to the system.

The location of a Web resource consists of the following:

- The location of a particular Web Server.
- The location of the resource within that server's document tree.

A standard World Wide Web URL identifies a file or directory residing on some Web Server. A ClearTrust SecureControl URL identifies a file or directory residing on a ClearTrust SecureControl-secured Web Server in a completely different way. It identifies Web Server objects. Identifying Web server objects is described later in this chapter.

Non-Web-Based Applications

As mentioned, ClearTrust SecureControl also manages non-Web-based application. Non-Web-based Applications do not contain resources directly, rather, they represent a group of resources implicitly. There is no standard way to identify individual non-Web-based resources. Instead, a ClearTrust SecureControl Application itself defines the resource(s) being protected implicitly.

Identifying Web Server Objects in ClearTrust SecureControl

With ClearTrust SecureControl you can simply Web Server administration by creating a symbolic name for each Web Server you want to protect. You can use the ClearTrust SecureControl Manager or the ClearTrust SecureControl API to define an *object* that identifies your Web Server rather than using a standard DNS name. This way, a single ClearTrust SecureControl-defined Web Server can logically represent multiple physical Web Servers.

The URI for a single page takes the same form as in the World Wide Web, `/dir1/dir2/page.html`. The URI for a set of pages grouped in a Directory Tree is the directory path followed by the string `/*`, for example, `/dir1/dir2/*`. For example, in Figure 2-6, the URI, `/markets/*` on Web Server, *Kiva Server*, has just been added to the Application *Emerging Markets*.

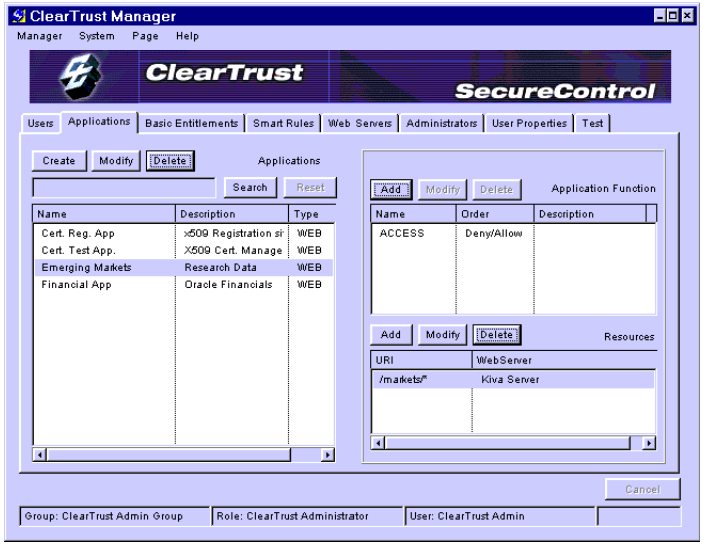


Figure 2-6. Adding Resources to Applications

Since a ClearTrust SecureControl Web resource can be a Directory Tree of Web pages, it is possible for one resource to *contain* another. For example, the resource `/*` on Web Server X includes all of the pages of the resource `/foo/*` on that same server. Because these are distinct resources, they may be added to different ClearTrust SecureControl Applications without violating the restriction that two Applications cannot contain the same resource. In all such cases, authorization privileges to any page contained in the sub-tree are determined solely by policies involving the sub-tree's Application. In Figure 2-7, the Finance application (FinanceApp) includes the resource `/*`, while the Human Resources Application (HRApp) includes `/foo/*`

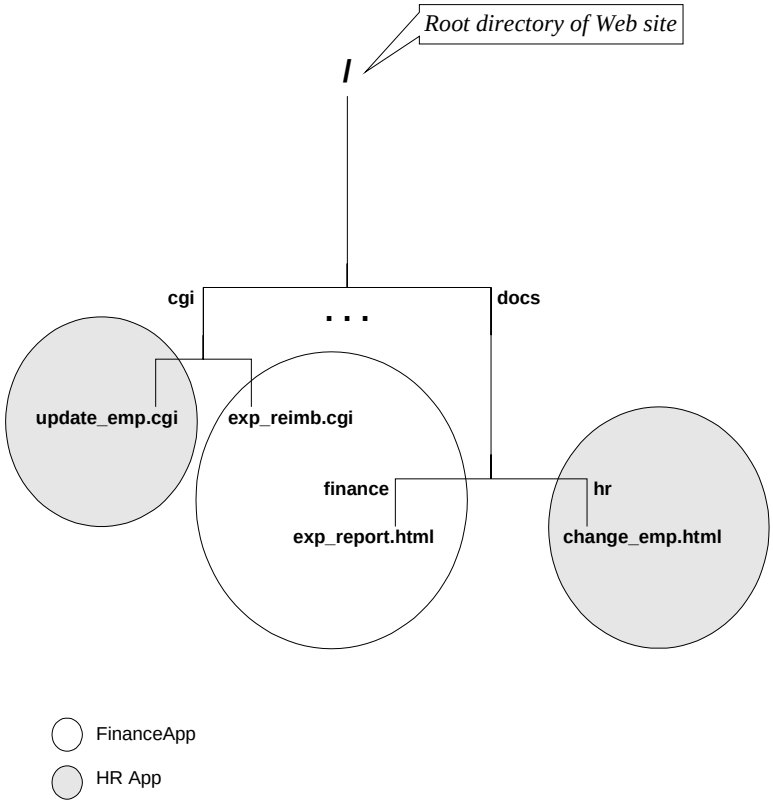


Figure 2-7. Nested Web Resources.

ClearTrust SecureControl does not interfere with your Web Server's environment variables in any way. CGI programs running on ClearTrust SecureControl enabled Web Servers run just as they normally do, with the exception being that you can secure them more tightly. In particular, the REMOTE_USER environment variable will be set properly, in case your CGI should behave differently depending on the User.

ClearTrust SecureControl Administrative Architecture

ClearTrust SecureControl's Administrative Architecture is a flexible model for defining ownership and administrative responsibilities of ClearTrust SecureControl objects. *Administrators* are Users with special functions and privileges. In an on-line banking Application, the bank's customers are regular Users but the bank employees that manage ClearTrust

SecureControl are Administrators. For details about how you assign Users to Administrative Groups, see “Setting up Delegated Administration” on page 105.

Figure 2-8 illustrates how Users and Administrators are Grouped into different hierarchies.

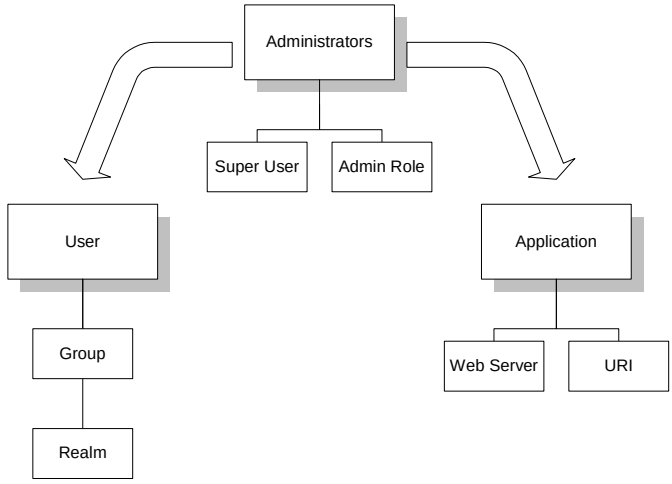


Figure 2-8. ClearTrust SecureControl Administration Hierarchies

Administrative Groups

The concept of ownership lets you delegate security policy administration within the ClearTrust SecureControl environment. You can segment protected objects by geographical location (for example, North America), organizational structure (for example, Marketing), or other groupings that are logical for your particular organization. When you segment protected objects as such, you can then assign an Administrator to each segment. The segment being administered is called an Administrative Group and an Adminisrator owns only his or her Administrative Group.

Administrative Roles

An Administrative Role is a set of Administrator capabilities or privileges within an Administrative Group. For example, an Administrator may be limited to modifying only Users and User Properties within the North American Administrative Group.

Example: Megasoft is using ClearTrust SecureControl to protect its external customer account Application but they are protecting their internal Human Resource information as well.

To manage administration of the ClearTrust SecureControl database, Megasoft defines two Administrative Groups:

Customer Administrative Group and HR Administrative Group.

Next, Megasoft defines two Administrative Roles, Customer Admin Role and HR Admin Role, giving each Administrative Role a full set of administrative privileges.

With an overview of the architecture and the fundamental workings of ClearTrust SecureControl Manager, you can begin creating policies and administering security for your enterprise.

Chapter 3
Using SecureControl Manager

The ClearTrust SecureControl Manager is the tool you'll use when working with ClearTrust SecureControl policy managment infrastructure. ClearTrust SecureControl Manager is a Java-based client application that installs on Windows NT or Solaris, and lets you create Users, Groups, Realms; identify the Web Servers and other resources you wish to secure; setup security policies across all applications; create Administrative groups to which you can delegate responsibility for specific administration tasks for select resources, and perform most of the other tasks covered in the remainder of this guide. This chapter contains information about:

- Logging on to ClearTrust SecureControl Manager
- Using the ClearTrust SecureControl Manager User Interface
- ClearTrust SecureControl Administration Task Summary

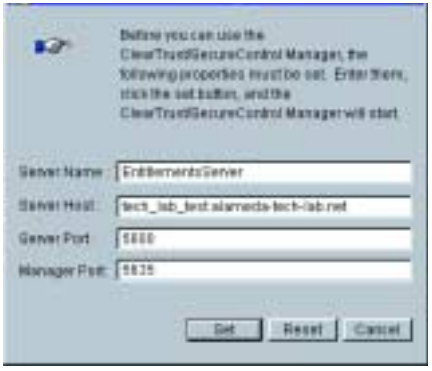
Logging on to ClearTrust SecureControl Manager

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

IMPORTANT: ClearTrust SecureControl installs with one default administrator account that you can use for initial logon. 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 on to ClearTrust SecureControl Manager:

1 From the Windows Start menu, select Programs, then ClearTrust Manager, to launch the ClearTrust Manager software. The first time you run this application, the ClearTrust SecureControl Configuration dialog displays so you can identify the location of the ClearTrust SecureControl server you want to manage:



2 In the Server Host field, enter the hostname (or the IP address) of the server that is running the Voyager daemon. You can leave all the other fields unchanged. Click on the Set button to continue. In a few seconds, the logon and password dialog displays:

3 Enter your UserID and Password and click the Login button to continue. The first time you launch the Manager application, however, you'll logon using the default administrator account (admin) and password, also admin.

—If you've already used the ClearTrust Manager and created additional Adminstrative Groups or Roles, a dialog displays prompting you for the Administration Role Choice.
—If you have not defined any Administrative Groups, you will automatically be logged on as a member of the default ClearTrust SecureControl Admin Group. In this case, the Administration Role Choice dialog does not appear; the ClearTrust SecureControl Manager window opens directly from the logon dialog.

4 Select the Administrative Group and Role under which you want to log on. You may be a member of more than one group, but you can log on only as a member of one group at a time, and you'll have only the privileges attached to that Administrative Group and Role.

In a few seconds, the ClearTrust SecureControl Manager graphical user interface displays. The key features of the ClearTrust Manager are discussed in the next section.

Using the ClearTrust SecureControl Manager User Interface

As shown in Figure 3-1, the ClearTrust SecureControl Manager consists of tabs, a menu bar, and various buttons that comprise typical windowing system GUIs. Starting from the upper-left-hand corner of the figure, the Manager menu lets you Exit the program entirely, or Logoff only, so you can logon again using another Admin account.

The System menu has a Flush Cache selection which updates the ClearTrust SecureControl run-time servers with new data as you change it using the Manager. 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.

The Page menu option provides a drop-down list of all the tabs that comprise the Manager; this is simply an alternative method for moving from tab to tab. The Help menu provides online information about using the Manager.

The status bar at the bottom of the window shows at a glance the Administrative Group, Administrative Role, and User account under which you're logged on at any given time.

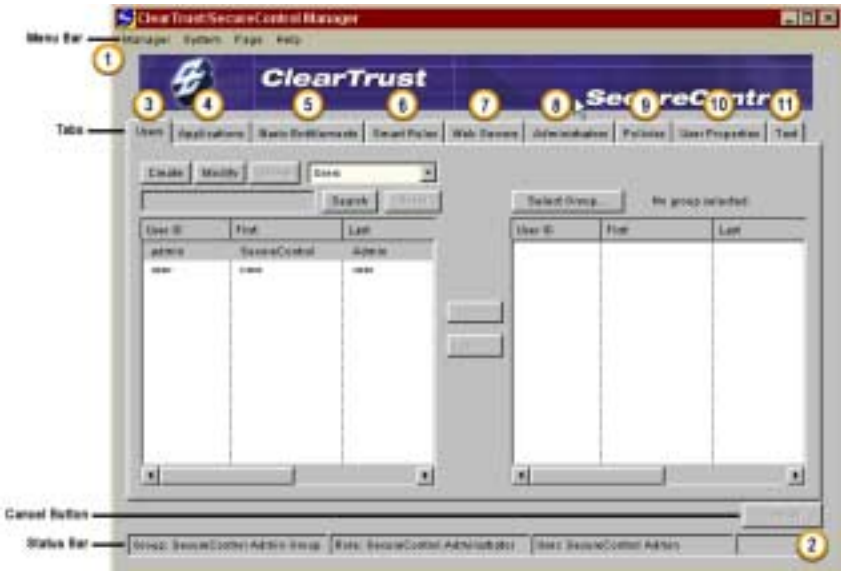


Figure 3-1. ClearTrust SecureControl Manager Window

The tabs that comprise the Manager are designed to flexibly handle each of the key functional security administration areas of the ClearTrust SecureControl system.

3 **Users** - Define Users, Groups, and Realms. For details, see Chapter 4, “Creating Users, Groups, and Realms.”

4 **Applications** - Define Applications and Application Functions and assign resources to Applications. For details, see Chapter 5, “Securing Resources.”

5 **Basic Entitlements** - Define mechanisms for granting or denying access privileges. See Chapter 6, “Defining Runtime Access Control.”

6 **Smart Rules** - Define mechanisms for defining access privileges based on logical rules involving the values of User Properties at run time. For details, Chapter 6, “Defining Runtime Access Control.”

7 **Web Servers** - Create ClearTrust SecureControl-enabled Web Servers and server trees. For details, refer to Chapter 5, “Securing Resources.”

8 **Administrators** - Define Administrative Groups and Administrative Roles; assign privileges to Administrative Roles and populate Administrative Groups with Users. For details, refer to Chapter 7, “Setting up Delegated Administration.”

9 **Policies**- Define Password policies that are associated with Administrative Groups and edit individual User passwords.

10 **User Properties** - Define User Properties, which are custom properties that you create in addition to the fixed attributes you specify each time you add a User to the ClearTrust SecureControl database. For details, refer to Chapter 4, “Creating Users, Groups, and Realms.”

11 **Test** - Simulate a specified User attempting to access a specified Web Server in order to test your security policies. For details, see “Testing Access Permissions” on page 102

The **Cancel** button activates when an action is in progress; you can click the **Cancel** button to cancel all cancellable requests.

Typically, you won’t be using any of the functions in a linear fashion. The nature of security administration is that it is an on-going process, as the user community and the resources they need to access evolve over time. Nonetheless, the next section provides some overall planning guidance.

ClearTrust SecureControl Administration Task Summary

The following list offers a logical way to set up a SecureControl security policy system:

1 **Planning Ahead**—Identify the resources (Web sites, URIs, Applications) that you want to secure. Identify the users that should access those resources and think about logical groupings of users with common needs; from these you can create 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 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.

2 **Setting up Delegated Administration**—Define Administrative Groups and Administrative Roles and assign Users to Administrative Groups.

3 **Creating Users, Groups, and Realms**—Define User Properties as needed and create Users, Groups, and Realms. Create user accounts for all Users to whom you want to provide access. You can import users from LDAP

directories by using the LDAP Replicator Tool; see the *Installation and Configuration Guide* for information about installing and using the LDAP Replicator. You can also create a batch load program by using the ClearTrust API; see the *Developer's Guide* for details.

4 **Defining Web Servers**—Define Web Servers. Create Server Trees if you want to delegate adminstration of specific resources to select VBUs. Create Applications, add resources to Applications, and change ownership of Applications to meet your needs.

5 **Defining Runtime Access Control**—Define Basic Entitlements and Smart Rules, and simulate implementation of your defined security policy to determine whether it is functioning as you intended.

6 **Testing Access Permissions**—Simulate Users requesting access to various resources to test the security policies you have defined.

7 **Auditing**—View ClearTrust SecureControl Manager activity logs.

Chapters 4-8 provide step-by-step instructions for performing these tasks.

Chapter 4
Creating Users, Groups, and Realms

This chapter tells you how to define User Properties and how to add Users, Groups, and Realms to your ClearTrust SecureControl database. It includes the following sections:

- Creating, Modifying, and Deleting User Property Definitions
- Creating, Modifying, and Deleting Users
- Creating, Modifying, and Deleting Groups
- Creating, Modifying, and Deleting Realms
- Searching for Users, Groups, or Realms

NOTE: Before entering any data, be sure to map out Users, Applications (accessible resources), and the conditions you want to use to determine whether or not a particular User can access a particular resource. Define User Properties *before* you create User accounts so you can enter values for these properties as you create Users.

Background Concepts

As you begin administering your ClearTrust environment, be aware of the following requirements:

- At least one Super User must exist at all times. By definition, the default 'admin' user account is a Super User.
- Only a User who is a member of an Administrative Group can be identified as a Super User.

- You must be logged on as Super User to perform some of the activities covered in this chapter, in particular, transferring ownership of any entity— User Property Definition, User, Group, and Realm—from one Administrative Group to another.
- Only Super Users can "lock out" a User. Locking out a user immediately disables all permissions that the user might have on protected resources.
- By default, User Properties, Users, Groups, and Realms are public, which means that all Administrative Groups can see these entities and the values they contain. When creating or modifying any of these entities, you can make them private by clicking the "Private" box on the associated create or modify dialog box. Private means that only the Administrative Group that created the entity can access or manipulate the entity.
- Password characteristics (expiration date, minimum length, and other policies) are determined by the password policy associated with the Administrative Group (VBU) that owns the User.

Creating, Modifying, and Deleting User Property Definitions

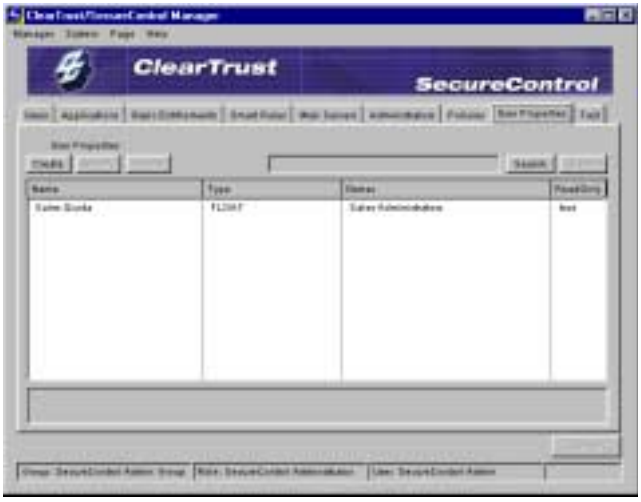
When you first create Users, you assign them certain *fixed attributes*, including UserID, First Name, Last Name, and Email Address. Alternatively, you can define and assign custom *User Property Definitions* upon which to base access through *Smart Rules*—conditional rules that determine access.

For example, you could create a User Property called "Account Balance" that could store the value of a banking customer's account balance and create a SmartRule that would permit or deny access if the value is above a specified threshold. See *"Defining Smart Rules" on page 98* for additional details. If you plan on implementing Smart Rules for access, for convenience sake you should create the User Properties upon which the rules will depend first, as described in this section.

These instructions presume you'll be implementing SmartRules in your ClearTrust SecureControl environment.

To define User Properties:

1 In the ClearTrust SecureControl Manager window, click User Properties to open the User Properties tab:



2 Click the Create button to display the Create User Property Definition dialog:

3 Enter a name for the property.

4 From the drop-down Property Type list, select the type of data that the user property can contain. Once you save this User Propery, you won't be able to change the type so choose carefully; allowable types are shown in the table:

TABLE 4-1: User Property Types

Type	Description	Example
BOOLEAN	A true or false value	Define a boolean user property to indicate if a user is a current depositor or not, if a user is an internal or external user, if a user is a customer or not, or any other true/false distinction.
STRING	A character string	Define a string property indicating the metropolitan area in which the User resides
INT	An integer	Define an integer property corresponding a series of User levels and perform tests such as User=1, User<=3, User >2, and so on
FLOAT	Floating point decimal property	Account balance, credit limit, or any other real number.
DATE	A date	Define a date property indicating the date on which the User set up his or her account at the client company

5 Mark the User Property private if you want this property to be accessible to your Administrative group only.

6 Select Read Only for the User Property if you want the field values to be read only.

7 Select Help Desk if the property will be manipulated by anyone in the Help Desk role.

—If you're a Super User and you want to transfer ownership of this User Property to an Administrative Group other than the one displayed, you can 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 User Property and redisplay the Create an Create User Property Definition dialog box.

8 Click **Save** to save the User Property Definition. A User Property Definition field corresponding to the property you defined is immediately created for all Users in the system.

To modify or delete User Property Definitions:

1 In the ClearTrust SecureControl Manager window, click User Properties to open the User Properties tab.

2 Select the User Property Definition you want to modify by clicking on the appropriate property in the pane on the left side of the tab. When you select a User Property, the Modify and Delete buttons become active.

——To delete the User Property, click on the Delete button. The User account is deleted, and the User account is also deleted from any any Groups and Administrative Groups with which it is associated.

3 Click Modify to open the Modify User Property Definition dialog:

4 Modify the User Property Definition. You can modify the name, description, and the ownership security settings (private, read only, help desk), but you cannot modify the property type.

