eTrust™ Single Sign-On

Getting Started

r8

Second Edition

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

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

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

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

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

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

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

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

© 2005 Computer Associates International, Inc.

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Contents

Chapter 1: Introduction to eTrust SSO

The Purpose of this Guide 1-1
Documentation 1-2
Advantages of Using CA Products 1-2
Advantages of Using eTrust SSO 1-4

Chapter 2: Introduction to eTrust IAM

eTrust IAM Product Suite 2-2
Common Components 2-2
Computer Roles 2-3
IA Manager 2-4
IA Manager Navigation 2-5

Chapter 3: Installing eTrust SSO

Overview of the Installation 3-2
Before You Begin the eTrust SSO Installation 3-3
Install the IAM Common Components 3-4

Chapter 4: Concepts Behind eTrust SSO

End Users 4-1
Primary Authentication 4-3
Applications in eTrust SSO 4-4
Scripts 4-5
Session Profiles 4-6
Resources 4-7
Policies 4-8

Chapter 5: Tour of eTrust SSO Components

Architectural Overview 5-2
SSO Client 5-3
Policy Manager 5-3
IA Manager 5-4
IAM Common Components 5-5
Data Stores 5-7

Chapter 6: Common eTrust SSO Processes

Authenticating Users 6-2
Launching Applications 6-5
Synchronizing Passwords 6-7

Chapter 7: Basic Tasks Using IA Manager

Manage Accounts 7-1
Manage Applications 7-5

Chapter 8: Basic Tasks Using Policy Manager

Policy Manager Navigation 8-2
Users 8-6
User Groups 8-8
Administrators 8-11
Sessions 8-14
Password Policies 8-19

Chapter 9: Frequently Asked Questions

Functionality and Benefits 9-1
Passwords and Logon 9-2
Authentication 9-4
Implementation 9-5
Integration 9-6

Chapter 1

Introduction to eTrust SSO

eTrust™ Single Sign-On (eTrust SSO) is a system that you can configure so that end users only have to authenticate (log on and identify themselves) once to gain access to all of their secure desktop applications.

The purpose of eTrust SSO is to:

- Simplify the logon and authentication process for end users
- Restrict access to specific data and applications on the network
- Create a more secure network environment
- Give administrators efficient and secure control over resources

Case study

Max works for a large corporation. During the course of his day, Max has to log on to six different applications. He has to remember a different password for each one (many of them have different password requirements such as length, character set and change dates). To remember all the passwords, Max has to write them down. If Max had eTrust SSO he would only need to remember one password to gain access to all his secure applications.

The Purpose of this Guide

The purpose of this guide is to introduce you to eTrust SSO. This guide is primarily aimed at administrators who have not worked with eTrust SSO before, but is also useful for administrators who have worked with earlier versions of eTrust SSO and managers interested in an overview of eTrust SSO. When you finish this guide, you will be familiar with the basic functionality and applications of this product.

Documentation

After reading through this guide, you can refer to the numerous other resources available to you for additional information. You can reference all the eTrust SSO user guides from the eTrust IAM Common Components Documentation CD. These guides will help you install and use eTrust SSO.

Advantages of Using CA Products

Computer Associates (CA) products can be used individually, in conjunction with other CA products, or with a number of third party software products.

When it comes to getting on the information fast track, CA Services can recommend and install a full suite of portal and knowledge management solutions to keep your business moving. Our associates offer the proprietary know-how on custom-fitting your enterprise for solutions ranging from life cycle management, data warehousing, and next-level business intelligence. Our experts leave you with the technology and knowledge tools to fully collect, exploit, and leverage your data resources and applications.

eTrust Product Suite

Security remains one of today's most pressing IT concerns. CA's eTrust solutions secure enterprise resources and provide organizations with a holistic view of the IT and physical infrastructure. Grouped into three solution areas — eTrust Identity Management, eTrust Access Management, and eTrust Threat Management, all with consistent visualization through eTrust Security Command Center — CA's eTrust solutions help organizations take control of security. Through CA's strength in management, commitment to security research, continued innovation, and openness to work with partners, eTrust provides organizations with the power to secure their entire enterprise.

CA Education Services

The more effectively and efficiently you are able to use your CA product, the more it contributes to the success of your company. CA develops its education programs to help you get the most out of the products you have installed.