5 Click Save to save your changes and return to the User Properties tab.

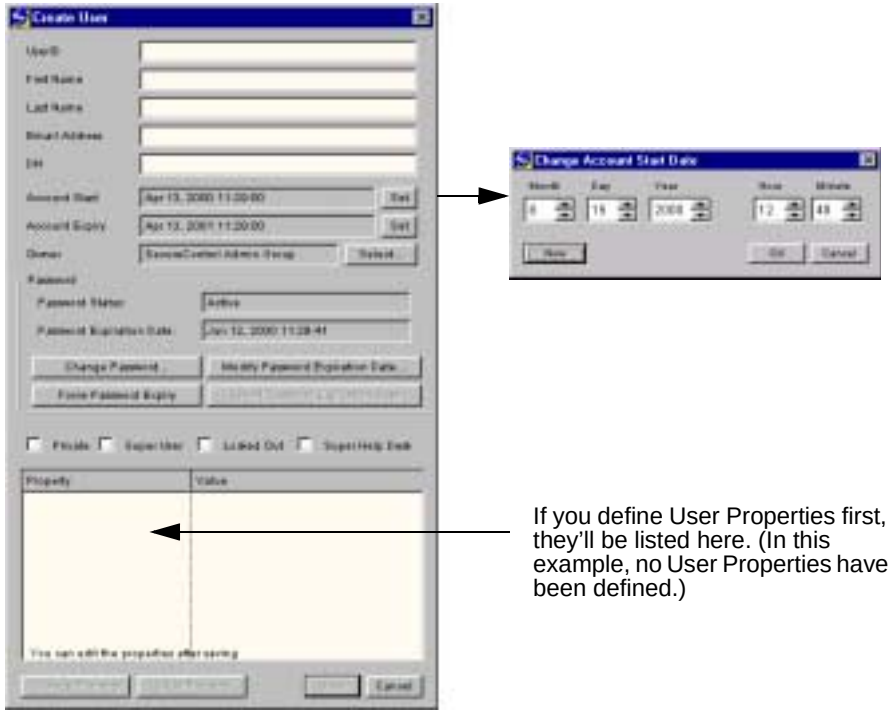
Creating, Modifying, and Deleting Users

This section tells you how to create, modify, and delete Users. The ClearTrust User account is the starting point for access control. To accesss any ClearTrust protected resource, one must have a ClearTrust SecureControl User account. Access control will be based either on a fixed attribute (for Basic Entitlements) or a custom attribute (User Property, for Smart Rules). At a minimum, you must give a User a UserID. If you want to use SmartRules, you should create the appropriate User Properties first, before creating Users as described in this section.

To create a User:

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

2. Select Users from the pull-down list near the upper-middle of the tab.
3. Click on the Create button to display the Create User dialog box:



4 Enter a name for the User account 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 properties as needed for your organization. You can also change any of the default settings. The remaining steps below discuss most of the buttons on the Create User dialog box, but you can also refer to Table 4-2 for information about defaults and usage.

NOTE: All password values are determined by the password policy associated with the VBU (virtual business unit; also known as the Administrative Group—see "Background Concepts" on page 105 for additional information).

TABLE 4-2: User Account Settings

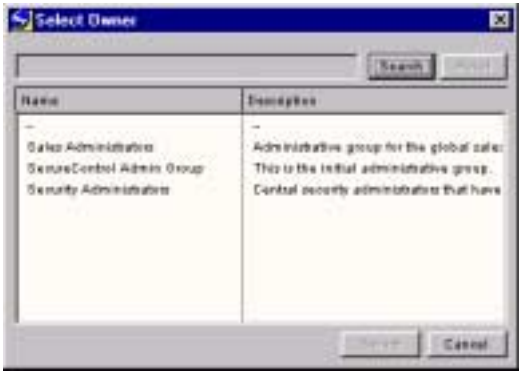
Field names	Description	Usage note
UserID	Login ID for the User	Required
First Name	User's first name.	Optional

Field names	Description	Usage note
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.The default settings for the account start and expiration dates by clicking the Set button to the right of the Account Start field to open the Change Account Start Date dialog. Use the pull-down Month, Day, Year, Hour, and Minute fields to select start date and time. Alternatively, you can 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
Owner	Administrative Group that owns the User account	Default is the Administrative Group
Password status	Indicates whether the password is *active* or has *expired*.	
Password expiration date	The default password, ch4nge_me is automatically set when you create a new user through the SecureControl Entitlements Manager. This password is inactive, however, if the force_password_expiration parameter is set to *true*. If this parameter is *not* set to true, the password is active for the period of time specified in the password lifetime of the Password Policy associated with the Administrative Group that created the User.	The Expiration field indicates the expiration date. The default lifetime of a password is determined by the password policy associated with the VBU that owns the User.
Change password		
Force password expiry		
Private	Identifies the User account as private; only the owning Administrative Group will be able to view this User.	Default is public. Private User can only be seen and manipulated by an Administrator in the same Administrative Group as the Administrator who created the User.

Field names	Description	Usage note
Super User	This checkbox is only enabled if you're logged on as a Super User. Super Users can perform any action on any User, Group, Realm, or Application.	Assign with caution. Must be an Administrator.
Locked Out	Immediately disables any permissions granted to the User.	Only Super Users can enable this feature. Use if you want to block a User immediately from accessing a protected resource.
Super Help Desk	Enables help desk personnel to change or reset passwords across all VBUs	User identified as Super Help Desk must also be members of an Administrative Group.
Change Property	Displays a Modify User Property dialog box that enables you to change the attributes of a User Property (except for its Type, that is, boolean, float, and so on).	Click on a User Property to highlight its name, and then click on Change Property to display the dialog box and change values.
Clear Property		Highligh the User Property name in the list and click on the Clear Property button to erase the value displayed.

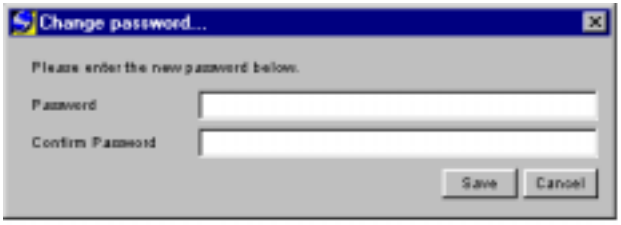
6 You can click on any Set button you see next to a field to display a date and time setting dialog box and change the values according to your needs.

7 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, you can 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.



—Click Select to transfer ownership to the selected Administrative Group.

8 Click the Set Password button to display the Change Password dialog box:



9 Enter the Password.

10 Re-enter the password in the Confirm Password field.

11 Click Save to save the password and return to the Users tab.

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 automatically expire the password.

12 You can 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 VBU default password expiration date has been overridden.

13 You can select the Revert Password Expiration button to revert back to the original password expiration.

14 Mark the User as Private, Super User, or Super Help Desk (or all three) by selecting the appropriate checkboxes. See Table 4-2 for additional information about these choices.

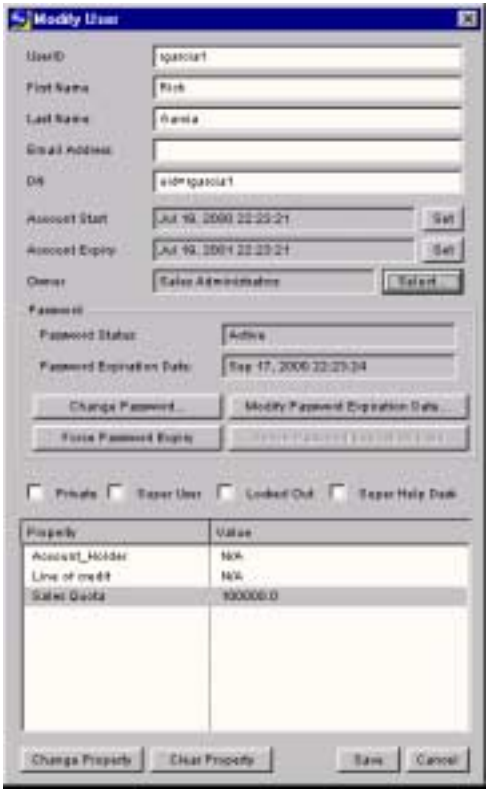
To modify or delete a User account:

1 Select Users from the pull-down list in the Users tab.

2 Select the User you want to modify or delete by clicking on the appropriate name in the User pane on the left side of the tab. When you select a User name, the Modify and Delete buttons become activated.

—To delete the User, click on the Delete button. The User account is deleted; the User account is also deleted from any any Groups and Administrative Groups with which it is associated.

3 To change any of the fixed attributes or user properties for the User account, click on the Modify button. The Modify User dialog displays.



4 Modify the User's fixed attributes in the text fields provided at the top of the Modify Users dialog.

5 Modify any of the User Properties by selecting the name from the list in the lower portion of the dialog box. You can:

- Change the User Property Definition value by clicking on the Change Property button to display a dialog box that lets you change the value of the selected property.

- Clear a User Property so that no value is displayed by clicking on the Clear Property button.

6 Click Save to save the new settings and return to the Users tab.

Creating, Modifying, and Deleting Groups

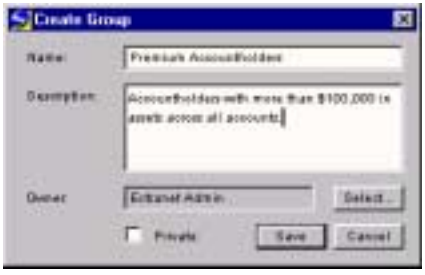
To streamline your administration tasks, you can organize Users that have similar access needs into a group—a collection of users—and then assign Basic Entitlements to the group rather than individual Users. This section tells you how to create, modify, and delete Groups.

To create a new Group:

1 Click Users in the ClearTrust SecureControl Manager window to open the Users tab.

2 Select Groups from the pull-down list near the upper middle of the tab.

3 Click Create to open the Create Group dialog box:



4 Enter the Name for the Group (required) and a description.

—If you're a Super User and you want to transfer ownership of the group to an Administrative Group other than the one displayed, you can click the Select button (next to the Owner field) to display the Select Owner box and select the Administrative group from the list. Click Select to save the change and exit the dialog box.

5 You can mark the Group as private by selecting Private checkbox. A private Group can be seen and manipulated only by an Administrator within the same Administrative Group as the Administrator who created the Group. Groups are created as public by default.

6 Click Save to save the Group and return to the Users tab. The Groups you create are listed on the left side of the Users tab when Groups is selected from the pull-down list.

Once a group is created, you can add users to it (see below), change its attributes, or delete it.

To modify the group's attributes (or delete a group entirely):

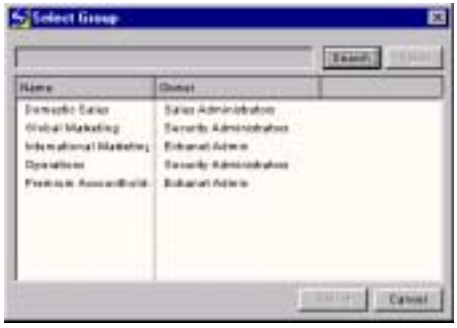
1. Select Groups from the pull-down list in the Users tab.
2. Select the Group you want to modify from the pane on the left side of the tab by clicking on its name. The Modify and Delete buttons become active.

   —If you want to delete the group, click the Delete button. You'll be prompted to confirm that you want to delete the group. Click Ok to proceed; the group is deleted.
3. Click the Modify button to open the Modify Group dialog; you'll see all the settings for the group as it was initially created.
4. Modify any attributes for the Group as needed.
5. Click the Save button to save your changes and return to the Users tab.

Creating a group simply creates the name of the group and ownership attributes; users don't belong to any group until you add them to the group, as described in the next section.

To add Users to the Group:

1. Select Users from the pull-down list in the Users tab.
2. Click Select Group to open the Select Group dialog:



3. Click on the name of the Group to which you want to add Users. If the list of groups is lengthy and you don't see the name displayed, you can click on the Search button and enter the name of the group in the Search dialog box. Search results will display in the Select Group Dialog; click Reset to return to the list of all Groups.

4 Click Select to Select the Group and return to the Users tab.

5 Select the Users you want to move into the Group from the table on the left side of the tab.

6 Select multiple Users by holding down the <Ctrl> key while clicking on the User name.

7 Click the right arrow (-->) to move the selected Users into the Group. Similarly, you can remove any users from the Group by clicking on the name or names in the right-hand pane and then clicking the left arrow (<--) arrow.

Creating, Modifying, and Deleting Realms

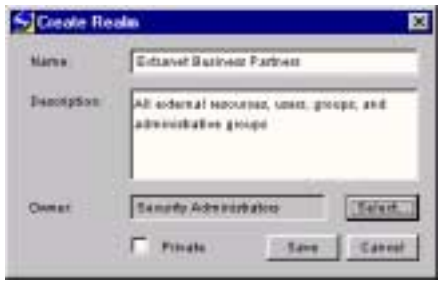
Just as using Groups can help you manage Users with common access needs, a Realm—a collection of Groups—can help you manage access rights for groups with similar needs. This section tells you how to create, modify, and delete Realms.

To create a Realm:

1 Click on the Users tab in the ClearTrust SecureControl Manager window to display the Users tab.

2 Select Realms from the pull-down list near the upper-left-side of the tab. Any existing Realms that are visible to your Administration group will display.

3 Click Create to open the Create Realm dialog:



4 Enter a name for the Realm. You should also add a meaningful description.

—If you're a Super User and you want to transfer ownership of the group to an Administrative Group other than the one displayed, you can click the Select button (next to the Owner field) to display the Select Owner box and select the Administrative group from the list. Save the change and exit the dialog box.

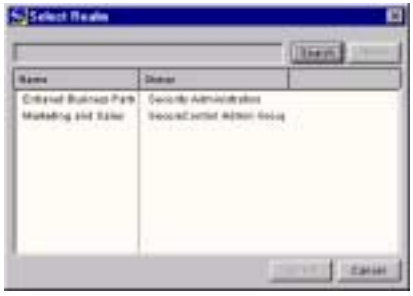
5 You can mark the Realm as private by selecting the Private checkbox. A private Realm can be seen and manipulated only by an Administrator within the same Administrative Group as the Administrator that created the Realm. Realms are created as public by default.

6 Click Save to save the definition of the Realm and return to the Users tab.

The Realms you create are listed on the left side of the Users tab when Realms is selected from the pull-down list. Once you've created a new Realm, you can then add Groups to the Realm.

7 Select Groups from the pull-down list in the Users tab.

8 Click Select Realm to open the Select Realm dialog:



9 Select the Realm to which you want to add Groups by clicking on its name in the list. If the list of Realms is extensive, you can search for the Realm by name by clicking on the Search button and then entering the Realm name in the dialog box that displays. The search results will display in this dialog; click Reset to close the dialog and redisplay the complete Realm list.

10 Click Select to select the Realm and return to the Users tab.

11 Select the Groups you want to move into the Realm from the table on the left side of the tab. Use the <Ctrl> key to select multiple groups. When you select any groups, the right arrow (-->) becomes active.

12 Click the right arrow to move the selected Groups into the Realm.

To modify or delete a Realm:

1 Select Realms from the pull-down list in the Users tab. A list of Realms displays in the left-hand pane.

2 Click on the Realm to highlight its name. When you do, the Modify and Delete buttons become active.

—Click on the Delete button to delete the Realm; the Realm is deleted from any Administrative Groups (VBUs).

3 Select the Realm you want to modify from the table on the left side of the tab.

4 Click Modify to open the Modify Realm dialog. This dialog is similar to the Add Realm dialog.

5 Modify the Realm's attributes.

6 Click Save to save your changes and return to the Users tab.

Searching for Users, Groups, or Realms

Use the Search button on the Users tab to search for a particular User, Group, or Realm by fixed attributes or User Properties. This feature is particularly useful when you have a large database of Users.

To search for a specific User, Group, or Realm:

1. In the ClearTrust SecureControl Manager window, click Users to open the Users tab.
2. In the pull-down list box in the upper right of the tab, select the type of entity—Users, Groups, or Realms—for which you want to search.
3. Click the Search button to open the Query User, Query Group, or Query Realm dialog. From the Query Group and Query Realm dialogs, you can search only by name.

4. Set up the search. You can search by fixed attributes, User Properties, or both. To search by fixed attributes, click on the Set button to the right of the attribute by which you want to search to open the Set Query for Attribute dialog box. This screenshot shows searching on the Last Name attribute:

5 Define the search by setting the Criteria and entering a Value.

6 Click Apply to save the search criteria; the Query User dialog box displays. You can repeat this process to add criteria to your search.

7 To set up a search by User Properties, follow these steps:

8 In the table of User Properties at the bottom of the Query User dialog, select the User Property Definition by which you want to search.

9 Click Set Property Query to open the Set Property Query dialog. This dialog is similar to the Set Query for Attribute dialog.

10 Use the Criteria and Value fields to define the search.

11 Click Apply to save the search criteria and return to the Query User dialog.

12 Repeat these steps to add criteria to the search.

13 From the Query User dialog, click Search to initiate the search. You can stop a search by clicking the Cancel button to the right of the Search button.

NOTE: The Cancel button is also useful if you have moved the scroll bar from top to bottom with a larger Users table and do not want to wait for the program to scroll through the list of Users.

When the search is complete, the system redisplays the Users tab. The search criteria is listed to the left of the Search button and the Users matching the search criteria are listed in the left panel. To revert to the list of all Users, click the Cancel button to the right of the Search button.

Chapter 5
Securing Resources

This chapter tells you how to create ClearTrust SecureControl Web Servers and Applications and how to add resources and Application Functions to the Applications you create. It includes the following sections:

- Creating, Modifying, and Deleting Web Servers
- Creating, Modifying, and Deleting Server Trees
- Creating, Modifying and Deleting Applications
- Defining Application Functions

For a more detailed discussion of the concept of ClearTrust SecureControl Web Servers, Resources, and Application Functions, see to “ClearTrust SecureControl Data Model” on page 31.

Background Concepts

The ClearTrust SecureControl Application is the central organizing concept for securing resources. Before you can create an Application, you must identify to the system the Web Servers that contain any resources you plan to secure. (You can also can delegate administrative tasks for specific server directory trees on any Web server to specific Administrative Groups. Administrators from these groups will then create the Applications and configure security.)

Within the Application tab of the ClearTrust Manager tool, you then create a name for the Application, identify the Application Functions that you want to enable, and select specific URIs that you want to secure. This section tells you how to create, modify, and delete Applications. Before getting into the details of using the ClearTrust Manager tool to do this, here’s a brief introduction to some of the background concepts.

How ClearTrust Maps URIs and Application Resources

When you create Applications by following the instructions later in this chapter, you'll need to enter URI (uniform resource identifier) names for the Web Server locations that you want to comprise the Application and to which you'll be configuring access controls. ClearTrust has specific rules for defining URIs as part of an Application:

- Any specific URI can be defined as a member of a single Application only: The same URI cannot be added to more than one Application.
- URIs from different Applications can overlap.
- URIs that comprise a single Application can span multiple Web Servers, as long as the Administrator is a member of the Administration Group that owns the Web Servers and the respective URIs.

Access to all other resources on the Web Server, regardless of whether explicitly specified as part of one of these Applications, must also be controlled.

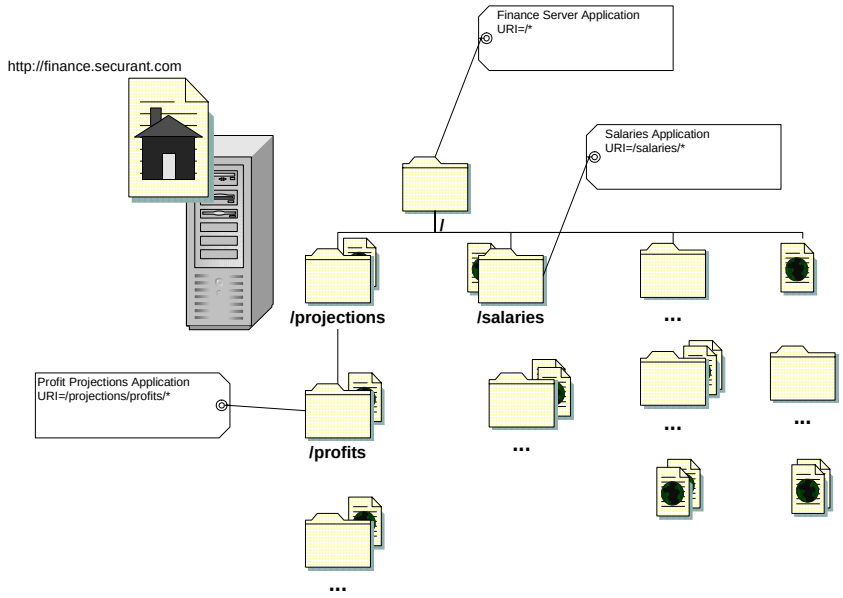
For example, say you have three Applications as shown in Figure 5-1:

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

The tags identifying the Applications in Figure 5-1 contain the URI that was entered in ClearTrust SecureControl when creating the Application.

As shown in the figure, the Finance Server Application subsumes all the sub-directories beneath the root directory (/), but as long as the contained entities aren't listed as part of this Application, that's okay.

FIGURE 5-1: A URI Can Only be Part of a Single Application



Both the Profit Projections and Salaries Applications overlap the definition of the Finance Server Application. What will happen when a User tries to access a URI that matches more than one Application? Which entitlements will be enforced?

ClearTrust SecureControl matches the actual URI a User tries to access with the most explicit Application URI that fits. Table 5-1 illustrates how some explicit URI access attempts would be interpreted by the system.

TABLE 5-1: How ClearTrust SecureControl Handles Overlapping URIs

URI	Most explicit	Application
/projections/profits/	/projections/profits/*	Profit Projections
/projections/spending/	/*	Finance Server
/salaries/executive.html	/salaries/*	Salaries
/salaries/slack/bob.gif	/salaries/*	Salaries
/salaam.html	/*	Finance Server

In this example, a single User defines each Application and all resources that comprise the Applications reside on the same server. Although it's usually best to keep related resources together whenever possible, some Applications may span multiple Web Servers or different parts of the same Web Server, so ClearTrust enables you to enter as many URIs as necessary when creating an Application.

Dynamic Content

Within ClearTrust SecureControl, you can usually treat server-side programs and scripts like any other Web content. If a CGI, Active Server Page, or something similar falls under one of the URIs for your Application, it will be part of the Application. Like any other content, you can enter the full name of your script or program instead of using a wildcard. 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

However, for dynamically created URIs—CGIs or any other server-side program that appends data to the URL at submission time (using GET, for instance)—you should use wildcards. Use an asterisk at the end of the URI you define in ClearTrust SecureControl. For example, to enable access to a URL such as:

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

you must define the ClearTrust SecureControl URI as:

`/budget/today.cgi/*`.

The same holds true for any dynamically generated content. If you won't know some or all of the content, you should protect the directory containing the automatically generated pages and images by using the wildcard in the URI. For example, if all of your automatically generated content is in a directory called `/results/daily/` on your Web Server, add the URI `/results/daily/*` to your Application.

Server Redirection

Sometimes you may want the ClearTrust SecureControl protected Web server to redirect a User's browser to another page. For example, if authorization fails you may want to redirect the User's browser to a login or help page.

HTTP allows a Web Server to refer the browser to a different page. Refer to the documentation that came with your Web Server to see how to configure it to perform redirection in the event of an error.

You can also configure the ClearTrust SecureControl Web Server Plug-in to redirect a User's browser to different locations in the event of authorization failure. You can configure ClearTrust SecureControl to return different HTML pages, depending on the reason for the authorization failure. For example, the system can return a customized denial error page, with particular reasons for denial, when a User is denied access. For more information on redirecting the User's browser, see the *Installation and Configuration Guide*.

Protecting Web Server Mapped Documents

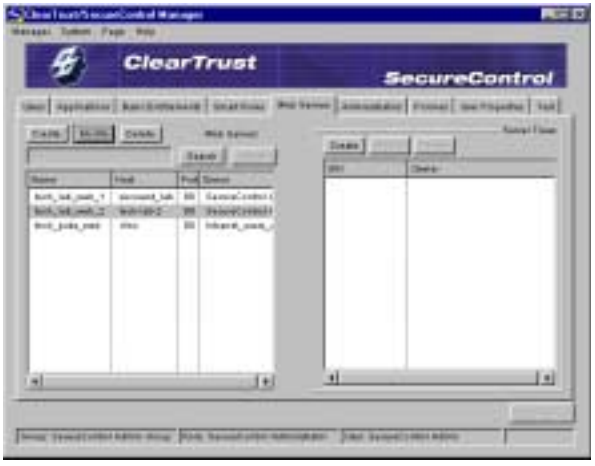
Web Servers typically have a default page that displays when you enter a URL. For example, entering http://www.acme.com in a Web browser will usually display the page `index.html`, located in the default document directory of the Web Server. To protect the default document (index.html) or any other documents that have been mapped to multiple URI reference points, be sure to define both resources for the Application. For this example, you'd specifically define both `/` and `/index.html`.

Creating, Modifying, and Deleting Web Servers

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 *ClearTrust SecureControl Installation and Configuration Guide* for additional information.)

To create a Web Server entry:

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



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

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 this table:

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 "Web Server;" 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 logon account is a member of will display. If you're logged on as a Super User, you can transfer ownership to another group if necessary.

4. You can 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. You can now identify Server Trees on this Web Server that will be managed by different Administration Groups (see "Creating, Modifying, and Deleting Server Trees" below), and you can also create Applications that include this Web Server (see "Adding Resources to Your Applications" on page 81).

   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.

To modify or delete a Web Server:

1. Select the name of the Web Server in the Web Servers pane (the left-hand area) and then click the Modify... (or the Delete button).
2. You can change the ownership of the Web Server (to delegate control to a different Administration Group), and you can change any of the resources (directory trees) associated with the Web Server at any time from the Web Servers tab.

   Be sure to Save your changes before exiting the Web Servers tab, and update the cached information on the Authorization Servers by selecting "Flush Cache" from the main menu.

Creating, Modifying, and Deleting Server Trees

These instructions presume that your organization delegates administration of different web resources to different Administration Groups.

When you create a Web Server (see *"Creating, Modifying, and Deleting Web Servers"*) access to the server is controlled by either the Administrative Group under which you were logged on when you created the server or by the Administrative Group to which you transferred ownership for that Web Server. You can also divide up resources on a Web Server into Server Trees and specify different Administrative Groups, or owners, for these trees. This allows different Administrative Groups to manage different resources on a single Web Server.

Server trees are inclusive—the URI `/marketing/applications/*` contains everything in the `/applications/`directory.

Since a Server Tree on a Web server is comprised of the resources of a specific Administrative Group, Administrators can only manage URIs in their own Group. If you try to add another Administrative Group's URI to an Application in your Group, the system sends you an error message indicating that you do not have authority to add this URI to your Application.

To create a Server Tree:

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

2 Click the Create button above the Server Tree pane on the right side of the Web Servers tab to open the Create new tree dialog box:

3 Enter the URI (uniform resource identifier) and a description of the Directory Tree information. You can also transfer ownership of the directory tree to another Administrative Group and mark the directory tree as Private if it makes sense to do so for this particular directory tree.

4 Click Save to save the Server Tree. The tree is now listed in the Server Trees pane of the Web Servers tab.

To modify or delete a Server Tree:

1 Select the Directory Tree by clicking on its name in the Server Tree pane of the Web Servers tab. When you highlight a Directory Tree name, the Modify and Delete buttons become active.

—If you want to delete the Server Tree, click on the Delete button.

2 Click the Modify button above the Server Trees pane to open the Modify Tree dialog.

3 Change the Server Tree information as needed.

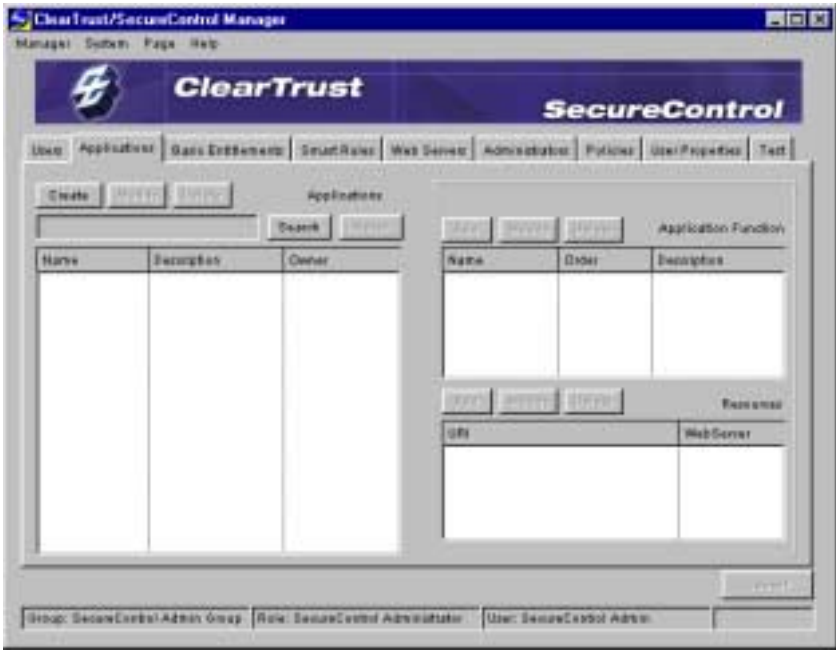
4 Click the Save button to save your changes and return to the Web Servers tab.

Creating, Modifying and Deleting Applications

These instructions presume that Web Servers have already been identified and created as detailed in “Creating, Modifying, and Deleting Web Servers” on page 75; to create an Application, you must identify resources that comprise the Application from the list of available Web Servers. You must be a member of the Administrator Group that owns the Web Server (or Web Servers) that comprise the Application. If not, you won’t see them in the listed Web Servers.

To create a new Application:

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



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

3 Enter a meaningful name for the Application in the App Name field. The Application name is 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.

—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 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.

5 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.

6 Click the Save button to save the Application. The server is now listed in the Applications pane on the Applications tab. You can add resources and functions to the Application as described in the following section.

To modify or delete an Application:

1 Select the Application by clicking on its name in the Applications pane on the Applications tab. When you select an application, the Modify and Delete buttons become active.

—To delete the Application, click on the Delete button. You'll be prompted to confirm that you want to delete the Application. Click on the Ok button if you want to proceed, and the Application is deleted. Or click the Cancel button to cancel.

2 To modify the Application attributes, click on the Modify button to open the Modify Application dialog box.

3 Change the Application information.

4 Click on the Save button to save your changes and return to the Applications tab.

Adding Resources to Your Applications

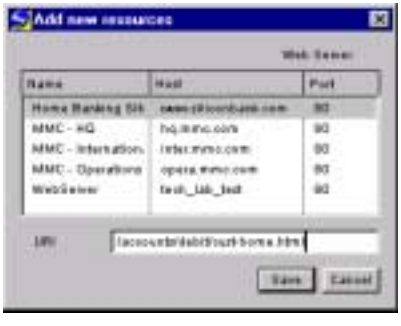
Resources are the specific URIs of each Application.

To add resources to an Application:

1 Click the Add button on the Applications tab (above the Resources pane) to display the Add new resources dialog box.

2 Highlight the name of the Web Server that contains the resource you'll be securing.

3 Enter the name of URI in the field. You can enter the complete URI, as shown in the screenshot, or you can enter a wildcard to secure everything under directory path:



NOTE: Entering /* as the URI of a Web Server defines all resources under the root directory as resources of the Application. Only those with ACCESS permission will be able to access URIs under /*, unless they've been given explicit rights to specific URIs.

4 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.

Defining Application Functions

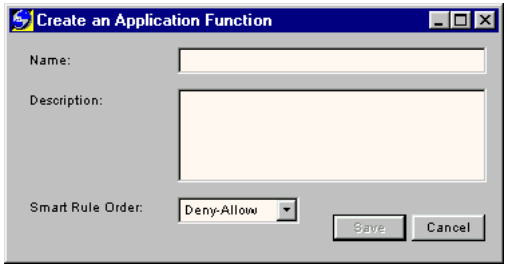
When you create an Application, ClearTrust SecureControl automatically creates the default Application Function, ACCESS. ClearTrust SecureControl-enabled Web Servers use this Application function to determine access to a requested resource. You can define a security policy controlling whether or not a User can access the Application. Additionally, you can implement *granular authorization* down to the function level, controlling different functions within the same Application in different ways. In order to take advantage of granular authorization, your software developer must use the ClearTrust SecureControl API to query Application Functions that define security policy for more than simple access.

You can use ClearTrust SecureControl Manager to create Application Functions that your developer uses for custom applications. You can then define Smart Rules that control access to a Web Server's resources based on custom User Properties or Basic Entitlements.

These instructions presume your organization is using the ClearTrust API to create custom Applications.

To define an Application Function:

1. Click Applications in the ClearTrust SecureControl Manager window to open the Applications tab.
2. Click the Add button above the Application Function pane in the Applications tab to open the Create an Application Function dialog:



3. Enter a Name for the Application Function. Software developers must refer to this name when querying security policy through the ClearTrust SecureControl API.
4. Enter a description of the Application Function; this is for information only.

5 Select the Smart Rule order for the Application Function. Smart Rule order is the order in which a Smart Rule based on this Application will be applied:

Deny-Allow or *Allow-Deny*. If Smart Rules conflict (for example, one rule allows access while another denies access), the **Smart Rule Order** specifies which rule takes precedence.

6 For more information about how ClearTrust SecureControl prioritizes multiple Smart Rules defined for a single Application Function, see “Combining Smart Rules” on page 93

—If you’re a Super User and you want to transfer ownership of the Application Function to an Administrative Group other than the one displayed, you can 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 Function and redisplay the Create an Application Function dialog box.

7 Click **Save** to save the Application Function and return to the Applications tab. The function you created is now listed in the Application Function pane:

To modify or delete an Application Function:

1 Select the Application Function you want to modify from the Application Function panel on the Applications tab.

2 Click the Modify button above the Application Function pane to open the Edit an Application Function dialog. This dialog is the same as the Create an Application dialog.

3 Change the Application Function information.

4 Click Save to save your changes and return to the Applications tab. The modified Application Function is listed in the Application Function panel.

5 Select the Application Function you want to delete from the Application Function panel on the Applications tab.

6 Click Delete above the Application Function panel to delete the Application Function.

Chapter 6
Defining Runtime Access Control

This chapter tells you how to define runtime access control using Smart Rules and Basic Entitlements. It includes the following sections:

- Background Concepts
- Defining Basic Entitlements
- Defining Smart Rules
- Testing Access Permissions

Background Concepts

Active and Passive Mode

Before using the Manager to configure entitlements as detailed in this chapter, you should be aware of whether your ClearTrust environment is configured for *active* or *passive* mode. Depending on this mode, the scope of your job in creating Applications will be greater or lesser. Moreover, access to any resource not explicitly defined as part of an Application (see Chapter 5) will depend on how the authorization server mode is configured.

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.)

Active mode means that only those resources with an associated Application Function are protected: If you don't define an Application and associate an Application Function (such as ACCESS, the default Application Function)

with a specific URI (even if it's an entire directory or sub-directory) for the Application, the resource (such as a Web page) will display when users enter its URL.

In passive mode, every resource is protected, whether or not it's defined as part of an Application. To provide access in this mode, you must expressly configure each resource, including .gif files that make-up part of an HTML page, for example, 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.

Either way, however, any resource that's protected will require either a Basic Entitlement or a Smart Rule for access permissions; these are introduced in the next section.

What is Runtime Access Control?

Runtime access control determines whether or not a particular User is allowed to access a protected resource. Runtime access control depends on:

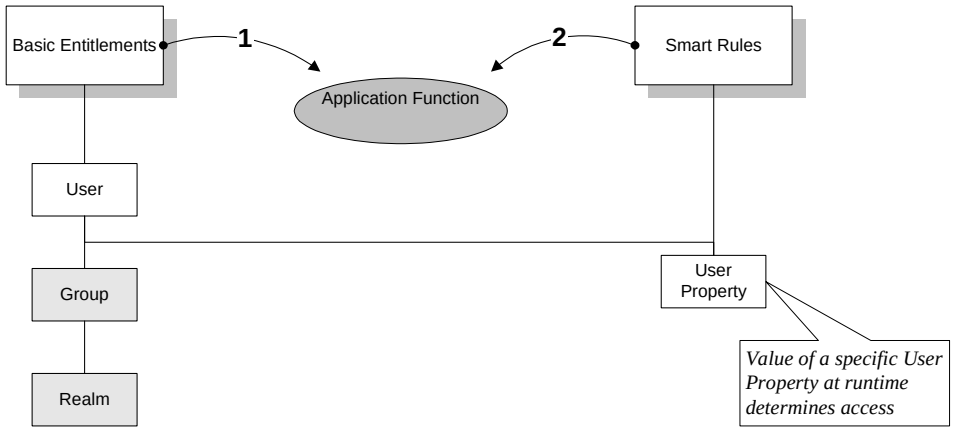
- Data about the User and the resource
- One or more authorization policies

ClearTrust SecureControl provides two distinct approaches to controlling access at runtime:

- **Basic Entitlements** enable access to a resource based on the identity of a User.
- **Smart Rules** enable access to a resource based on the value of a specific User Property.

Both Basic Entitlements and Smart Rules are associated with Application Functions (see Figure 6-2). By default, each Application you configure has a built-in "Access" Application Function, which means that the entitlements either enable (or prevent) a User from accessing the URI specified. You can also create your own custom Application Functions, as part of work-flow, application portal, or other scenarios; to do so, you must create applications that implement the ClearTrust SecureControl API. See the *Developer's Guide* for details.

FIGURE 6-1: Basic Entitlements and Smart Rules



Basic Entitlements take precedence over Smart Rules. If a Smart Rule says that a user must have a balance of $5,000 or more to access a resource, and user Bob meets this criterion but User Bob has also been explicitly denied access (or denied permission to another Application Function), he'll be denied.

Understanding Basic Entitlements

Similar in concept to traditional Access Control Lists (ACLs), a Basic Entitlement explicitly allows or denies access to a specific resource or Application Function based on the identity of a particular 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.

For example, 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. Since Users can belong to multiple groups, and groups can belong to multiple Realms, it's possible to create contradictory authorizations.

Resolving Multiple or Contradictory Authorizations

Resolving entitlements to resources is driven by several key principles:

- The most specific Basic Entitlement takes highest priority

- All entitlements at a given level must equal “allow” in order for a user to access a resource (security is as tight as possible)

These principles dictate that if a User has an explicit *allow* access as a member of a group that has been granted access but also has an explicit deny access based on his individual User account, he will be denied access to the Application Function. Likewise, an *allow* at the User level takes precedence over a Group- or Realm-level *deny.*

For example, the Finance group has been given a Basic Entitlement to the ACCESS Application Function for the Budget Application, but User Joe, a member of the group, has been denied; User Joe won’t be able to access the Budget Application.

Moreover, when Users are members of more than one group (or when a Group belongs to multiple Realms), all entitlements must be set to *allow* or the User will be denied access (the “security must be as tight as possible” principle).

NOTE: You cannot assign more than one Basic Entitlement to any given pair of Application Function and User (or Group or Realm).

Understanding Smart Rules

Basic Entitlements enable you to specify access to resources on a per-User, per-Group, or per-Realm basis. This approach meets the needs of many organizations. However, some organizations may want more flexibility and administrative ease than Basic Entitlements provide. ClearTrust’s Smart Rules let you apply access rules directly to *resources* (rather than to Users, Groups, or Realms).

Smart Rules detemine a User’s access rights to an Application Function based on the runtime values of custom User Properties that your organization creates. User Properties can include a vast array of attributes that make sense in the context of your organization’s workflow or other application scenarios, such as age, account status, department, date of hire, account holder, state of residence, type of customer, and so on.

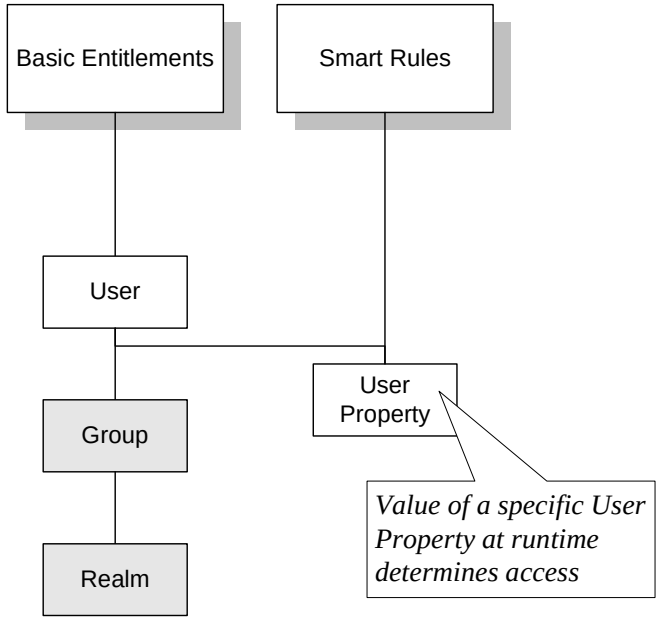


FIGURE 6-2: Smart Rules

Then, when the value of the property changes, a given User's access privileges change simultaneously and immediately, without Administrator intervention. The next time the User tries to access a Smart Rule-controlled resource, the new value determines whether he or she will be able to use the Application Function or not.

NOTE: Smart Rules decide a User's accessibility to a specified Application Function ***only*** if no relevant Basic Entitlement exists any level (User, Group, or Realm). Basic Entitlements ***always*** take precedence over Smart Rules. For details about the authorization algorithm, see "Authorization Processing" on page 176

For example, if an organization has implemented a User Property called "Employee" that's been setup as a boolean value (you're either an employee or you're not), then when employees are terminate, the Smart Rule for Employment Status can instantly revoke all access privileges as soon as that one property is changed. If you used Basic Entitlements to accomplish the same thing, you would have to manually remove the employee from each of several Groups.

As shown in Table 6-3, Smart Rules can be created in one of three different types—ALLOW, DENY, or REQUIRE.

TABLE 6-3: Smart Rules Processing Depends on the Type

Type	Processing Order (Default)	Logic for Multiple Rules of This Type	Usage Note
Allow	First	OR	If the User Property meets the condition, the User can access the Application Function immediately; no other rules are evaluated
Deny	Second	OR	If the value of the User Property meets the condition, the User is denied access immediately; no other rules are evaluated.
Require	Last	AND	If the value of the User Property meets the condition, SecureControl evaluates all other Require rules. If all other User Properties meet the conditions, the User is granted access.

If a User does not satisfy any of the ALLOW or DENY rules and doesn't meet the conditions of all of the REQUIRE rules, the User is denied access. You can combine the three types of Smart Rules in numerous ways to implement business rules and effectively control access to an Application Function. All ALLOW and DENY rules are evaluated before any REQUIRE rules. REQUIRE rules are only evaluated if none of the ALLOW or DENY conditions are met. These are explained in more detail in the next section.

Combining Smart Rules

An individual Smart Rule imposes a single condition on one particular User Property. To create more complex conditions for privileges to an Application Function in an Application, you can define and combine multiple Smart Rules for that Application Function. For example, an Application Function may have two Smart Rules associated with it as follows:

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

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

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

If the default processing order is in effect (Deny->Allow), then the Smart Rules will be evaluated as follows:

- **DENY** if Age < 21
- **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 Smart Rules. Administrators can reverse the order—so that Allow Rules are processed before Deny Rules—by setting the Smart Order Rule field to Allow-Deny in the Edit an Application Function dialog box. (On the Applications tab select the Application Function you want to protect, then click Modify. For details, see "Creating, Modifying and Deleting Applications" on page 79.)

Changing the processing priority to Allow->Deny changes the processing order:

- **ALLOW** if State = CA
- **DENY** if Age < 21

Evaluating the rules in this order means that Joe will be granted access. He is from the state of California, so the `ALLOW` condition is met and he is granted access. The `DENY` rule is never evaluated.

Switching the processing priority around provides you with a way to create sophisticated and elaborate combinations of Smart Rules with ease.

For example, one month an insurance company makes a special offer available to residents of California, Texas, and Oregon from its Web site. To accomplish this the insurance company creates three Smart Rules:

- **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 Web site and everyone else is denied access. But a month later, the insurance company decides it must prevent any users with bad credit from accessing the site, regardless of state. Modifying the rules to accomplish this is simple.

First, make sure that the priority toggle for this Application Function is set to its default value, **DENY -> ALLOW**. Then we add a single rule so that the Smart Rules look like:

- **DENY** if Credit = Bad
- **ALLOW** if State = CA
- **ALLOW** if State = TX
- **ALLOW** if State = OR

Now only users with good credit from California, Texas, or Oregon can access the insurance company's "special offer" web site.

You can also combine Smart Rules for compound processing.

Consider a site that wishes to limit access to retail customers with account balances in excess of $100. This is a compound condition - both parts of the condition must be satisfied or the user should be denied access. In such a case we turn to **REQUIRE** rules:

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

Only retail users with account balances in excess of $100 will be allowed access to the site.

Updating the Values Contained in User Properties

If you're going to use a Smart Rule, you must keep the values contained in any User Properties (upon which the rule is based) current and accurate according to your business rules.