To take advantage of the product functions that work best for you, your staff must know what each of the functions achieve, how to implement them, and how to use them best in daily operations. Computer Associates education programs can provide the training to give your staff the knowledge and skills to make this possible. For more information, see www.ca.com/education.

CA Technology Services

Nobody knows CA technology solutions better than CA Technology Services. Our consulting teams work closely with CA Education to provide seamless implementation consulting that builds on the knowledge your staff acquires in our training curriculum. With direct access to CA Product Development and Support, CA Technology Services consultants can leverage best practices to ensure that your implementation goes smoothly.

CA Technology Services offers both customized and packaged services to meet your needs. From assessments to implementations to migration assistance, CA Technology Services offers the right assistance at the right time to shorten your deployment cycle and maximize your productivity. For more information, see www.ca.com/services.

CA User Groups

CA User Groups provide a forum for discussing current product releases, product enhancements, and future directions. With over 200 recognized User Groups worldwide, one is sure to meet your needs.

Computer Associates understands that their partnership with CA Recognized User Groups is of great importance, and endorses and encourages the formation of user groups, advisory boards, and executive committees. We recognize that these groups play an important role in ensuring active and ongoing communications between our clients and our development and support personnel. For more information, see www3.ca.com/support.

Customer Support

Our Technical Support site on the World Wide Web is the most comprehensive online resource that we provide. The site offers access to the same searchable support databases that our Technical Analysts use. The databases contain thousands of documented technical issues for all of our products.

For online technical assistance and a complete list of locations and phone numbers, contact Customer Support at http://ca.com/supportconnect. Customer support is available 24 hours a day, 7 days a week.

For telephone assistance, call:

- U.S. and Canada 1-800-645-3042
- International (1) 631-342-4683

Advantages of Using eTrust SSO

You can group the advantages and features of eTrust SSO into four main categories:

- Benefits for end users
- Benefits for administrators
- Enhanced security
- Enhanced flexibility

Benefits for End Users

Why burden your users with the need to remember multiple sign-on processes, IDs, or passwords? There is a better, simpler way with eTrust SSO.

eTrust SSO provides a smooth transitional experience and familiar interface for end users to help them move to a more secure network environment with minimal disruption to their working routine.

Besides smooth implementation, eTrust SSO also creates convenient end-user access to secure applications and provides a customized list of applications that the end user can access.

Compatibility with Applications and Environments

eTrust SSO can simplify logons to virtually any network application. Applications commonly used in eTrust SSO include email packages, secure databases, and legacy applications.

The most obvious benefit from eTrust SSO is that you can configure it so that your users can access all of their secure applications via eTrust SSO and only have to authenticate once. You can configure eTrust SSO to log on to applications based on the following environments:

- Windows
- Web
- UNIX
- Mainframe

Web Logon Security

eTrust SSO has advanced HTML Web support that enables you to secure and manage your corporate web sites quickly and efficiently. eTrust SSO for the Web handles both in-house and external HTML Web applications, and not only permits smooth access, but also enables you to personalize the user interface for each user. Once a user is authenticated to the eTrust SSO system, access to all authorized HTML Web applications and resources is handled by eTrust SSO.

Fewer Password Resets

Users often forget a password when they return from leave, or have to log on to a system that they do not access frequently. This leads to frustration and downtime. eTrust SSO can help reduce user inactivity due to lost, forgotten, or compromised passwords. This directly improves business productivity and the bottom line by reducing help desk costs and decreasing downtime for end users.

eTrust SSO creates a solution that means users only need to remember one authentication process to access all of their secure applications.

Familiar Interface

You can seamlessly integrate eTrust SSO with the end users' current Windows desktop interface through either the Start menu or using desktop icons. This means that end users are more likely to quickly accept eTrust SSO because they are not required to learn a new system.

Personalized Application Lists

You can configure eTrust SSO so that each user only sees the applications they actually use. This improves productivity and provides a smooth and simple user experience.

Application Migration

If your company has a Citrix Metaframe client-server environment, users can transfer an application session launched through eTrust SSO from one workstation to another. This feature is only available when eTrust SSO is deployed with a Citrix Metaframe client-server environment. Citrix products are sold independently of eTrust SSO.

Using Metaframe Application Migration, a user can log on to eTrust SSO on workstation A, open an application from their eTrust SSO list, and start working on that application (this is standard eTrust SSO functionality). The user can then move to workstation B, log on to eTrust SSO, launch the *same* application, and continue working where they left off because their original session has been transferred (migrated) to the second workstation. Citrix Application Migration works with multiple application sessions.