The values of User Properties for individual Users can be updated in several ways. For example, a billing department could do one of the following to update a User's Account Status User Property:

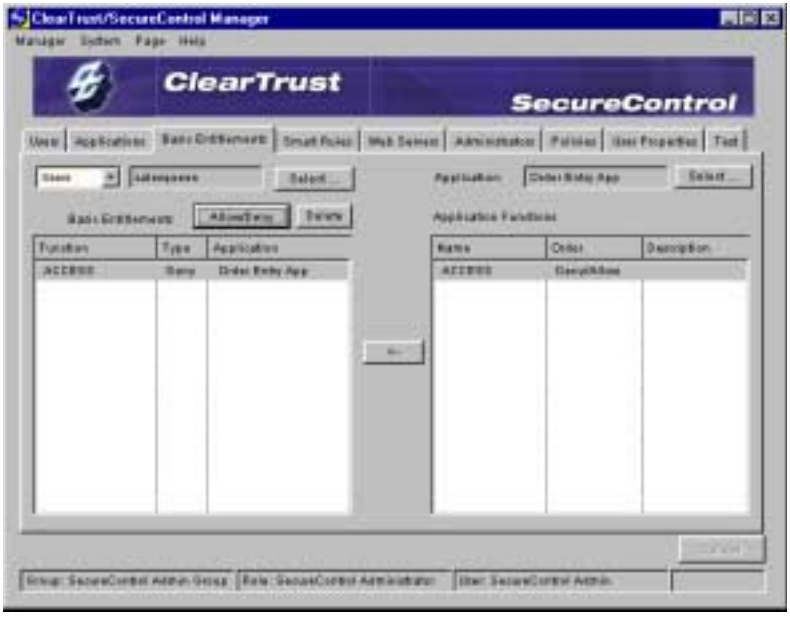
- Use the Modify User dialog (in the Users tab select a User, then click **Modify**) to directly manipulate the *account_status* User Property.
- Write a custom Application that changes the value of the User Property via the ClearTrust SecureControl API.

- Have User Property data replicated in from an external LDAP (Lightweight Directory Access Protocol) database. This useful feature of ClearTrust SecureControl allows User data to be shared instantly between ClearTrust SecureControl and other LDAP-based Applications.

Defining Basic Entitlements

To define Basic Entitlements:

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

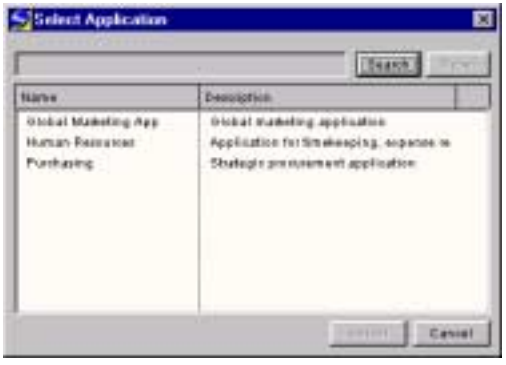


2. Select the entity for which you want to define a Basic Entitlement: Users, Groups, or Realms from the pull-down list box in the upper left corner of the tab.
3. Click the Choose button above the Basic Entitlements pane to open the Select User, Select Group, or Select Realm dialog (depending on which entity you have chosen in the list box):

4 Select the User, Group, or Realm to which you want to assign a Basic Entitlement from the Select User, Select Group, or Select Realm dialog.

5 Click Select to confirm your selection and return to the Basic Entitlements tab.

6 Select the Application you want to protect by highlighting its name and clicking the Choose button. The Select Application dialog displays:



7 Highlight the name of the Application from the list and then click the Select button to confirm your selection and return to the Basic Entitlements tab.

The Application you selected is now listed, along with the Application Functions associated with that Application.

8 Copy the functions you want to include as part of the Basic Entitlement from the Application Functions pane to the Basic Entitlements pane.

9 Select the Application Function you want to include from the Application Functions pane.

10 Click the left arrow button to copy the function to the Basic Entitlements pane. The Allow/Deny button is now active:

11 Click Allow/Deny to toggle the access type to Allow or Deny.

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

To modify or delete a Basic Entitlement:

1 Select the entity to which the Basic Entitlement you want to delete corresponds: Users, Groups, or Realms from the pull-down list box in the upper left corner of the Basic Entitlements tab.

2 Select the Basic Entitlement you want to delete in the Basic Entitlements pane.

3 Click the Delete button above the Basic Entitlements pane to delete the selected Basic Entitlement.

Defining Smart Rules

A Smart Rule defines an authorization policy by specifying a criterion that must be met by the value of a User Property. For example, a bank that wants to make a specific area of its Web site available only to current depositors could do so by following these steps:

1 Create a User Property of type boolean.

2 Group the Web resources and URIs into a ClearTrust SecureControl Application and establish a ClearTrust SecureControl User Property of type boolean called Current Depositor:

3 Set up an ALLOW-type Smart Rule that expresses the condition that if a User's Current Depositor (Property) = (Operator) "yes" (Value), the user will be granted access to that Application.

These instructions presume you've created a User Property.

To define a Smart Rule:

1 In the ClearTrust SecureControl Manager window, click Smart Rules to open the Smart Rules tab. User Properties that have been defined display in the User Properties pane of the Smart Rules tab.

2 Click on the Select button next to the Application field (in the upper-right corner) to display the Select Application dialog box.

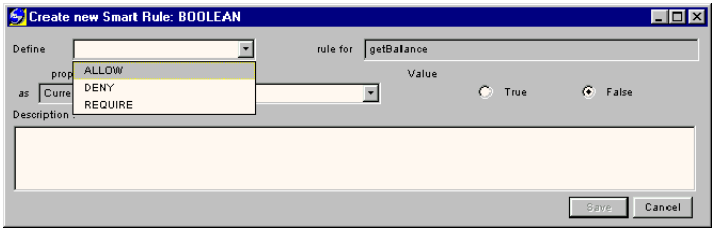
3 In the Select Application dialog, select the Application you want to protect.

4 Click Select to confirm your selection and return to the Smart Rules tab. The Application you selected is now listed in the Application field, and the Application Functions associated with that Application are listed in the Application Functions pane. (By default, ACCESS is the only Application Function associated with any Application.)

5 In the Application Functions pane, select the Application Function for which you want to define a Smart Rule.

6 In the User Properties pane, select the User Property on which you want to base the Smart Rule.

7 Click the left arrow button to display the Create new Smart Rule dialog box.



8 Define the type of Smart Rule processing that you want to be applied to the rule. The three possible types are Allow, Deny, and Require, as described in the table:

Type	Processing Logic
Allow	If the rule is satisfied, the User should be allowed access to the resource without any further rule processing
Deny	If the rule is satisfied, the User should be denied access without any further rule processing

Type	Processing Logic
Require	If the rule is satisfied, the system should continue to the next rule to determine accessibility; however, if the rule isn't satisfied, the User should be denied access. If no REQUIRE-type Smart Rules exist, and all ALLOWs and DENYs are processed without determining a result, the User is denied access.

9 Specify the operator you want to use in the Smart Rule against which to evaluate the User Property. The operators available in the Operator field vary, depending on the data type of the User Property, as shown in the table:

User Property	Operator
Date	Before, After
Boolean	Is Not, Is
String	Does Not Contain, Ends With, Equals, Starts With, Contains
Integer, Float	>=, <, +, >, <=, !=

10 Enter in the Value field the criterion that must be met.

11 Click Save to save the Smart Rule and return to the Smart Rules tab. The Smart Rule you created is now listed in the Smart Rules pane.

For example, you could create a Smart Rule that allows (Define) a User to update his or her account only if the Account Balance (Property) is >=(Operator) $100,000 (Value)

To modify Smart Rules

When your business rules change, or for any other reason, you can easily modify any Smart Rules that you've created using this same tab. To modify an existing Smart Rule:

1 Select the Smart Rule you want to modify from the Smart Rules pane on the Smart Rules tab.

2 Click the Modify button above the Smart Rules pane to open the Modify Smart Rule dialog. (This dialog is the same as the Create a New Smart Rule dialog.)

3 Change the data about the Smart Rule, including whether the rule allows, denies, or is required for the Application Function.

4 Click Save to save your changes and return to the Smart Rules tab. The modified Smart Rule is now listed in the Smart Rules pane.

To delete an existing Smart Rule:

1 Select the Smart Rule you want to delete in the Smart Rules pane on the Smart Rules tab.

2 Click the Delete button above the Smart Rules pane to delete the selected Smart Rule.

Testing Access Permissions

ClearTrust SecureControl's Smart Rules mechanism determines a User's access rights to an Application Function based on the runtime values of certain custom-defined properties of the User, such as age, account status, department, or date of hire. That is, you associate a User Property definition with an Application Function through a Smart Rule.

Before you begin implementing a security policy based on Smart Rules, it is a good idea to test access permissions on your system to see if the Smart Rules are controlling access in the way you envisioned. Using the Test tab in the SecureControl Manager window, you can simulate a User attempting to access a resource and determine whether or not the Smart Rules you have defined are controlling access to that resource as you planned.

To set up an access permissions test:

1 Click **Test** from the ClearTrust SecureControl Manager window to open the Test tab:

2 Select a User on which to perform an access permissions test.

- Enter the UserID in the **User** field and proceed to step 3, or click the **Choose** button to the right of the User field to open the Select User dialog.
- In the Select User dialog, select the User on which you want to perform the access permissions test.
- Click **Select** to select the User and return to the Test tab.

3 Select a Web Server on which to perform an access permissions test.

- Enter the Web Server name in the Web Server field and proceed to step 5, or click the **Choose** button to the right of the Web Server field to open the Select WebServers dialog.
- In the Select WebSevers dialog, select the Web Server on which you want to perform the access permissions test.
- Click **Select** to select the Web Server and return to the Test tab.

4 Enter the URI for which you want to test access permissions.

To run an access permissions test:

1. Specify the User, Web Server, and URI for which you want to test access permissions, as described above.
2. Select Flush Cache from the System menu to flush the cache.
3. Click Test to run the Test. The test results appear in the Test Results pane of the Test tab.

Chapter 7
Setting up Delegated Administration

Providing the ability to delegate security administration tasks is central to the architecture of ClearTrust SecureControl, and is one reason the solution easily scales to support enterprise-class, business-to-business environments. This chapter tells you how to create a delegated administration system to manage your organization's security policy, provides an example of a delegated administration hierarchy, and addresses the issue of resource ownership. It includes the following sections:

- Background Concepts
- Delegated Administration Example
- Resource Ownership
- Public and Private Resources
- Adding, Modifying, and Deleting Administrative Groups
- Defining Administrative Roles
- Assigning Users to Administrative Roles

Background Concepts

Administering a security policy for a large User base can be a daunting and time-intensive task. A delegated administration system not only makes this task more manageable, it also helps to ensure the privacy of User information. Only certain Administrators have access to private User data, such as credit card or social security numbers, for example. This prevents an Administrator's actions from becoming a threat to the security of the overall infrastructure.

The ClearTrust SecureControl solution's approach to delegated administration is built on the concept of Virtual Business Units (VBUs; also called Administrative Groups—the names are inter-changeable) in which all resources belong to a particular Administrative Group and are managed by an Adminstrator who is a member of a particular Administrator Role. These concepts are discussed in more detail in the next sections.

Administrative Groups (Virtual Business Units)—Administrative Groups usually reflect an organizational structure (such as Marketing, Sales, Shipping, and Engineering) or geography (such as New York, Chicago, and Los Angeles). Each Administrative Group has a name, a description, and a set of roles that are unique to that Administrative Group. An Administrative Group can have any number of Administrative Roles. Virtual Business Units (VBUs) may be lines of business such as Marketing, Sales, and Human Resources. Administrative Groups, or VBUs, may also include Extranet partners.

NOTE: Administrative Groups and Virtual Business Units (VBUs) are the same entities within ClearTrust SecureControl. These terms are used interchangeably throughout this guide.

Administrative Roles—A collection of privileges assigned to an Administrator. Each role is given a name and a description. You can assign roles to User(s) in a particular Administrative Group. Examples of Roles include "Help Desk" and "Power Admin." Examples of privileges within a role include "Change Passwords", "Delete Users", and "Create Users".

Administrators—The personnel assigned to administer the security policy. Each Administrator is given a set of privileges based on the Administrative Group to which he or she has been assigned and the roles associated with that Group.

The figure below illustrates the relationship of Administrative Groups, Administrative Roles, and Administrators.

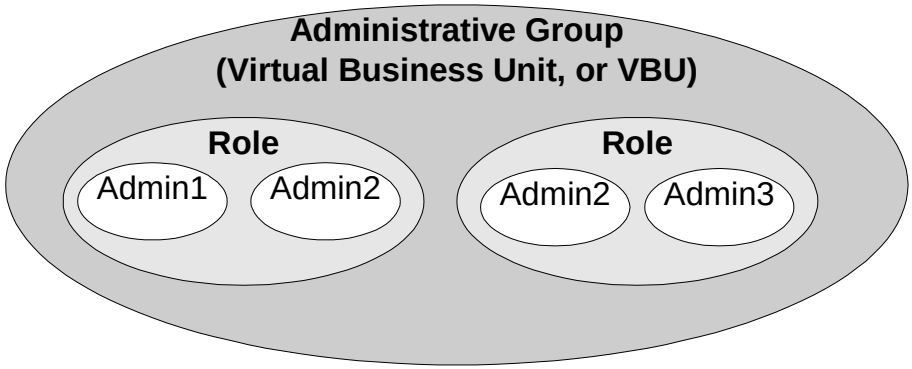


FIGURE 7-1: Administrative Data Model

Delegated Administration Example

This section illustrates how a delegated administration structure works. The illustration below shows a delegated administration hierarchy in which the Administrative Group at the highest level contains two Roles: Development and Testing. Each Role contains three Administrators, all of which are partitioned into different Roles and Administrative Groups.

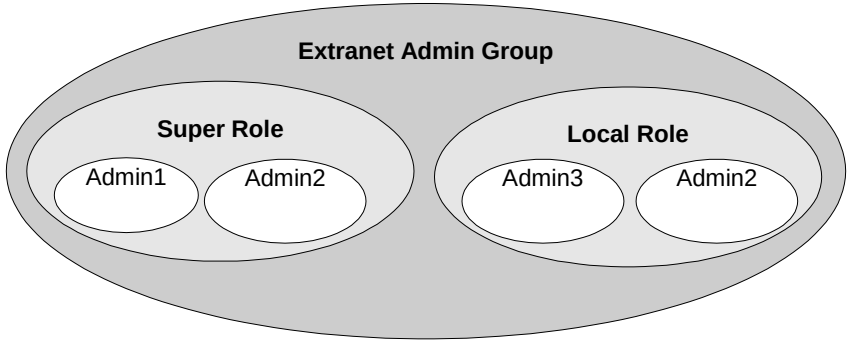


FIGURE 7-2: Delegated Administration Hierarchy

Resource Ownership

Every ClearTrust SecureControl-protected resource (Application, User, Group, Realm, and Web Server) is associated with an owner. This principle of ownership provides a system of accountability and control over the manipulation of the protected resources. An Administrative Group can modify and delete only the resources that it owns.

The following figure illustrates a system of ownership in which different types of resources are owned by different Administrative Groups: Administrative Group 1 owns Web Server1, User1 and User2; Administrative Group 2 owns Web Server2, User3 and User4.

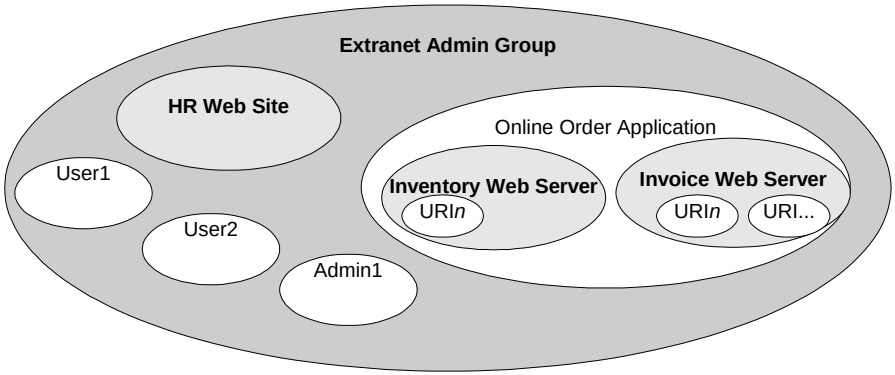


Figure 7-1. Ownership of Objects by Administrative Groups (also called VBUs)

Each of the following resources is assigned an owner when it is created:

- User
- Group
- Realm
- Application
- Owned Web Server URI
- Web Server
- User Property Definition

The owner can be either the Administrative Group to which the Administrator creating the entity belongs or another Administrative Group.

Public and Private Resources

If you designate a resource as a private resource (by selecting the **Private** check box when you create the resource), the resource can be seen only by Administrators who are members of the Administrative Group that owns the resource. A public resource, on the other hand, can be viewed by all Administrators, regardless of whether or not they are members of the Administrative Group that owns the resource. But only members of the owning Administrative Group can modify and delete public resources.

As an Administrator creating a resource, you can specify whether the following resources are public or private:

- User
- Group
- Realm
- Application
- Web Server
- Owned Web Server URI
- User Property Definition

Once a resource is created, you can change its public/private designation by clearing or selecting the **Private** check box in the appropriate Modify dialog.

It is important to make some resources public so that they can be managed by other Administrators and to make other resources private so that they cannot be seen by other Administrators. For example, you may want to make Users' social security numbers private so that other Administrators cannot view them. But you may want mark the User property account balance as public so other Administrators can view the balance, without modifying it, and report it to the customer.

In Figure 7-2, Administrators in the Extranet Admin Group cannot see any of the resources owned by Intranet Admin Group (Web Server 1, User2 and User1) because these resources are private. On the other hand, Administrators in Intranet Admin Group can see the Online Order App owned by the Extranet Admin Group because this resource has been marked as public.

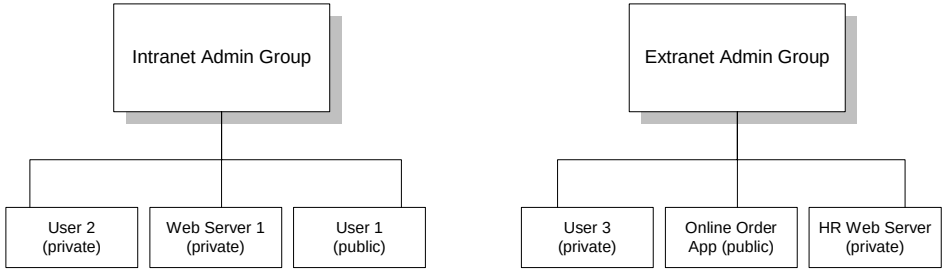


Figure 7-2. Every Resource is Associated with an Administrative Group

By default, all resources are public. To make a resource private, check the Private checkbox in the Create dialog when creating the resource. If the Group already exists, check the Private checkbox in the Edit dialog (select the resource in the appropriate tab, then click Modify).

The following subsections tell you how to define Administrative Groups and Administrative Roles and how to populate the Groups you have created with Administrators.

Adding, Modifying, and Deleting Administrative Groups

This section tells you how to add, modify, and delete Administrative Groups. You must log on as a Super User in order to perform these tasks.

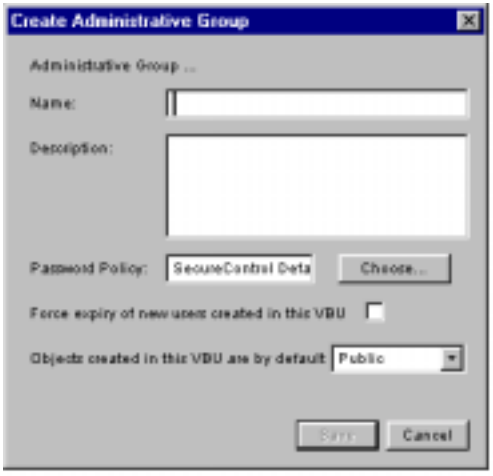
To create an Administrative Group:

1 Click Administrators in the ClearTrust SecureControl Manager window to open the Administrators tab:

The Administrators tab consists of four separate panes:

- The VBU - Administrative Groups pane displays existing Administrative Groups (only the ClearTrust Admin Group exists when you initially install the product).
- The Roles pane displays the currently-defined roles for the Administrative Group selected in the VBU-Administrative Groups pane.
- Privileges of this Role—A table of checkboxes, indicating the privileges associated with the role selected in the Roles panel. Use the scroll bar at the right of this table to scroll through the information.
- Users of this Role—A table of the Users assigned to the role selected in the Roles panel.

2 Click the Add button above the VBU-Administrative Groups panel to open the Create Administrative Group dialog.



3 Enter a Name and Description for the Administrative Group.

4 Click Save to return to the Administrators panel; the Group you entered now appears in the VBU-Administrative Groups panel.

5 Repeat steps 2-4 to add additional Administrative Groups.

To modify or delete an Administrative Group:

1. Click the Modify button above the VBU-Administrative Groups panel in the Administrators tab to open the Modify Administrative Group dialog. This dialog is similar to the Create Administrative Group dialog.
2. Edit the Name and/or Description as desired.
3. Click Save to Save your changes and return to the Administrators tab.

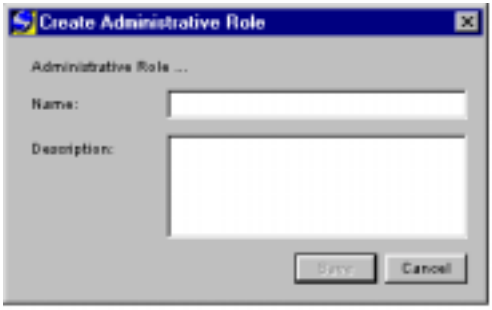
To delete an existing Administrative Group:

1. Select the Administrative Group that you want to delete from the VBU-Administrative Groups panel on the Administrators tab.
2. Transfer ownership of the selected Administrative Group's resources to another Group.
   - Click the Delete button above the VBU-Administrative Groups panel to open the Delete Group dialog.
   - Select the Administrative Group to which you want to transfer ownership of all the objects in the Group selected to be deleted from the Delete Group dialog.
3. Click Transfer/Delete to transfer ownership of all objects in the Group selected in the VBU-Administrative Groups panel on the Administrators tab to the Group selected in the Delete Group dialog and delete the Group selected in the VBU-Administrative Groups panel on the Administrators tab.

Defining Administrative Roles

To define roles within an Administrative Group and assign privileges to those roles:

1. Click the Add button above the Roles panel from the Administrators tab (shown above) to open the Create Administrative Role dialog.
2. Enter a Name and Description.



3 Click Save to return to the Administrators tab. The Administrative Role displays in the list. You must now assign privileges to this role. You can create several roles at once by repeating these steps, and when you're finished, you can assign privileges to each of them by following the next series of steps.

To assign privileges to Administrative Roles:

1 Select the Administrative Role to which you want to assign privileges from the Roles panel in the lower left of the Administrators tab. When a role is first created, it has no privileges assigned to it.

2 Select the privileges you want to assign to the role by selecting the appropriate check boxes in the Privileges for this Role panel in the upper right of the Administrators tab.

For example, if you were defining a Sales Admin Group to which you wanted to assign only the privileges of adding, modifying, and deleting Users, you would scroll down to the Users row and select the Add, Modify, and Delete checkboxes.

To clear all the checkboxes in the Privileges for this Role panel, click Revert.

You can configure the Administrative Role by selecting any combination of the following privileges:

- **Administrative Roles** - Allow an Administrator to add, modify, or delete Administrative Roles.
- **Ownership** - Allows an Administrator to modify ownership of resources.
- **Users** - Allow an Administrator to add Users, modify Users' fixed attributes and User Properties, and delete Users.
- **Groups** - Allow an Administrator to add Groups, modify Group properties, or delete a Groups.

- **Realms** - Allow an Administrator to add a Realm, modify a Realm's properties, or delete a Realm.
- **Applications** - Allow an Administrator to add, modify, or delete Web Applications, including Application resources (or URIs).
- **Web Servers**- Allow an Administrator to add, modify, or delete Web Servers.
- **Passwords** - Allows an Administrator to modify (but not create or delete) a User's password.
- **Property Definitions** - Allow an Administrator to add, delete, or modify User Properties.

3 Click the Apply button above the Privileges for this Role panel to confirm your settings.

4 Repeat steps 1-3 to assign privileges to other Administrative Roles.

NOTE: The Super User role supercedes Administrative Group boundaries and Administrative Role permissions; however, when you assign ownership of objects as a Super User, the ownership is still determined by the Administrative Role you selected when you logged on to ClearTrust SecureControl Manager.

Assigning Users to Administrative Roles

When you add a User to an Administrative Role, that User becomes a ClearTrust SecureControl Administrator. (Before you can assign Users to Administrative Roles, you must define Users. For details, see"Creating, Modifying, and Deleting Users" on page 58.)

To assign Users to Administrative Roles:

1 Select the Administrative Role to which you want to assign Users by clicking the desired role in the Roles panel of the Administrators tab.

2 Click the Add button above the Users in this Role panel to open the Add User To Administrative Role dialog. This dialog lists all currently-defined Users.

3 Select the User(s) you want to assign to the role. To select multiple Users, hold down the Ctrl key as you click on the desired User names.

4 Click Select to assign the selected User(s) to the Administrative Role.

5 Repeat steps 1-4 to assign Users to other Administrative Roles.

To remove a User from an Administrative Role:

1. Select the Administrative Role from which you want to remove a User by clicking the desired role in the Roles panel of the Administrators tab.
2. Select the Users you want to remove from the role in the Users in this Role panel in the lower right corner of the Administrators tab. To select multiple Users, hold down the Ctrl key as you click on the desired User names.
3. Click the Remove button above the Users in this Role panel to remove the selected Users from the role.

Ownership Transfer

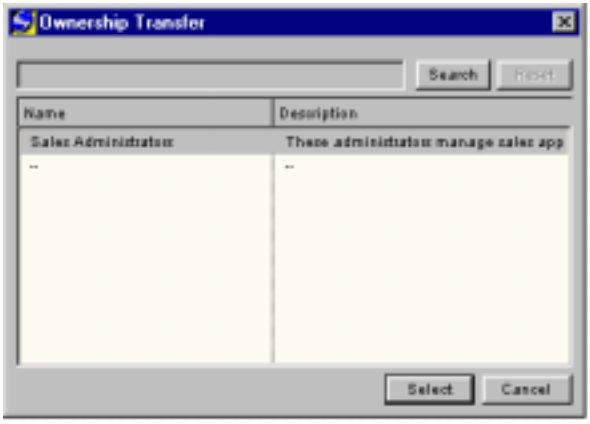
Once a resource is created, ownership of that resource can be transferred to another Administrative Group. The ClearTrust SecureControl Manager provides two methods for transferring ownership of resources:

- **Bulk transfer of ownership**—From the Administrators tab, you can transfer ownership of all resources owned by one Administrative Group to another Administrative Group. Before you delete an Administrative Group, for example, you must transfer ownership of all the resources owned by that Group to another Group.
- **Granular transfer of ownership**—From the Users, Applications, Web Servers, or User Properties tabs, you can transfer ownership of all resources or of selected resources owned by one Administrative Group to another Administrative Group.

Bulk Transfer of Ownership

To transfer ownership of all resources of one Administrative Group to another Administrative Group:

1. In the VBU - Administrative Groups pane in the upper-right corner of the Administrators tab, select the Administrative Group from which you want to transfer ownership of resources.
2. Click Ownership Transfer above the VBU - Administrative Groups pane to open the Ownership Transfer dialog, shown in the figure below. The name of the Group you selected is not listed in this dialog, since you will not be transferring ownership from a Group to itself.



3 Select the Group to which you want to transfer ownership from the Ownership Transfer dialog.

4 Click Select to transfer ownership from the Group selected in the VBU - Administrative Groups panel to the Group selected in the Ownership Transfer dialog.

Granular Transfer of Ownership

Every User, Group, Realm, Web Server, and Application is associated with an Administrative Group that owns the resource. You can transfer the ownership of a resource from one Administrative Group to another.

To transfer ownership of a specific resource from one Administrative Group to another:

NOTE: You must be logged on as a Super User to transfer ownership of a resource from one Administrator to another.

1 Select the resource for which you want to transfer ownership from the appropriate tab (Users for Users, Groups, or Realms; Web Servers for Web Servers; or Applications for Applications).

2 Click Modify to open the Modify <Resource> dialog, where <Resource> is the type of resource selected.

3 Click the Select button to the right of the Owner field to open the Select Owner dialog, shown in the figure below. If your list of Administrative Groups is long you can use the Search button to search for owners by name.

4. Select the Administrative Group to which you want to transfer ownership of the resource in the Select Owner dialog. The name of the current owner is represented by dashes in the table, as it does not make sense to transfer ownership from one Administrative Group to itself.
5. Click Select to transfer ownership of the resource to the selected Administrative Group and return to the ClearTrust SecureControl Manager window.

Chapter 8
Auditing

This chapter describes the User and administrator logging features provided by ClearTrust SecureControl. It contains the following sections:

- ClearTrust SecureControl Logging Overview
- User Activity Logging
- ClearTrust SecureControl Manager Activity Logging
- ClearTrust SecureControl Web Server Plug-in Access and Error Logging

ClearTrust SecureControl Logging Overview

ClearTrust SecureControl provides extensive logging of User and Administrator activity, providing a single point to examine activity for all Users across platforms and servers. In addition, ClearTrust SecureControl supports multiple levels of auditing granularity and allows for more comprehensive security audit data than is available from standard Web Server logs.

The ClearTrust SecureControl system creates several log files. Some of these logs are generated during installation and change infrequently, while others are generated by the servers during runtime and must be managed. All logs reside in the directory
`<SECURANT_HOME>/cleartrust/<ORACLE_SID>/logs/`

`CT_API_Errors.log`—If an error occurred while processing an API request, the API Server writes a detailed account of the error to the CT_API_Errors.log. Use this information to help diagnose problems with an API Client.

`CT_API_Logon.log`—The API Server records all API Client connections and disconnections in the API logon log. Use this log to audit API usage.

`CT_API_Transaction.log`—The API Server records a summary of all transactions in this log. Use it to audit all API usage.

`CT_Configuration.log`—The configuration log is created during the installation process. It simply records any errors that may have occurred during installation.

`CT_DatabaseInstaller.log`—The database installer log is created or appended to whenever the database schema is built. Any errors that occur during a schema build appear on this log.

`CT_Dataserver.log`—The dataserver log file records all errors that occur during runtime operation of the server, including all SQL-related errors. Automatic rotation of the log occurs when it reaches a size of five megabytes. This log will grow over time because some SQL errors are part of normal operation.

`CT_Dispatcher_Events.log`—The dispatcher event log records events that are part of the normal operation of the dispatcher. When a Plug-In requests the list of available authorization servers, when an authorization server registers with the dispatcher, or when an authorization server's readiness to handle requests is assessed, an event is entered in the log. This log will grow over time, so you will need to manage it.

`CT_Dispatcher_Errors.log`—The dispatcher errors log records all errors that occur within the dispatcher. The size of this log should remain at zero bytes—any size above that indicates improper operation of the server.

`CT_Authorizer_<port>.log`—The authorization server log is named using the port supplied during startup. It records all errors that occur during runtime operation of the server. The size of this log should remain at zero bytes—any size above that indicates improper operation of the server.

`CT_UserActivity_<port>.log`—The User activity log records information about the actions taken by ClearTrust SecureControl Authorization Servers on User requests. Each Authorizer has its own log file, and its port is used in the name of the log file. For details, refer to the section titled, *"User Activity Logging"*, later in this chapter.

`CT_KeyServer.log`—The keyserver log records information about the keyserver processing.

User Activity Logging

Once Web Servers are protected with the ClearTrust SecureControl Plug-In, keeping track of User activity, attempted break-ins, and Web resource usage is easy. Each Authorization Server generates a User Activity Log that records details of the system's use. You can configure the level of detail captured in the log file, as well as the format of log file, its maximum size, and its name. Most major log file parsing and reporting programs can read the log file, so you can easily generate reports and graphs of User activity. You configure the User activity event log system via the Default.conf file. For details, refer to Chapter 5 of the **ClearTrust SecureControl Installation and Configuration Guide.**

User Activity Events

The User Activity Event Logging system records information about requests made to protected Web Servers. Each time a Web User requests a protected document, an entry is made in the User Activity Event Log. This entry in the log is a User activity event. The following data are recorded for each event:

Log Timestamp: The date and time the event was written to the log. Example: "Tue Nov 24 13:49:43 PST 1998".

User Name: The ClearTrust SecureControl User name of the User requesting the protected resource.

IP Address: The IP address of the User's computer making the request.

Event Type: A string indicating the type of event (see below).

Event Time: The time the event actually occurred. Under high load, the Authorization Server may not immediately write to the log, making the Log Timestamp entry inaccurate. Use this entry instead. The format is the same as the Log Timestamp.

URI: The URI of the protected resource. Example: "/marketing/index.html".

Web Server Name: The name of the Web Server hosting the protected resource, as defined in the ClearTrust SecureControl Manager.

Application Name: The name of the Application that contains the protected resource, as defined in the ClearTrust SecureControl Manager.

Log File Format

Each User activity event takes one line in the log file. The event's data are concatenated with the specified log delimiter and written to the file.

Example of a Log File:

```
Tue Nov 24 19:51:11 PST
1998,andy,206.234.199.162,USER_ENTITLEMENT_ALLOW,Tue Nov 24
19:51:13 PST 1998,/marketing/index.html,MainWebServer,Marketing
Application
```

This sample log file can be broken down into the following units:

Log Timestamp:	Tue Nov 24 19:51:11 PST 1998
User Name:	andy
IP Address:	204.224.195.162
Event Type:	USER_ENTITLEMENT_ALLOW
Event Time:	Tue Nov 24 19:51:13 PST 1998
URI:	/marketing/index.html
Web Server Name:	MainWebServer
Application Name:	Marketing Application

Log File Name and Location

The name of the log file is composed of three parts: a prefix, a port number, and a suffix. The prefix is set in the `Default.conf` config file. The default value is adequate in most circumstances. The port number is the same as the authorization server's listen port, which also appears in the `Default.conf` file. The suffix is always `.log`. Combining all three parts yields a file name such as `CT_UserActivity_5020.log`.

The User Activity Event Log is stored in the ClearTrust SecureControl log directory. This directory is named `logs` and is located below the directory designated as the ClearTrust SecureControl root directory.

Event Types

User activity events are broken down into three categories: User validation events, access denied events, and access allowed events. You can configure which categories are logged and which are discarded.

User Validation Events

Events generated during the User authentication phase are known as User validation events. The following are the User validation events for ClearTrust SecureControl:

`INVALID_USERNAME`: The User name was not in the ClearTrust SecureControl database.

`INVALID_PASSWORD`: The password was invalid.

`INACTIVE_ACCOUNT`: The account is inactive because the start date has not arrived.

`EXPIRED_ACCOUNT`: The account expiry date has passed, expiring the account.

Access Denied Events

Events generated during the User authorization phase that result in the Users being denied access to requested resources are known as access denied events. The following are the access denied events for ClearTrust SecureControl:

`USER_ENTITLEMENT_DENY`: User Explicit Entitlement denied access to the resource.

`GROUP_ENTITLEMENT_DENY`: Group Explicit Entitlement denied access to the resource.

`REALM_ENTITLEMENT_DENY`: Realm Explicit Entitlement denied access to the resource.

`SMART_RULE_DENY`: Smart Rule denied access to the resource.

`NO_ENTITLEMENT_DENY`: No entitlements granted access to the protected resource, so access is denied.

PASSIVE_DENY:The resource is unprotected, but the Authorization Server is in Passive Mode, so access was denied.

CACHED_DENY:The inaccessibility of the resource to the User was cached in the Authorization Server.

Access Allowed Events

Events generated during the User authorization phase that result in the Users being allowed access to requested resources are known as access allowed events. The following are access allowed events in ClearTrust SecureControl:

USER_ENTITLEMENT_ALLOW: User Explicit Entitlement allowed access to the resource.

GROUP_ENTITLEMENT_ALLOW: Group Explicit Entitlement allowed access to the resource

REALM_ENTITLEMENT_ALLOW: Realm Explicit Entitlement allowed access to the resource

SMART_RULE_ALLOW: Smart Rule allowed access to the resource.

CACHED_ALLOW: The accessibility of the resource to the User was cached in the Authorization Server.

Logging Levels

ClearTrust SecureControl uses the concept of Logging Levels to control which events are recorded. Four levels of detail are supported, ranging from no logging to logging of every event type. Like all configurations for the auditing system, the level is specified in the **`Default.conf`** file. Table 8-1 summarizes the logging levels system; an X indicates events of that type will be logged.

TABLE 8-1: User Activity Logging Levels

	0	10	20	30
User Validation Events		X	X	X
Access Denied Events			X	X
Access Allowed Events				X

Combining Log Files

Each authorization server generates its own log file. Depending on the type of install and the reporting tool used, you may need to combine multiple log files.

- If all Web Server Plug-ins are configured in Standard mode (all requests go to one authorization server) then there will be only one User Activity Log file that fills with events. In that case there is no reason to combine the log files.
- If any Plug-Ins are configured in Distributed mode (requests are distributed to all Authorization Servers), there are two or more Authorization Servers running, and the reporting tool used does not support multiple log files, then you will need to combine the logs. To do this, concatenate the files together using whatever utility is available (e.g. "cat" on Unix systems). Then take the single log file and parse it with the reporting tool.

ClearTrust SecureControl Manager Activity Logging

Each time an administrator logs on to ClearTrust SecureControl Manager and creates, modifies, or deletes objects, that activity is recorded in the **`AdminActivity.log`** file. This file is tab-delimited and can be read by most major log file parsing and reporting programs, so you can easily generate reports and graphs of administrative activity.

The Admin GUI Logging system records the following actions an administrator takes while using ClearTrust SecureControl Manager.

- **Administrator logs on to ClearTrust SecureControl Manager**— When an administrator logs on to ClearTrust SecureControl Manager, a row is appended to the **`AdminActivity.log`** file located in the **`ClrTrust\ct_root\logs`** directory. The row contains the following data:
  - Date/time stamp indicating when the administrator logged on to ClearTrust SecureControl Manager.
  - The word **`register`**, indicating that an administrator logged on to ClearTrust SecureControl Manager.
  - The first and last name of the administrator who logged on to ClearTrust SecureControl Manager.

- **Administrator logs off ClearTrust SecureControl Manager** using the **Logoff** command from the **Manager** menu—When an administrator logs off ClearTrust SecureControl Manager, a row is appended to the **`AdminActivity.log`** file located in the ClrTrust\ct_root\logs directory. The row contains the following data:
  - Date/time stamp indicating when the administrator logged off ClearTrust SecureControl Manager.
  - The word **`unregister`**, indicating that an administrator logged off ClearTrust SecureControl Manager.
  - The first and last name of the administrator who logged off ClearTrust SecureControl Manager.

Note: If the administrator logs off ClearTrust SecureControl Manager in any way other than selecting Logoff from the Manager menu, the event is not recorded.

- **Administrator creates/modifies an object using ClearTrust SecureControl Manager**—When an administrator creates/modifies an object using ClearTrust SecureControl Manager, a row is appended to the **`AdminActivity.log`** file located in the ClrTrust\ct_root\logs directory. The row contains the following data:
  - Date/time stamp indicating when the object was created/modified.
  - The word **`save`**, indicating that an administrator created/modified an object.
  - The first and last name of the administrator that created/modified the object.
  - Every data field in the database record, written out.

NOTE: You cannot distinguish a newly-created object from a modified object that existed previously by examining a row. The same information is written out for creates and modifies. If you need to determine what changes were made to an object, look to see if there is a previous save row for that object in the log file, then compare the differences.

- **Administrator deletes an object using ClearTrust SecureControl Manager**—When an administrator deletes an object using ClearTrust SecureControl Manager, a row is appended to the **`AdminActivity.log`** file located in the ClrTrust\ct_root\logs directory. The row contains the following data:
  - Date/time stamp indicating when the object was deleted.
  - The word **`delete`**, indicating that an administrator deleted an object.
  - The first and last name of the administrator who deleted the object.
  - Every data field in the database record, written out.

Sample AdminActivity.log File Entries

This section lists representative rows in the AdminActivity.log file corresponding to different types of administrator activity.

Logon
Tue Apr 27 11:57:26 PDT 1999 register

Logoff
Tue Apr 27 11:57:56 PDT 1999 unregister ClearTrust Admin

Create User
Tue Apr 27 12:08:15 PDT 1999 save ClearTrust Admin User ID: 100021 ADMIN_GROUP_ID: 1 PUBLIC_STATE: 1 SUPER_USER: 0 NAME: 1 FIRST_NAME: 1 LAST_NAME: 1 EMAIL: CREATION_DATE: 1999-04-27 12:08:13.0 BEGIN_DATE: 1999-04-27 12:08:03.0 INACTIVE_DATE: 1999-10-27 12:08:03.0 DN:

Edit User
Tue Apr 27 12:08:29 PDT 1999 save ClearTrust Admin User ID: 100021 ADMIN_GROUP_ID: 1 PUBLIC_STATE: 1 SUPER_USER: 0 NAME: 2 FIRST_NAME: 2 LAST_NAME: 2 EMAIL: CREATION_DATE: 1999-04-27 12:08:13.0 BEGIN_DATE: 1999-04-27 12:08:03.0 INACTIVE_DATE: 1999-10-27 12:08:03.0 DN:

Delete User
Tue Apr 27 12:08:42 PDT 1999 delete ClearTrust Admin User ID: 100021 ADMIN_GROUP_ID: 1 PUBLIC_STATE: 1 SUPER_USER: 0 NAME: 2 FIRST_NAME: 2 LAST_NAME: 2 EMAIL: NULL CREATION_DATE: 1999-04-27 12:08:13.0 BEGIN_DATE: 1999-04-27 12:08:03.0 INACTIVE_DATE: 1999-10-27 12:08:03.0 DN: NULL

ClearTrust SecureControl Web Server Plug-in Access and Error Logging

ClearTrust SecureControl does not interfere with the normal logging of your Web Server. The name and location of log files varies from one Web Server to another. Most Web Servers—including Netscape Enterprise, Apache, and IIS—use separate log files for reporting errors or normal accesses.

When ClearTrust SecureControl allows a User to access a particular resource on the Web Server, your Web Server records the access as normal. Similarly, when ClearTrust SecureControl denies access, your Web Server records it as an error in the normal way.

Furthermore, ClearTrust SecureControl records its own errors in the error log of your Web Server. Anytime the ClearTrust SecureControl Plug-In needs to contact the Server Dispatcher to get a new list of Authorization Servers, it makes a note in the error log. This normally only happens once when the server first starts up, but may happen again if an Authorization Server goes down or becomes overworked. Refer to *Chapter 10, Password Policies*, to learn more about the functions of the Server Dispatcher and Authorization Server.

Chapter 9
Password Policies

This chapter provides an introduction to ClearTrust SecureControl's password policies and gives answers to frequently asked password policy questions. It includes the following sections:

- Introduction to Password Policies
- Creating Password Policy
- SecureControl Password Policy Enforcement Mechanisms
- Individual Password Management

Introduction to Password Policies

NOTE: Only Super Users have access to this feature.

Password policy is an integral part of a well-designed security policy. Because passwords are the most common means of User authentication, it is important that they be as secure as possible. If passwords are too easy to guess, the overall security of your system will be low. To prevent this, ClearTrust SecureControl comes with a set of tools to help you define and enforce a consistent password policy for each Administrative Group or VBU that you create. These tools allow you to create a set of quality checks that new User passwords must pass before being considered acceptable. If you do not create a new password policy for an Administrative Group, the SecureControl Default Password Policy is automatically assigned to that Group.

SecureControl provides a powerful yet flexible definition and enforcement mechanism. It is important to use the tools provided with SecureControl along with common sense to create policies that are suitable to each individual VBU.

In addition, it is important to remember that passwords ensure only a limited degree of security. If a large enough number of Users are uncomfortable with a strict password policy, you may want to consider using a more secure authentication method. Forcing Users to live with an overly strict password policy may cause them to compromise security (most commonly by writing their passwords down).

The following section describes how to use the Policies tab to create a new password policy for an Administrative Group or VBU.

Creating Password Policy

You can create and modify password policy using the Policies tab of the ClearTrust SecureControl Manager.

FIGURE 9-1: Password Policies Tab

To create a new password policy:

1 From the Policies tab (shown above), click the Create button to display the Create Password Policy dialog box:

FIGURE 9-2: Create Password Policy Dialog

2 Enter all the settings for the new password policy as follows:

- Name - Create a useful name for the Password Policy.
- Description - Enter a meaningful description of the Password Policy.
- Minimum number of characters in password - Enter an integer that defines the minimum number of characters required for passwords. This value must be less than or equal to the “Maximum number of characters in password” parameter.
- Maximum number of characters in password - This is an integer that defines the maximum number of characters allowed in passwords. This value must be greater than or equal to the “Minimum number of characters in password” parameter.
- Number of past passwords to exclude - This is a protective measure to ensure that Users don’t re-use older passwords. SecureControl archives 25 past passwords for each user. This field can take values between 0 and 25.
- Files containing excluded passwords - This is a file that contains a list of excluded passwords so that if a User enters a password contained in this file, the system rejects it and asks for another password. A filename must be present in this field.
- SecureControl includes two excluded password files, called “words.txt” and “empty.txt”. The first one contains a list of words to exclude as passwords and the second is empty for you to add your own list of words.