Case study

A doctor logs in to eTrust SSO on workstation A, and opens the Patient History application from the eTrust SSO list. The doctor then gets called away to another ward but wants to continue working on the same patient history in the new ward. Using Metaframe Application Migration, the doctor simply has to log on to eTrust SSO on workstation B and reopen Patient History. The application automatically opens exactly where the doctor was last working.

Shared Local Workstations

You can implement and use eTrust SSO in a shared workstation environment. This means that you can designate and configure common computers so that any eTrust SSO user can log on and see their own secure applications, while the desktop remains the same.

Benefits for Administrators

eTrust SSO has significant benefits for administrators and reduces the overall administration overhead of a secure logon system.

eTrust SSO provides administrators with obvious benefits such as a significantly reduced number of password resets, a clear central management GUI, and flexible tools to configure and administer the system.

Fewer Password Resets

In an eTrust SSO environment, end users have fewer passwords and need fewer password resets, which reduces the number of help desk calls. This frees Help Desk technicians and administrators for more important tasks and saves valuable system and security administrator resources.

Easily Updated Users and User Access

Managing identities is a major security challenge. IT security departments must quickly get internal users online and productive, while controlling access to corporate resources based on the business identity of external users and partners. eTrust SSO lets administrators add new users efficiently.

Centralized Management GUI

You can use either of the central administration tools, the IA Manager or the Policy Manager, to set and maintain the entire organization's access strategy.

This management GUI also means that behind the scenes, system or security administrators can implement security controls without interfering with user logons.

Flexible Administrator Tools

eTrust SSO lets administrators interact with the Policy Server in three different ways:

Tool	Interface	Used to
Policy Manager	Windows GUI	Set up and administer eTrust SSO.
IA Manager	Web GUI	▪ View and terminate specific eTrust SSO sessions for specific users. ▪ Manage users, groups and accounts ▪ Manage access to applications
selang	Command line language	Upload large amounts of data directly into the Policy Server data stores. For more information, see the *eTrust SSO selang Command Reference Guide.*

IA Manager Session Administration

Users can be logged into multiple eTrust SSO sessions concurrently on different computers, unless limits are set in the Policy Manager. Administrators can track and manage those sessions using the IA Manager.

The eTrust SSO IA Manager gives administrators the power to view and terminate a user's eTrust SSO session on the network. The IA Manager is a web-based GUI that comes as part of the eTrust IAM suite.

The IA Manager lets administrators:

- View users logged on to eTrust SSO
- Terminate all sessions associated with one user
- Terminate individual sessions associated with one user
- Terminate all sessions for all users

For information about how to configure the Policy Manager to automatically restrict the number of concurrent sessions an eTrust SSO user can have, see the Session Management Settings section later in this chapter.

Easy Troubleshooting

eTrust SSO gives administrators the tools to easily troubleshoot and solve any problems using eTrust Audit and eTrust Client logging tools. This saves time and creates a more secure environment.

The Policy Server can write log messages to eTrust Audit. eTrust Audit is a centralized auditing application that collects and stores designated information from UNIX and Windows servers and other eTrust products, including eTrust SSO. eTrust Audit is available independently from eTrust SSO.

You can also configure the SSO Client to log issues with the client. This assists with the resolution of any problems that may occur on the client-side.

Enhanced Security

eTrust SSO enhances overall security by automating access to all of your authorized enterprise-wide applications and systems that have a single logon, including Web applications.

In today's distributed computing environments, users sign on to many different applications and systems — including e-mail, networks, databases, and Web servers — each typically requiring its own security procedure. The more systems each user must navigate, the more IDs and passwords they must remember, and the greater the likelihood of user errors and compromised security. In other words, multiple passwords result in multiple security risks.

Fewer Visibly Recorded Passwords

Users will no longer have to remember multiple passwords, which means they are less likely to write down their passwords on bits of paper, or create a file on their computer that records all their passwords.

More Secure Authentication

When users have to remember multiple passwords, they often choose short, simple passwords including names, dictionary words, and birthdays. Users are also likely to use the same passwords for multiple systems.

Because eTrust SSO reduces the number of passwords that a user has to remember, they are more likely to choose a secure password.

Not only are users more inclined to select secure passwords, but you can configure eTrust SSO to force users to select secure passwords and to give them online reminders about this.

You can also implement biometric authentication (such as iris or finger-print scanning) or two-factor authentication such as smart cards for greater security.

Password Management

Password-enhancing mechanisms include password auto-generation, password policies, and password exits for adding self-defined quality checks according to the needs of the enterprise.

The *strength* of passwords is set in the Policy Manager, and insecure passwords are rejected.

eTrust SSO can also keep passwords for target applications synchronized with the primary authentication password, addressing such requirements as remote access with a single password.

Sensitive Application Mode

You have the option to designate certain applications as *sensitive*, which means that users are required to re-authenticate themselves when they launch this application through eTrust SSO. While this negates some of the convenience of the single sign-on functionality, it does give particular protection to highly sensitive applications or information, which may even have a legal requirement to be even more highly protected than usual.

Passwords Securely Stored

Users' IDs and passwords are stored in one central and secure location – on either a UNIX or Windows server – using the Policy Server. You can store these User IDs in the Access Control database or alternatively in an LDAP compliant data store such as eTrust Directory (which comes with eTrust SSO) or Microsoft Active Directory. This creates a secure environment to stores users' credentials.

Session Management Settings

Users can log on to multiple eTrust SSO sessions concurrently on different computers. This is important flexibility for many users, but also must be managed for security reasons. You can configure eTrust SSO to limit the number of sessions a user can have open at one time.

Session management also helps to protect sensitive data left unattended on a workstation because it can be used with Windows screen lock.

Session management can:

- Keep count of how many active logons a user currently has
- Reject a new logon by a user when they reach their set limit
- Log the user out at any moment, either manually, or when triggered by an event
- Be used with Windows screen lock
- Close old sessions when opening a new one

These features are defined on the Policy Server using the Policy Manager.

For information about how administrators can manually manage and terminate User Sessions, see the IA Manager Session Administration section in this chapter.

Secure Network Traffic

All information communicated between the eTrust SSO components is fully encrypted.

One-Time Password Capability

The One-Time Password (OTP) functionality increases eTrust SSO password security for UNIX applications that transmit passwords in clear text, such as Telnet.

As soon as you log onto a remote server, eTrust SSO OTP agent connects to that server and changes your password so that anyone who intercepted the clear text password cannot use it to gain access to the server.

Secure Authentication

eTrust SSO provides its own method of authentication and also supports several third-party authentication methods so you can choose which authentication method best suits the needs of your enterprise.

With the support of several third-party user authentication methods, eTrust SSO lets administrators strengthen and customize the logon process based on the sensitivity of the protected resource.

eTrust SSO supports the following authentication methods:

Authentication Software	Authentication Method
eTrust SSO	Password
LDAP	Password
Novell	Password
Windows	Password
Entrust	Digital certificates
Certificate	Digital certificates
RSA SecurID	Secure ID card + PIN
Safeword	Token

If you want to use an authentication method not listed here, you can use the eTrust SSO Integration Kit to create your own authentication agent to integrate eTrust SSO with third-party methods such as Kerberos, smartcards, or biometrics.

Enhanced Flexibility

eTrust SSO is built to be flexible, so when your business changes, it can change too.

Identity and Access Management (eTrust IAM)

eTrust SSO is now part of a suite of products called eTrust Identity and Access Management (eTrust IAM).

eTrust IAM gives you a common architecture and user interface for all products within the eTrust IAM suite. This means that we have changed the product infrastructure to make it integrate more easily with the other products in the eTrust IAM suite, and we have provided a new management interface called the Identity and Access Manager (IA Manager).

Product Suite

The eTrust IAM suite is comprised of the following products:

eTrust Admin
Supplies policy-based user and access rights provisioning.

eTrust Access Control
Provides end-to-end platform and system resource security.

eTrust Single Sign-On
Provides complete enterprise single sign-on to both desktop and web-based applications.

eTrust Web Access Control
Enables secure intranet and extranet management.

Benefits of the Suite

The benefits of the eTrust IAM suite include:

Streamlined management process
The state-of-the-art management interface gives you the ability to fully manage a user from hire to retire. All user identities across different systems are created, modified, suspended, revoked or removed according to role and policy.

Increased revenues
Seamless integration across a secure, open platform permits fast deployment and reduced complexity, enabling a quick return on investment.