To add a new dictionary, you can simply use the “empty.txt” file or create a file of the same format and place it in the root directory where you installed the server.

- List of excluded characters - This is a list of characters that cannot be used in passwords.
- Maximum password lifetime - This value determines the default lifetime of a password for a user owned by the VBU. This value must be entered in the following format: an integer followed by a single letter that stands for time increment desired. Use d for days, h for hours, m for minutes, and s for seconds. For example, to say the maximum lifetime of the password is 60 days, you enter 60 d.
- Since Password Policy is set according to VBU, and all users in a VBU share the same policy, you may need to override the “Maximum password lifetime” parameter for an individual user. To do this, you can change the (password) expiration date in the Create/Modify User screen from the Users tab.
- Require at least one non-alphabetic character - This check box lets you define policy that makes Users include at least one non-alphabetic character in their passwords for added security.

3 Click on the Save button to save the new policy and re-display the ClearTrust Manager Policies tab.

The Default Password Policy

One of the Password Policies in the SecureControl system is the Default Password Policy. This is the Password Policy associated with newly created Administrative Groups. To set a password policy as the default policy, choose it from the list of password policies that appears in the password policies section of the Policies tab and click Set as Default.

FIGURE 9-3: SecureControl DEFAULT Password Policy Settings

Modifying Password Policy

To modify an already existing Password Policy, select the Password Policy from the list of Password Policies that appears in the password policies section of the Policies tab. Once you have selected a Password Policy, the current parameters for that Password Policy appear on the right half of the screen. These values can be edited. Once you edit the values and are satisfied, save them by clicking Save Policy Details. To restore the current set of parameters, click, Revert to Saved.

Deleting Password Policy

Since there must be exactly one Default Password Policy in the system at all times, the Default Password Policy cannot be deleted unless you set another policy as the default. To delete the Default Password Policy then, set a new Password Policy as the Default and then highlight the original Default Password Policy and click, Delete.

SecureControl Password Policy Enforcement Mechanisms

The password policy enforcement mechanism provided with SecureControl is flexible and modular. You need only enable the policy-checking mechanisms you deem necessary for your particular security needs. SecureControl provides the following password policy enforcement mechanisms:

- Length
- Non-Alphabetic Characters
- Character Exclusion
- Dictionary Search
- Password History
- Password Lifetime
- Password Expiration

Length

Passwords that are too short are vulnerable to brute force attacks, but passwords that are too long can sometimes cause problems in some poorly-written programs, allowing malicious hackers to compromise the system. A password shorter than six characters is probably unacceptably weak, but a password longer than 32 characters could also be problematic.

NOTE: Because the algorithm used by SecureControl for encrypting passwords reduces all passwords to the same length, the length of the password is unimportant to SecureControl 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, password becomes pa$5w04D). On its own, however, this mechanism is rarely strong enough to deter attacks, because 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 is a good idea to exclude certain characters from passwords. Characters such as `&`, `*`, and `/` can have unpredictable effects when used in strings passed to some common UNIX commands. SecureControl allows you to filter these characters.

Dictionary Search

The dictionary policy uses a list of words that are not accepted as passwords. Users' new passwords are checked against this list and are not allowed if they match a word on the list. The word list bundled with SecureControl contains a list of several thousand commonly-used words. Any word in this list will inevitably be included as part of any dictionary attacks on the system, so it is a good idea to add to this list instead of replacing it altogether.

Password History

Even conscientious Users hate dealing with passwords because it is difficult to come up with good ones and they are often hard to remember. 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. Obviously, this defeats the purpose of requiring regular password changes. Tracking a User's password history eliminates this problem by allowing SecureControl to check Users' new passwords against a list of their previous passwords and reject the new password if a match is found.

Password Lifetime

The longer a password exists, the more likely it is to be compromised. Attackers can use packet sniffers to capture passwords sent over the network in the clear; Users can watch over other User's shoulders as they type in their passwords; and malicious hackers can break into your system and collect passwords before being shut out. Therefore it is a good idea to force Users to change their passwords periodically. When Users' passwords expire, they will be locked out of any SecureControl-protected resources until they choose a new, valid password.

WARNING Set the password lifetime with discretion. Password lifetime is probably the most powerful enforcement tool provide by SecureControl, yet it is also the easiest to abuse. If you create a policy that combines a long password history with a short password lifetime, you may make Users' experiences with SecureControl nearly unbearable, driving them to either forget their passwords or write them down, and thereby negating the security of the password.

Password Expiration

SecureControl also provides a forced password expiration feature. You can force password expiration either through the SecureControl API or you can go to the User's Tab and set the User's (password) expiration date to match the (password) creation date. This feature forces the expiration of a specified User's password and forces the User to change his/her password the next time he/she authenticates.

Individual Password Management

SecureControl's API provides full functionality for individual password management. This functionality is provided in the form of CGIs and Java Servlets. In order to take advantage of this functionality, SecureControl includes some examples.

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 the Web site.

The Password Change Web page asks the User to provide his or her old password and a single new password two times. The old password provided 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 checked for compliance with password policy.

If the password meets the format requirements, a success message is returned to the User via Web page and 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 the User is instructed to provide a compliant password.

Forgotten Passwords

When Users forget their passwords, they call the help desk to be issued a new password. The help desk attendant accesses a SecureControl secured 'Password Reset' Web page available only to help desk attendants. The help desk attendant issues 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 your organization doesn't want to have passwords going across email then they could alternatively have the help desk attendant read the generated password to the User or leave the password on the User's voicemail. This should be done in accordance with the organization's security policy.

Chapter 10
Using SecureDetector

This chapter tells you how to use ClearTrust SecureDetector to monitor suspicious activity at the application level. It contains the following sections:

- What is ClearTrust SecureDetector?
- Running the SecureDetector Manager
- Testing Attack Policies
- Generating Reports
- SecureDetector Reports Panel

What is ClearTrust SecureDetector?

ClearTrust SecureDetector is an integrated component of ClearTrust SecureControl that acts as an application-level threat detection tool. As such, it monitors suspicious user and administrator activity at the application level.

Application-level threat detection tools like SecureDetector complement the many network-level intrusion tools available today as the two serve different purposes. While network-level intrusion detection tools protect the network itself from unauthorized access, application-level threat detection tools protect online resources once users have gained access to the network. Network-level intrusion detection tools detect users attempting to access the network illegitimately or identify protocol level attacks on the network while application-level threat detection tools monitor suspicious user activity such as password guessing and unauthorized access attempts. SecureDetector also monitors administrator activities, API transactions, API logins, API errors, and system errors.

SecureDetector provides you with the ability to establish policies for detecting and responding to potential application misuse. Using SecureDetector, you link suspicious event profiles with a defined level of occurrence to automatically trigger specific responses. The action generated can be to alert the Administrator via email, suspend or disable the account, or any action that you want to customize through the SecureControl API.

As the administrator, you need only to establish policies and link event profiles with a defined level of occurrence, SecureDetector then monitors the activity on its own. If SecureDetector notices a pattern of suspicious activity, several responses can occur. First, the intruder's activities are logged for analysis. Then, notification can be sent to administrators. And finally, the intruder can be automatically restricted from further application access.

Running the SecureDetector Manager

The ClearTrust SecureDetector Manager is a separate application but is tightly integrated with the SecureControl access management solution. Because detecting events is a time-dependent task, it is recommended that you install it on the same machine as other ClearTrust server components. This is because like SecureControl, SecureDetector, uses the system time of the host it is running on.

If you install SecureDetector on a host other than where the SecureControl database resides, the system time must be in synch so that events are logged and timestamped properly.

To start SecureDetector:

- On a Windows NT system, from the Windows NT **Start** menu, select **Programs**, then **Securant**, then **SecureDetector Manager**.
- On a Solaris system, run the `Manager` script in the directory in which SecureDetector is installed.

Starting the SecureDetector Daemon

The Daemon is responsible for monitoring activity on the network. It works in the background somewhat like a security camera. The Daemon accepts definitions and profiles for responses from the SecureDetector Manager.

To start the SecureDetector Daemon:

- On NT-based systems, from the Windows NT **Start** menu, select **Programs**, then **Securant**, and then **SecureDetector Daemon**.
- On Solaris systems, run the script **`Daemon`** in the directory where you installed SecureDetector.

Configuring SecureDetector

Configuring SecureDetector for Database Connectivity

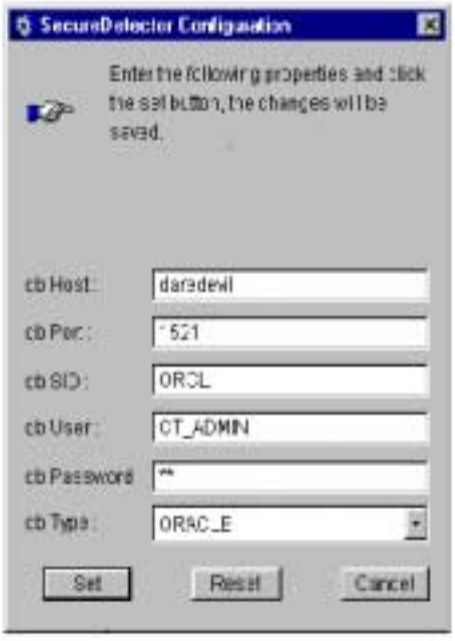
The first time you start SecureDetector, the system prompts you to configure SecureDetector for database connectivity. After the initial run, you can manually configure SecureDetector for database connectivity as described below.

To configure SecureDetector for database connectivity:

- On a Windows NT system, go to the directory where you installed SecureDetector and run `config.exe`.
- On a Solaris system, go to the directory where you installed SecureDetector and run `Config`.

1. When you run config.exe or `config`, the screen shown below appears. Fill in the following fields with the appropriate information.
   - **dbHost** - Host where SecureControl database is running.
   - **dbPort** - Database listener port (default is 1521).
   - **dbSID** - The instance name of the SecureControl database.
   - **dbUser** - A SecureControl database User (default is CT_ADMIN).
   - **dbPassword** - The SecureControl database user password.
   - **dbType** - Type of database (Oracle or Sybase from drop-down list).
2. When you have filled in the fields, click **Set** to set configuration and proceed with SecureDetector. You can also select Reset to cancel the values you set and re-enter, or click Cancel to quit SecureDetector without saving your configuration.

.



Before SecureDetector can begin monitoring for suspicious activity, you must set up the system for monitoring. To do this, you must first configure the Daemon and the API server. Then you must define attack policies and configure actions. And finally, you must configure browser and mail server options. The following subsections tell you how to perform these configuration tasks.

Configuring the Daemon

The SecureDetector Daemon searches the event table in the ClearTrust database for suspicious activity.

To configure the Daemon:

1 From the ClearTrust SecureDetector Manager window, click the **Configuration** tab to access the Configuration panel.

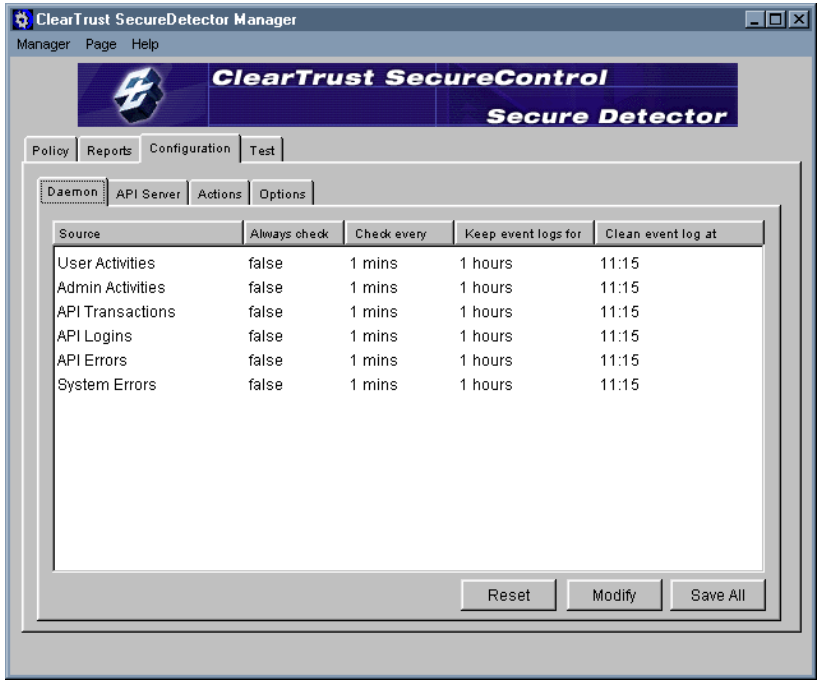


FIGURE 10-1: Configuration Panel Showing Daemon Tab

2 On the Configuration panel, click the **Daemon** tab to open the Daemon panel. When you open the Daemon panel, the system display a list of possible sources for where attacks originate. Sources include User Activities, Admin Activities, API Transactions, API Logins, API Errors, and System Errors.

3 The first time you go to this panel, only the Sources are displayed. To configure the attributes for each Source, highlight the Source and then click **Modify** to display the specific Source configuration screen you have highlighted. For example, if you highlight User Activities and click Modify, the system displays the User Activities Configuration screen, as shown on the following page.

NOTE: After you have configured all of the Sources, the configuration attributes appear next to the Source on the Daemon panel. You can then highlight a specific Source and use the Modify button to go back and make changes to its original configuration or you can highlight a specific source and use the Reset button to clear the original configuration.

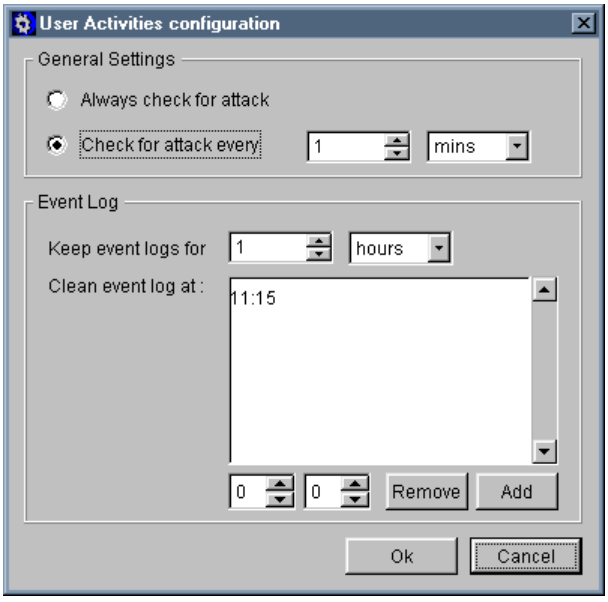


FIGURE 10-2: User Activities Configuration

4 On the User Activities Configuration screen, enter the following information in the *General Settings* field:

- Select **Always check for attack** to direct the Daemon to scan constantly for attacks. This option causes the Daemon to poll the database for suspicious activity at its default of every one minute.
- Select **Check for attack every** and use the pull-down list boxes to direct the Daemon to scan for attacks at a specified interval of minutes, hours, days, or months.

5 Then move to the *Event Log* field to specify how long SecureDetector will keep event logs and how often it will clean the event log:

- Use the **Keep events for** pull-down list boxes to specify how many hours, days, or months SecureDetector will keep events in the event log.
- Use the **Clean event log at** pull-down list boxes to specify a time you want the event log to be cleaned. Typically you will want the SecureDetector Daemon to clean the event log every one or two days at

the most, depending on how much disk space is available for the Daemon database and how much activity you anticipate on the monitored Web Servers. For more information, contact a Securant representative.

NOTE: It is very important that you maintain this log in the Daemon to keep it from getting too large.

6 Click **Modify** to list the time in the Clean event log at field. At the specified time, the Daemon searches the event log for events older than the period you have specified in the **Keep event logs for** field and deletes any events that it finds. To delete a time for cleaning the event log, select the time you want to delete in the Clean event logs at field, then click **Remove** to remove that time. Note that the Clean event log values are in 24-hour formats so that to clean the log at 6:00am, the value you enter is 6:00; for 6:00pm, the value is 18:00.

7 Click **OK** to save your settings and to re-display the Daemon panel.

8 When the system displays the Daemon panel, you can select other Sources and follow the same steps as outlined for the User Activities Source.

9 When you have configured all Sources, click **Save All**.

Configuring the ClearTrust API Server

In order to perform actions that disable or suspend a user's account if suspicious activity is detected, the SecureDetector Daemon must be able to connect to the ClearTrust API Server.

To configure the API Server:

1 Click the **Configuration** tab to access the Configuration panel from the ClearTrust SecureDetector Manager window.

2 From the Configuration panel, click the **API Server** tab to access the API Server panel.

3 Enter the following:

- **Host** - The hostname for the API Server.
- **Port** - The port number on which the API Server is running. (The default is 5091).
- **Admin User** - The name of the Administrator who you want to log on as. The Administrator you log on as must be privileged to modify the account of a User who is launching an attack or the action(s) triggered by a policy that has been satisfied will not succeed. The admin password for connecting to the API server is stored in:

```
<securedetector_install_dir>/conf/default.conf
```

Administrators in VBUs have specific permissions associated with them. Therefore, logging in through the API will allow the administrator to perform tasks that only they have privileges to perform. Since you can only configure SecureDetector with one administrator, it is recommended that you choose a super user of SecureControl.

- **Password** - The password for this Administrator.
- **Admin Role** - The name of the Administrative Role.
- **Enable SSL** - Check this box to specify whether or not the API Server has been configured to require the use of SSL.

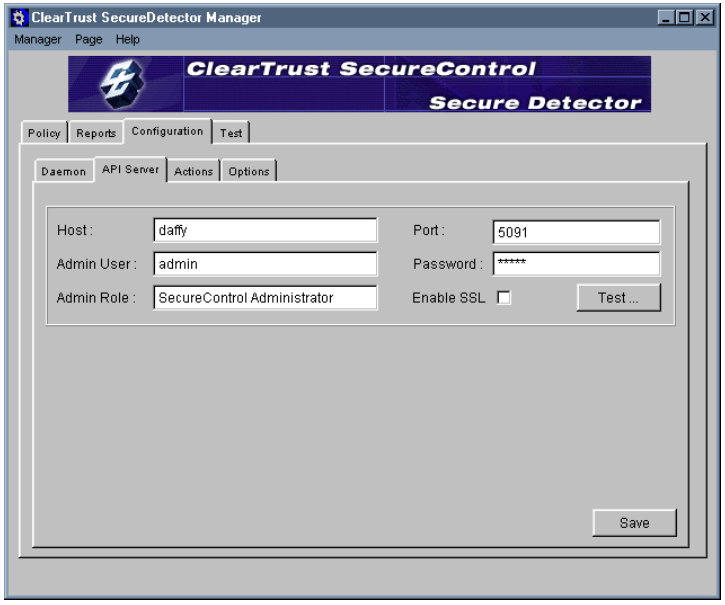


FIGURE 10-3: Configuration Panel Showing API Server Tab

4 Click **Save** to save the API server configuration.

5 Click **Test** to test that you can access the API server and that the Administrator you have specified can log on. When the test is complete, a dialog with the test status (access successful or exception) appears.

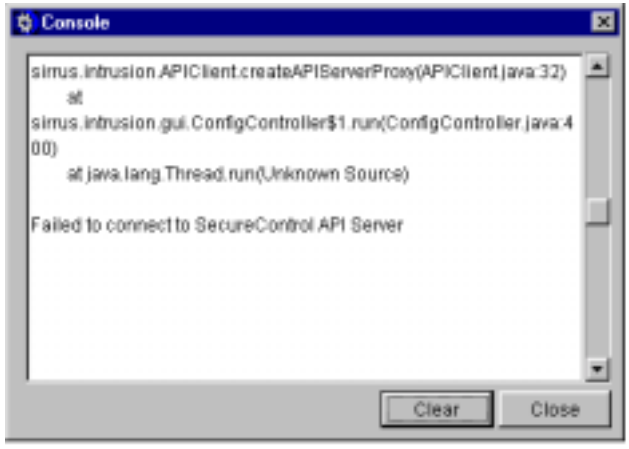


FIGURE 10-4: Test Console

Configuring Actions

You need to configure the type of action you want SecureDetector to take when it detects an attack. Once an attack is detected, SecureDetector can respond automatically by performing one of the following actions:

- Email an Administrator
- Suspend the account
- Disable the account
- Take a custom (user-defined) action

Adding an Action

To configure these actions:

1. From the SecureDetector Manager window, click the **Configuration** tab to access the Configuration panel.
2. From the **Configuration** panel, click the **Actions** tab to access the Actions panel. The first time you display this panel, there will be no actions displayed (you add actions through the Add button as you will see). The following screen shows some sample actions already added to the system.

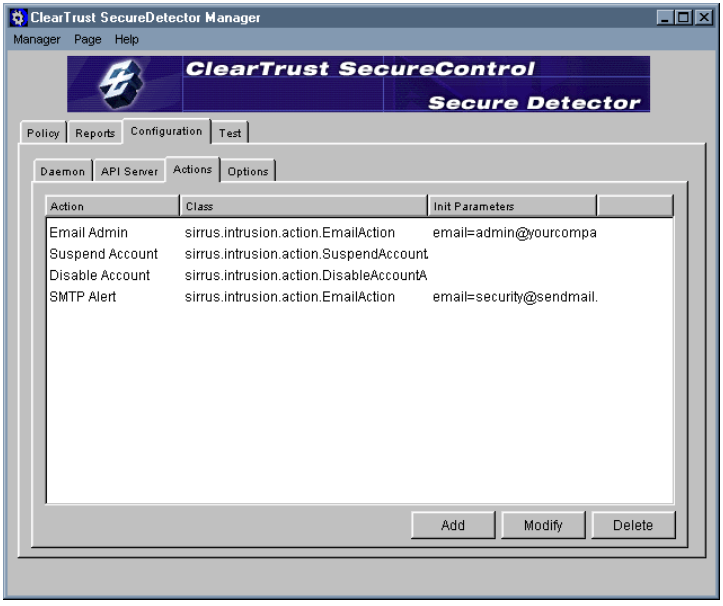


FIGURE 10-5: SecureDetector Configuration Panel Showing the Actions Tab

3 Click **Add** from the Actions panel to access the Load Class dialog. The Load Class dialog displays the available Java action classes.

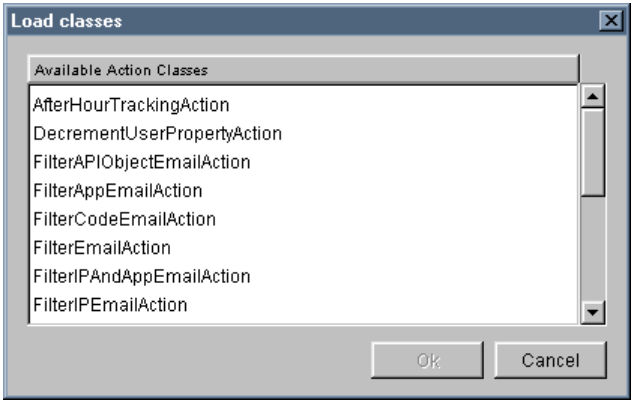


FIGURE 10-6: Load Class Dialog

4 In the Load Class dialog, highlight the fully qualified Java class name of the action that you want to add or modify.

5 Click **Ok** to add the Java class action. This Java class action will now appear in the Actions Panel f the Configuration Tab (or click the Cancel button to discard the action and re-display the Actions pane.)

Modifying an Action/Initialization Parameter

To modify an action/initialization parameter:

1 In the Actions panel, highlight the action you want to modify.

2 Click Modify to open the Modify Action dialog.

3 Change the action parameters as desired. Enter the Name of the action and the associated Class appears in the Class Field.

4 Modify the initialization parameters for the Java class as desired. Enter the Value for the initialization parameter.

5 Click the Apply button.

6 Click Ok to save your changes and return to the Actions panel, or click the Cancel button to discard the action and return to the Actions panel.

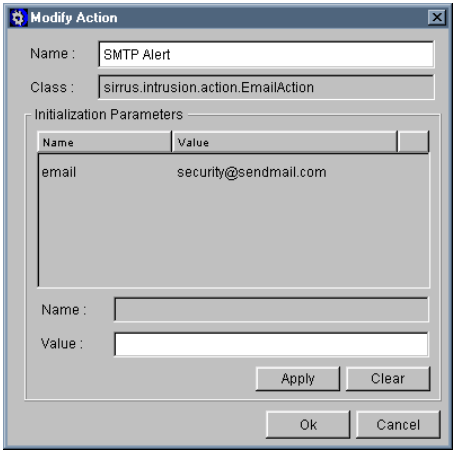


FIGURE 10-7: Modifying an Initialization Parameter

Customizable Actions SecureControl provides the following customizable actions. The following descriptions show you what you need to modify to change the defaults using the Modify Action/Initialization Parameter dialog as described above.

Name: sirrus.intrusion.action.EmailAction

Description: This action emails a specified user.

Initialization Parameter: Enter the email address, such as *yourname@yourcompany.com*.

Usage: Use this action when you want an email notification of an event. This action can be used with all events from any source.

Name: sirrus.intrusion.action.Suspend AccountAction.

Description: This action suspends a valid user for the days specified by *suspendTimeInDays*.

Initialization Parameter: Enter an integer to indicate the number of days from the current day to suspend the account. For example, if you set the integer value to 1, and the user is valid, the user will be suspended for one day starting immediately.

Usage: Apply this action to users, not to sources, when you want to suspend a user(s) associated with certain events from the User Activities source.

Name: sirrus.intrusion.action.DisableAccountAction.

Description: This action disables a valid user from the SecureControl system by enabling the lockout feature.

Initialization Parameter: None.

Usage: Apply this action to disable users associated with certain events from the User Activities source.

Name: sirrus.intrusion.action.DecrementUserPropertyAction.

Description: This action decrements and integer User Property specified by userPropertyName, by an amount specified by decrementalAmount.

Initialization Parameter: Enter a UserPropertyName, a string specifying the User Property to decrement.

Enter a decrementalAmount, an integer specifying the User Property to decrement.

Usage: Apply this action to decrement a user's User Property associated with certain events from the User Activities source. Do not apply this action to a source other than User Activities.

Name: sirrus.intrusion.action.IncrementUserPropertyAction.

Description: This action increments and integer User Property specified by userPropertyName, by an amount specified by decrementalAmount.

Initialization Parameter: Enter a UserPropertyName, a string specifying the User Property to decrement.

Enter an incrementalAmount, an integer specifying the User Property to increment.

Usage: Apply this action to increment a user's User Property associated with certain events from the User Activities source. Do not apply this action to a source other than User Activities.

Name: sirrus.intrusion.action.FilterAppEmailAction

Description: This action emails a user specified by email only if the specific application that was associated with the event is specified in the application(s).

Initialization Parameter: Enter an email address, specifying the destination of the email.

Enter an application(s) specifying the application(s) to filter from a user event. Separate each application with a space (for example, getBalance getTransactions, etc.).

Usage: Apply this action when you want to be notified if a user accesses a specific application. Only apply this action to User Activities.

Name: sirrus.intrusion.action.FilterCodeEmailAction

Description: This action emails a user specified by email only if the specific return code of an API event is specified by code.

Initialization Parameter: Enter an email address, specifying the destination of the email.

Enter a code specifying a code macro. The code macro can be one of these three:

INVALID_PASSWORD-an API event code where the invalid password is used to make an API call.

NOT_AUTHORIZED-an API event code where the administrator isn't authorized to perform an API call.

ADMINISTRATOR_NOT_FOUND-an API event code where an invalid administrator was used to make an API call.

Usage: Apply this action when you want to be notified if a specified return code of an API Transaction occurs. Only apply this action to API Transactions.

Name: sirrus.intrusion.action.FilterUserEmailAction

Description: This action emails a user specified by email only if the specific user that was associated with the event is specified in user(s).

Initialization Parameter: Enter an email address, specifying the destination of the email.

Enter a string specifying the user(s) to filter from an event. Separate the list with spaces.

Usage: Apply this action when you want to be notified if a specified user is associated with an event. Apply this action to all sources except for System Errors.

Name: sirrus.intrusion.action.FilterIPandAppEmailAction

Description: This action emails a user specified by email only if the specific IP and Application of a User event matches that of the IP Address(es) and application(s), respectively.

Initialization Parameter: Enter an email address, specifying the destination of the email.

Enter a string specifying an IP Address or list of IP Addresses. An IP Address can be 111.111.111.111., or 111.11.111.*.

Enter an application(s) specifying the application(s) to filter from a user event. Separate each application with a space (for example, getBalance getTransactions, etc.).

Usage: Apply this action when you want to be notified if a specified user from a specific IP address accesses a specified application(s). Only apply this action to User Activities sources.

Name: sirrus.intrusion.action.FilterIPEmailAction

Description: This action emails a user specified by email based on an IP address specified by IP Address(es).

Initialization Parameter: Enter an email address, specifying the destination of the email.

Enter a string specifying an IP Address or list of IP Addresses. An IP Address can be 111.111.111.111., or 111.11.111.*.

Usage: Apply this action when you want to be notified if a specified user from a specific IP address is associated with an event. Only apply this action to User Activities sources.

Name: TimeStampAction

Description: This action timestamps a User Property specified by userPropertyName.

Initialization Parameter: Enter a userPropertyName specifying a date user property to set to the current date.

Usage: Apply this action when you want to timestamp a specified User Property when an event occurs. Apply this action to all sources except System Errors.

Name: sirrus.intrusion.action.UpdatePropertyAction

Description: This action updates an integer User Property specified by the UserPropertyName. A user property UpdatePropertyActionProperty will be created if userPropertyName isn't set. The user property will be set to the newIntValue.

Initialization Parameter: Enter a userPropertyName specifying an int user property to set to the new IntValue.

Enter a newIntValue, specifying an integer value.

Usage: Apply this action when you want to update an integer User Property to newIntValue when an event occurs. Apply this action to all sources except System Errors.

Name: sirrus.intrusion.action.AfterHourTrackingAction

Description: This action updates a date User Property based on the parameter userPropertyName to the current time. If userPropertyName isn't set, a date user property AfterHourTrackingProperty is created. In order to track after hours usage, begin AfterHourTime and endAfterHourTime must be with the format hh:mm. The userPropertyName is a date of the last after hour access.

hh=the hour

mm=the minute

Initialization Parameter: Enter userPropertyName, specifying the current date.

Enter beginAfterHourTime, specifying the begin time of after hours.

Enter endAfterHourTime, specifying the end time of after hours.

Usage: Apply this action when you want to timestamp a user's last after hours event when an event occurs when triggered. Apply this action to all sources except System Errors.

Name: sirrus.intrusion.action.FilterAPIObjectEmailAction

Description: This action emails a user specified by email based on the objectType, and objectName of an API Transaction. objectName and API Transaction must be set in order to filter the correct object type and object name for an API Transaction. The type and name of the object is extracted from the description of the API Transaction log entry. In order to test an API Transaction policy that detects events 'Object Created','Object Modified', or 'Object Deleted', the description format should be of type: <objectCommand>[type=<objectType>, name=<ObjectName]. ObjectCommand can be arbitrary. ObjectName can be arbitrary. ObjectType can be of type: User, Group, Realm, WebServer, WebApplication.

Initialization Parameter: Enter email address.

Enter objectType, specifying the type of the object.

Enter objectName, specifying the name of the objectType.

Usage: Apply this action when you want be notified by email hen a specific object is modified by an API Transaction. Only apply this action to API Transaction events.

Name: sirrus.intrusion.action.TimeStampDeltaAction

Description: This action sets UserPropertyName to the current date if the time between the last access date specified by LastAccessPropertyName and the current time is greater than delta in minutes specified by deltaMin.

Initialization Parameter: Enter the userPropertyName, specifying a date user property to set to the current date.

Enter the lastAccessPropertyName, specifying a date user property to set to that last access date.

Enter deltaMin, an integer specifying the delta in minutes.

Usage: Apply this action when you want to timestamp a user's User Property for events from the User Activities source. Only apply this action to User Activities events.

Deleting an Action

To delete an action:

1. In the Actions panel, highlight the action you want to delete.
2. Click **Delete** to delete the action.
3. Click **Ok** to confirm your changes.

Re-using the Email Administrator Policy

At times, you may want to create an action and email administrators other than the one defined.

To re-use an existing email administrator policy:

1. From the SecureDetector Manager window, click the Configuration tab to open the Configuration panel.
2. From the Configuration panel, click the Actions tab to open the Actions panel.

3 Click Add to open the Load Classes dialog.

4 Enter sirrus.intrusion.action.EmailAction as the Class.

5 Enter an appropriate Name for the action.

6 Click Ok to display the Modify Action dialog.

7 In the fields at the bottom of the Modify Action dialog, enter the initialization parameter for the Java class.

- Enter an appropriate Name for the initialization parameter.
- Enter the actual email address of the person to notify when a threat is detected. Click the Add button.

8 Repeat step 7 to add other administrators to notify.

9 Click Add to add the parameter to the Initialization Parameters table.

Defining Attack Policies

You specify the types of suspicious activities which you want ClearTrust SecureDetector to monitor by defining attack policies. The SecureDetector Daemon then searches the event logs for patterns of activity that match the defined attack policies. When SecureDetector finds a match, it takes the configured actions.

To define attack policies:

1 From the SecureDetector Manager window, click the **Policy** tab to access the Policy panel.

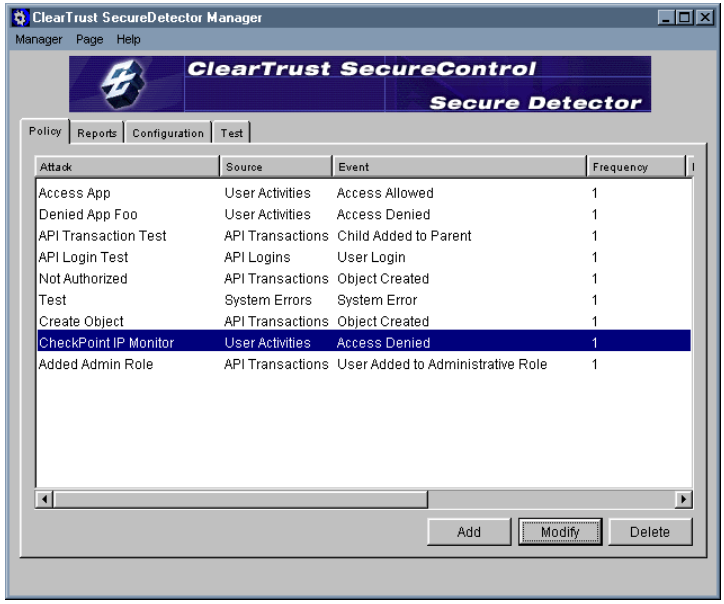


FIGURE 10-8: SecureDetector Policy Panel

2 Click **Add** to open the Define Attack dialog.

3 Enter the following information:

- **Attack Name** - The name you want to assign to the attack policy.
- **Source** - The source from which the attack originates. Use the pull-down menu to choose from *System Errors, User Event, Admin event, API Transactions, API Login, or API Errors*.
- **Event** - The event you for which you want SecureDetector to scan. Use the pull-down menu to choose from the list of possible events.

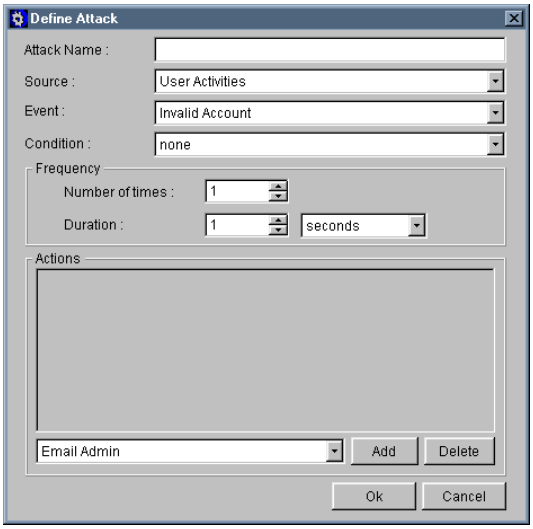


FIGURE 10-9: Define Attack Policy Panel

Condition - The condition for which you want SecureDetector to scan.

none - Monitor all events of the type you specified in the **Event** field.

same account - Monitor all events of the type you specified in the **Event** field that originate from the same account.

same IP address - Monitor all events of the type you specified in the **Event** field that originate from the same IP address.

same URI - Monitor all events of the type you specified in the **Event** field that are associated with the same URI.

Frequency - Define the number of an event beyond which you want SecureDetector to take the specified action. If the specified event and condition occur more than the specified **Number of times** within the specified **Duration**, SecureDetector takes the specified action(s).

4 Specify the action(s) that you want SecureDetector to take if the specified attack profile is detected.

- From the pull-down list box at the bottom of the Define Attack dialog, select an action. The actions available in this list are the actions you configured in the Configuration tab. For more information about configuring actions, refer to the section titled, “Configuring Actions”.
- Click **Add** to add the action to the list of actions in the Actions panel. To delete an action from the list, click the desired action to select it, then click **Delete**.

5 Repeat step 4 to specify additional actions.

6 Click **Ok** to save the event policy and return to the Policy tab.

Configuring Browser and Email Server Options

If you want to generate reports to a browser, you must specify the directory path for where the executable is located to launch the browser. For details about generating SecureDetector reports, refer to the section titled, “Generating Reports” later in this chapter. Similarly, if you want to configure an attack profile that includes an action of emailing an Administrator, you must configure mail server settings.

To configure browser and mail server options:

1 From the SecureDetector Manager window, click the **Configuration** tab to access the Configuration panel.

2 In the Configuration panel, click the **Options** tab to access the Options panel.

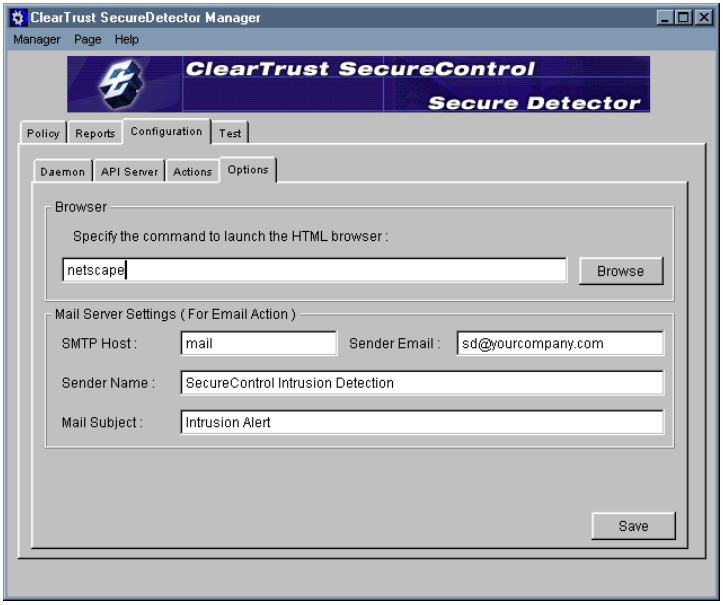


FIGURE 10-10: Configuration Panel Showing Options Tab

3 In the *Browser* area, enter the path to launch the HTML browser to which you want to generate reports. You can also use the **Browse** button to launch a dialog for navigating to the location of this file.

4 In the *Mail Server Settings* panel, enter the following information

- **SMTP Host** - The SMTP hostname for the mail server.
- **Sender Email** - The email address which will be inserted into the “from” field for emailed intrusion notification.
- **Sender Name** - The name which will be inserted into the “from” field for emailed intrusion notification.
- **Mail Subject** - The subject line to use on intrusion notifications.

5 Click **Save** to save your browser and mail server settings.

Testing Attack Policies

To ensure that you have configured your attack policies correctly, you can simulate suspicious events to test them.

To test an attack policy:

1 From the SecureDetector window, click the **Test** tab to access the Test panel.

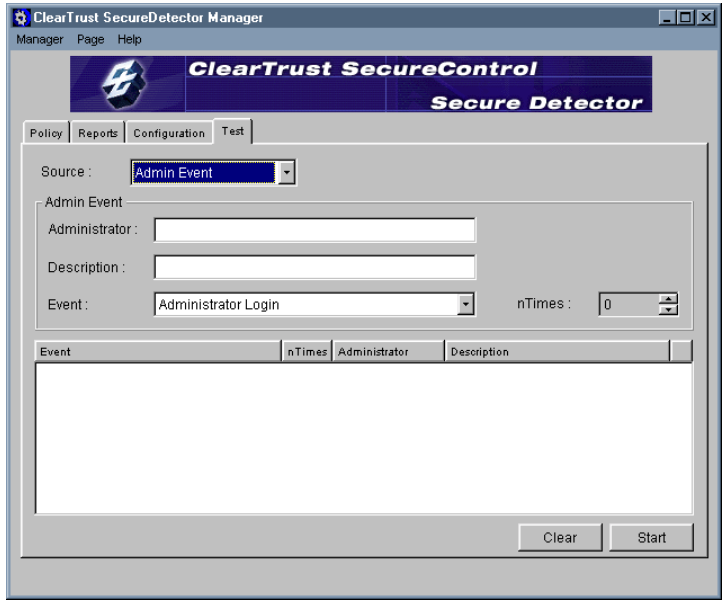


FIGURE 10-11: SecureDetector Test Panel

2 Make sure Daemon is running and then set up the event simulation.

- SecureDetector monitors activity that originates from a variety of different sources, including System Errors, User Events, Admin Events, API Transactions, API Logins, and API Errors. The system defaults to System Errors but you can select a different **Source** from the pull-down menu.
- For each Source, the system prompts you for different information as shown below:

System Errors

1 Enter a Description of the System Error.

2 Enter an Exception for the System Error.

3 From the pull-down menu, select the type of Event you would like SecureDetector to monitor.

4 From the pull-down menu, select the number of times this activity should occur before SecureDetector responds.

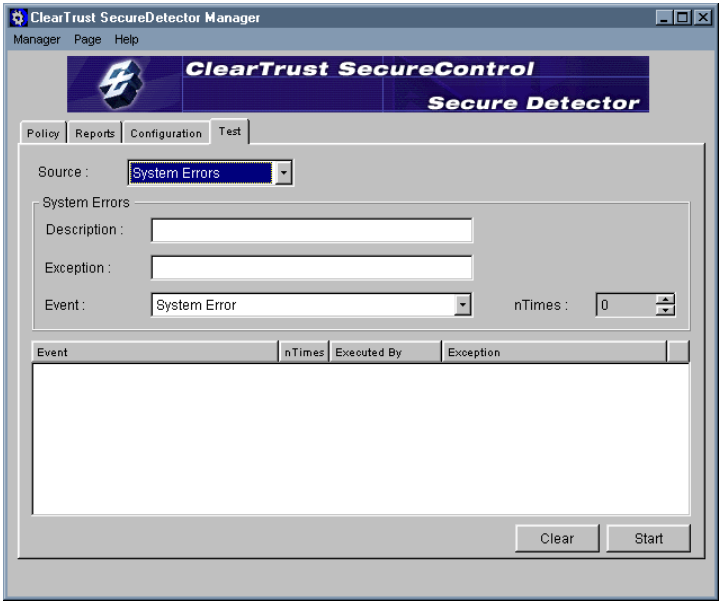


FIGURE 10-12: SecureDetector Test Panel: System Errors

User Event

1 Enter the Username and IP Address from which the event will originate.

2 Enter the Application and the URI to attempt to access.

3 From the pull-down menu, select the type of Event you would like SecureDetector to monitor.

4 From the pull-down menu, select the number of times this activity should occur before SecureDetector responds.

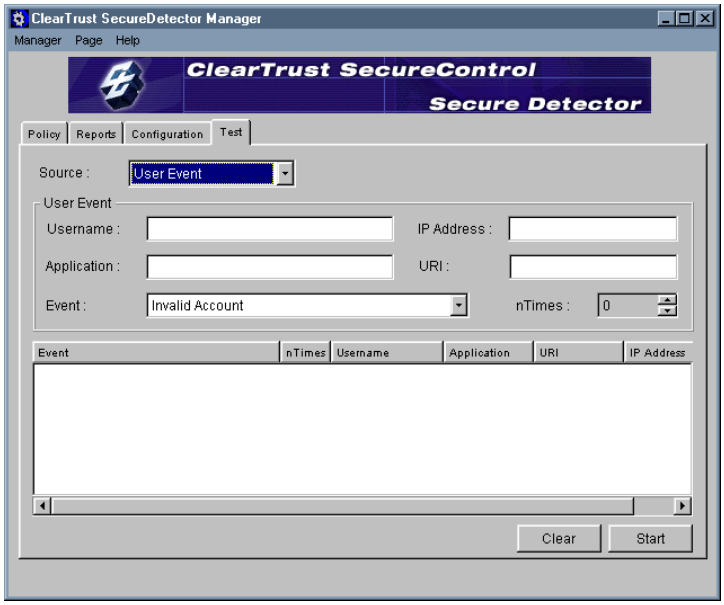


FIGURE 10-13: SecureDetector Test Panel: User Events

Admin Event

1. Enter the Administrator you want SecureDetector to monitor.
2. Enter a Description of the Admin Event.
3. The type of Event SecureDetector monitors is shown in the pull-down menu as an Admin Activity Event.
4. From the pull-down menu, select the number of times this activity should occur before SecureDetector responds.

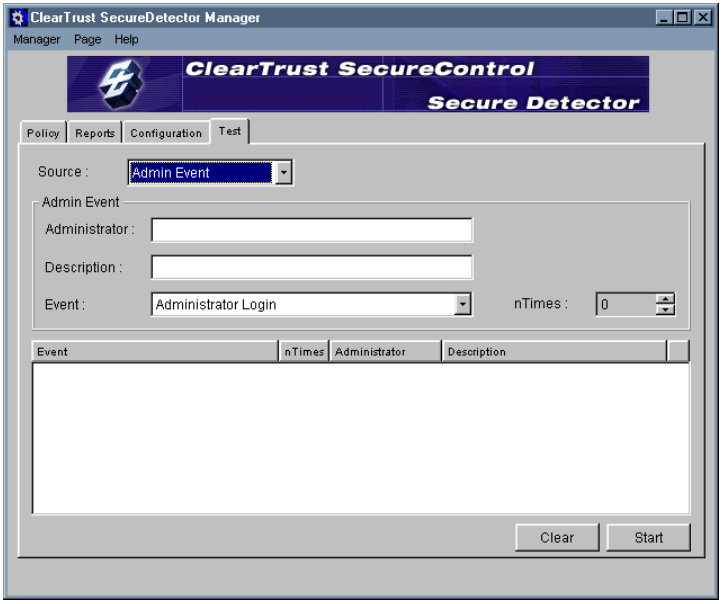


FIGURE 10-14: SecureDetector Test Panel: Administrator Events

API Transaction

1. Enter the Administrator's name in the Executed by field.
2. Enter a Result Code.
3. The type of Event SecureDetector monitors is shown in the pull-down menu as an API Transaction Event.
4. From the pull-down menu, select the number of times this activity should occur before SecureDetector responds.

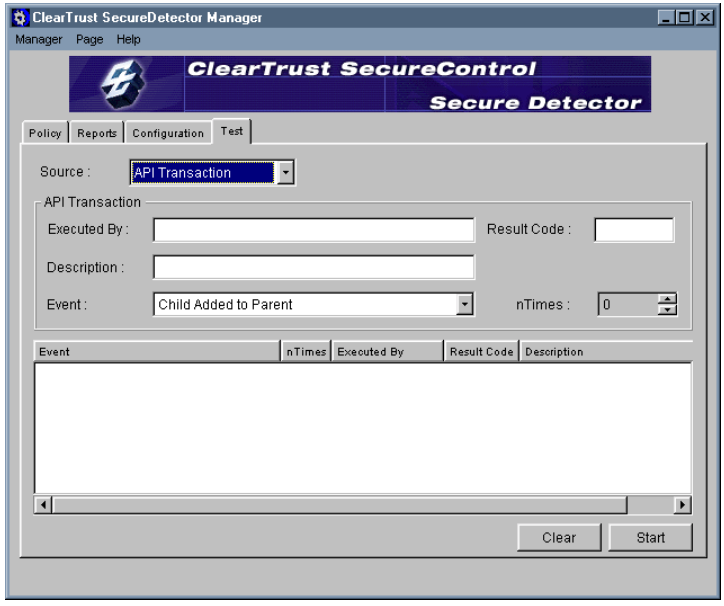


FIGURE 10-15: SecureDetector Test Panel: API Transaction Errors

API Login

1. Enter the Administrator you want SecureDetector to monitor.
2. Enter a Description of the Admin Event.
3. The type of Event SecureDetector monitors is shown in the pull-down menu as an API Login Event.
4. From the pull-down menu, select the number of times this activity should occur before SecureDetector responds.

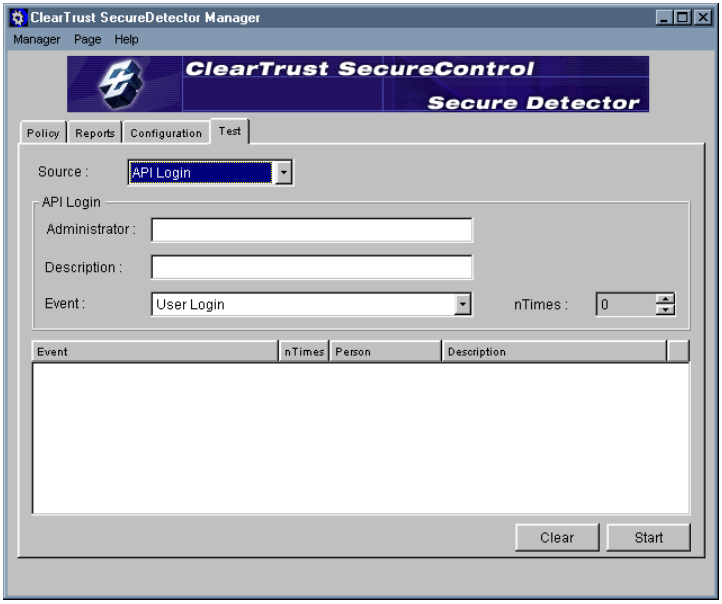


FIGURE 10-16: SecureDetector Test Panel: API Login Errors

API Errors

1. Enter the Administrator's name in the Executed by field.
2. Enter a Result Code.
3. The type of Event SecureDetector monitors is shown in the pull-down menu as an API Error Event.
4. From the pull-down menu, select the number of times this activity should occur before SecureDetector responds.

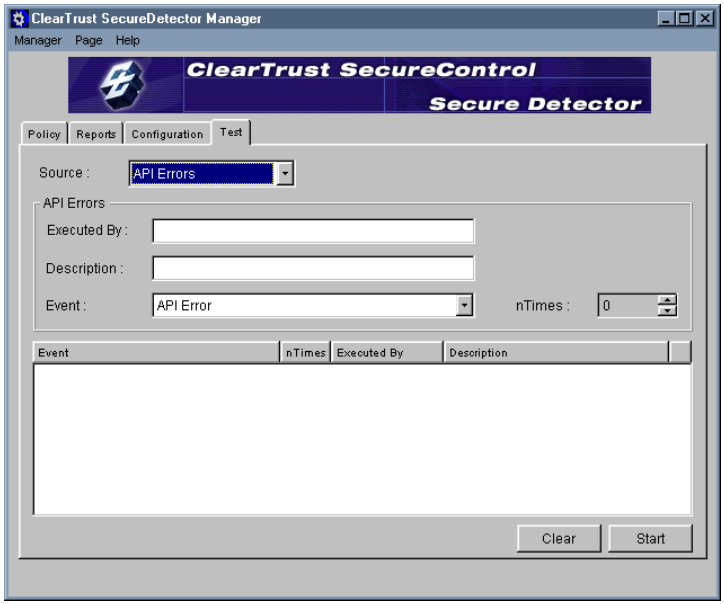


FIGURE 10-17: SecureDetector Test Panel: API Errors

5 Click Start to run the test. A pop-up dialog appears and displays the status of the simulation.

6 Determine whether your event policies are in place by generating a report and checking to make sure that the specified attacks were detected. For more information about generating SecureDetector reports, refer to the section titled, “Generating Reports”.

7 Determine whether the specified actions were taken by validating that an email was sent to the specified Administrator or that the specified account was suspended or disabled.

Generating Reports

To generate SecureDetector reports:

1 From the SecureDetector window, click the Reports tab to access the Reports panel.

2 Highlight the report you want to generate. SecureDetector allows you to generate different types of reports, including Violating IP Addresses, Attack Log Summary, Attack Resource Summary, Suspicious Users Report, Search Attack Log, Event View, Search Event Log, and Attack Log.

3 Certain reports allow you to select a source for a summary of events.When you select Attack Log Summary, Event View, and Attack Log, the Select Source dialog appears. Highlight the source for the activities you want reported.

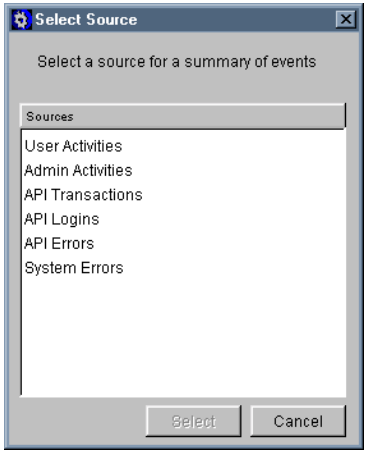


FIGURE 10-18: Select Source Dialog

4 Highlight the source you want to select for reporting and click Select.

5 When you select the Search Event Log report, the following dialog appears. Select the Source of the event from the pull-down menu and then select the event from the Event pull-down.

6 Enter the Username and IP Address for the source and the event you are searching on.

7 Click Search.

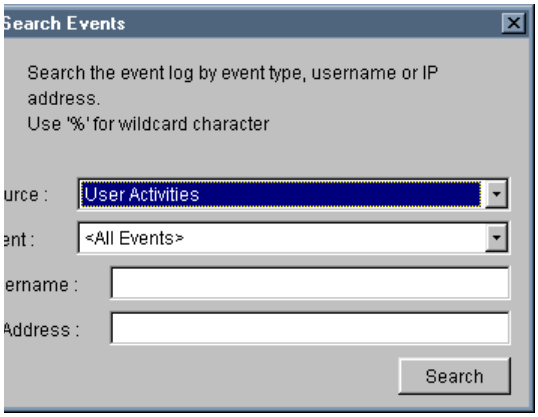


Figure 10-1. Search Events Dialog

1. When you select the Search Event Log report, the following dialog appears.

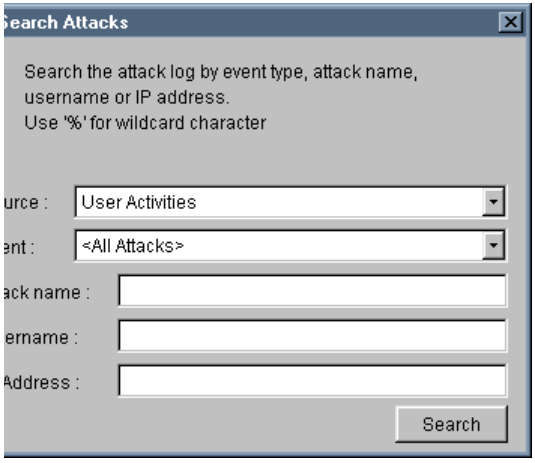


Figure 10-2. Search Attacks Dialog

2. Select the Source of the event from the pull-down menu and then select the event from the Event pull-down.

3. Enter the Attack name, the Username and IP Address for the source and the event you are searching on.

4. Click **Search**.

5. Specify whether you want to generate the report **to browser** or **to file** by selecting the appropriate radio button.
   Note: If you choose to generate a report to a browser, you must configure the path to locate the browser. Refer to the section titled, "Configuring Browser and Email Server Options" earlier in this chapter for more information.

   Note: Generating reports to Netscape browser (Netscape Communicator 4.7 on the Solaris platform) may result in an error message and not display automatically (although the report will be generated to an .html file). To workaround this conflict between the Java runtime environment and Netscape 4.7, find the file "Dt" (located in the /usr/dt/app-defaults/ directory) and rename it to "Dt.bak" (delete Dt to get it out of the way.

6. Click **Generate** to generate the report.

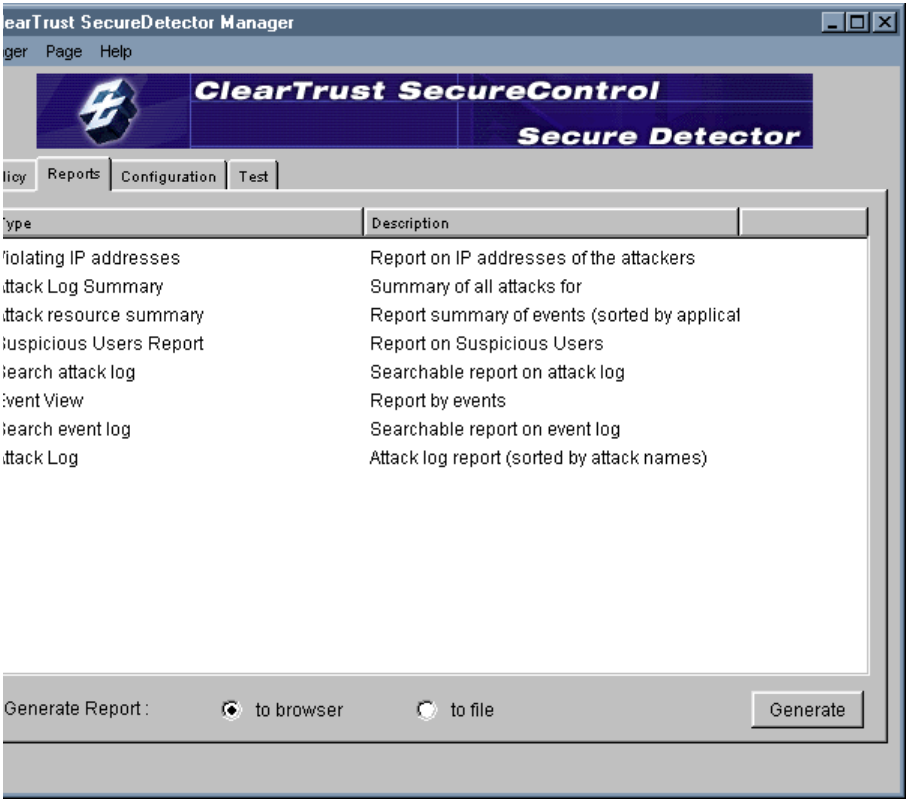


Figure 10-3. SecureDetector Reports Panel

Appendix A
Algorithm Reference: Authentication, Authorization, and SSO Processing

This appendix describes the algorithms for processing Authentication, Authorization, and Single Sign-On. It includes the following sections:

- Authentication Processing
- Authorization Processing
- Single Sign-On Processing

Authentication Processing

When an Authorization Server receives an Authentication request from either a ClearTrust-enabled Web Server or from a ClearTrust API Client, it performs the steps illustrated in Figure A-1 for validation.

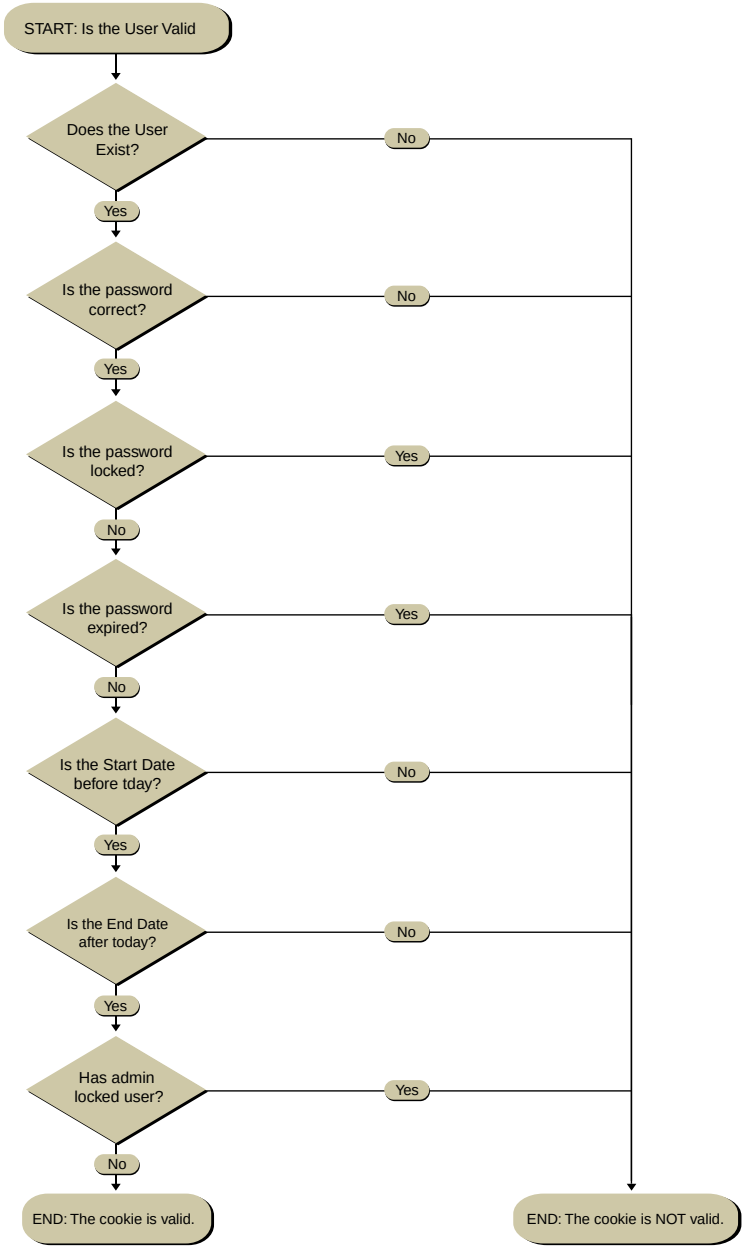


FIGURE A-1: Authentication Processing Algorithm

Authorization Processing

When an Authorization Server receives an Authorization request from either a ClearTrust-enabled Web Server or from a ClearTrust API Client, it performs the steps illustrated in Figure A-2 for authorization.

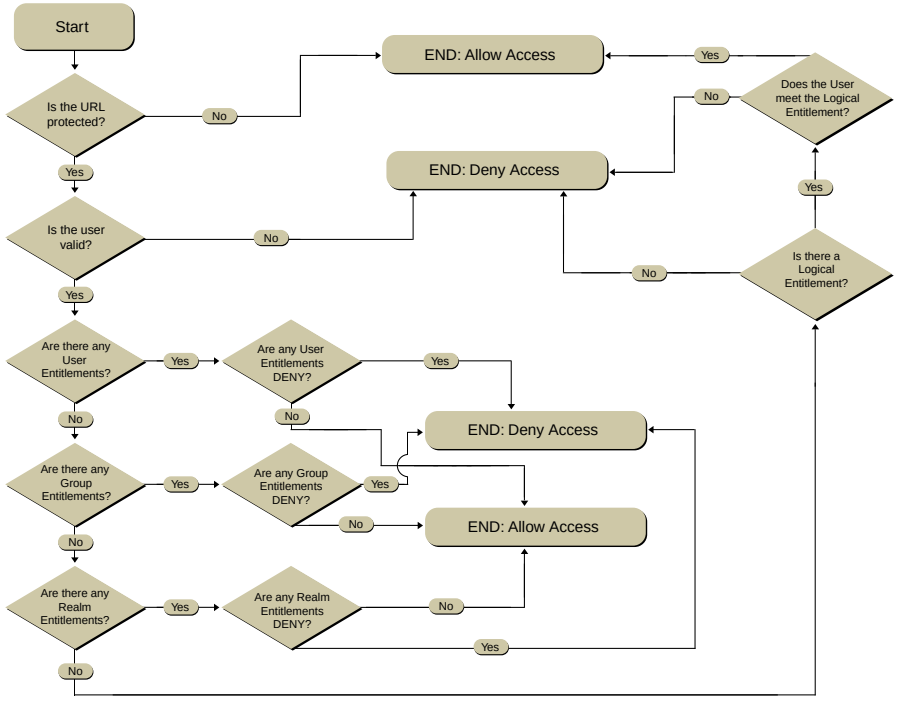


FIGURE A-2: Authorization Processing Algorithm

Single Sign-On Processing

ClearTrust can provide common user IDs and passwords across all of your Web Servers. With ClearTrust's Single Sign-On functionality, Users do not have to re-enter their IDs and passwords for each new Web Server they encounter. Although authorization is still separate for each Application, once Users have authenticated themselves to one ClearTrust-enabled Web Server, they do not have to re-authenticate when they browse to other Web Servers.

For details about how to configure Single Sign-On, see the *ClearTrust SecureControl Installation and Configuration Guide*.

ClearTrust enforces two separate time limits on User sessions:

- **Idle Timeout**—When a User has not accessed a ClearTrust-enabled Web Server for more than the value specified as the Idle Timeout, the User's session is no longer valid. The next time the User tries to access a ClearTrust-enabled Web Server, he or she must re-authenticate. The Idle Timeout is typically set to some number of minutes.
- **Session Length**—This value places a limit on the amount of time a User can access ClearTrust-enabled Web Servers without re-authenticating. Once the Session Length has been exceeded, the User is asked to re-enter his or her user ID and password. The Session Length is typically set to some number of hours.

Figure A-3 illustrates the algorithm used to process these Single Sign-On time limits.

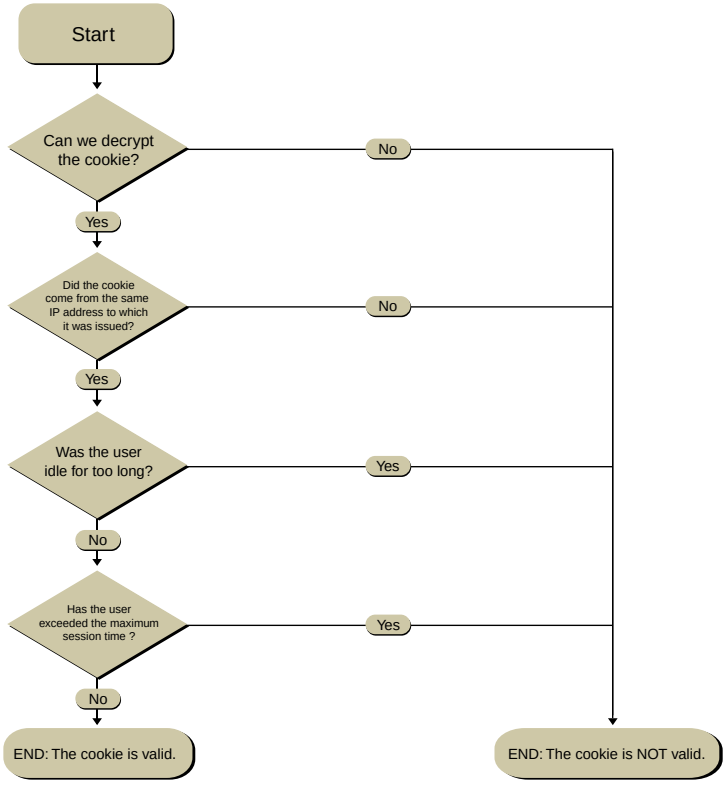


FIGURE A-3: Single Sign-On Processing Algorithm

Index

P

R

S

T

U

V

W