Reduced security risks
Centralized identity management and access rights enforcement reduces the problem of privilege creep (the accumulation of privileges during employment that become inappropriate as an employee changes roles) and the possibility of old identities remaining active in the system after termination.

Protected investments and growth with new technology
The modular, open design of eTrust IAM provides standards-based interfaces to existing and future investments in security technology. It accommodates additional integration of eTrust IAM and third-party products.

Assisted regulatory compliance
Integrated, powerful security, auditing, and reporting capabilities enhance support for regulatory compliance. The strong security features also protect privacy-related information.

Phased Implementation

Organizations can implement eTrust SSO in phases, based on where the user need is greatest and which applications are the most critical. eTrust SSO can then be deployed in stages to other business units or departments.

This lets you reap benefits from eTrust SSO very quickly and maintain a stable environment as you migrate to the new system.

Legacy Systems Integration

Most companies want to be able to use or migrate from legacy systems and data until they are ready to decommission the application or data in a controlled way. Using eTrust SSO, you can leave mission-critical legacy systems in place and create a high-security layer around them. This also means that legacy systems can be phased out gradually.

eTrust SSO is available for mainframe applications so that users can access legacy mainframe applications from their personal eTrust SSO application list.

For information about how you can reuse user information from existing legacy systems, see the Easily Populated Databases section in this chapter.

Easily Populated Databases

In the past, building a single sign-on database was a time-consuming and resource-intensive process. eTrust SSO provides unique facilities that automatically create a central repository for user IDs and passwords. It also provides the tools to quickly populate those data repositories with existing data you may have from a legacy system.

Multiple Authentication Methods

When you implement eTrust SSO, you can use one of the authentication methods that come with eTrust SSO, or you can select a third-party authentication method.

eTrust SSO has been developed to work with multiple third-party authentication software and hardware systems. eTrust SSO comes ready to use with several external authentication methods, or you can use the API to create your own interface to any other system.

Scalable Data Store

eTrust SSO has a directory data store (eTrust Directory) specially designed to safely and efficiently handle large numbers of users. When eTrust SSO is deployed in a server farm environment, it can be scaled to accommodate any number of users.

Robust Failover Capability

Large enterprises often use server farms to assist with the processing workload of distributed networks. eTrust SSO facilitates load balancing and helps with workload distribution in a server farm environment.

eTrust SSO also provides the tools for administrators to back up and restore data held in the eTrust SSO data stores. When you deploy eTrust SSO in a server farm environment, you can configure the system to provide hot-backup.

Smooth Implementation of New Systems

Most companies want to be able to implement new systems and software in their enterprise in a smooth and controlled way to reduce user impact and implementation instability. eTrust SSO is built to permit gradual and controlled implementation of new systems.

For example, you can plug in new authentication or authorization mechanisms behind the scenes without users being aware of any change.

For more information about phased integration, see the Legacy Systems Integration section in this chapter.

Chapter 2

Introduction to eTrust IAM

Organizations typically have disparate systems for user provisioning and access rights management that can result in increased costs, an inability to combat escalating Internet threats, and failure to fully perform auditing requirements to meet regulatory compliance. The Computer Associates eTrust Identity and Access Management (eTrust IAM) suite combines identity and access management, providing comprehensive, integrated solutions to these problems. eTrust IAM is a suite of products that provides flexible and powerful functionality for user provisioning, resource and application security, automated workflow process, and policy enforcement.

The suite is scalable and offers flexibility to use and manage one or more products. Business-critical applications are integrated so that information flows freely between the components without administrators needing to perform time-consuming integration tasks. Additionally, eTrust IAM provides a foundation for additional integration from third-party vendors, thus reducing deployment costs and protecting current investments.

The new management interface is called the Identity and Access Manager (IA Manager). This is a web-based interface that provides a comprehensive management tool for all the products in the suite. Using the IA Manager, you can provision and secure new web services and web-based applications, as well as legacy applications, for your customers, partners, and employees.

This chapter explains the concepts of the eTrust IAM suite.

eTrust IAM Product Suite

Products in the eTrust IAM suite provide solutions to identity or access management requirements on a combination of platforms using a single web-based interface.

The eTrust IAM suite is comprised of the following products:

eTrust Access Control
Provides end-to-end platform and system resource security.

eTrust Admin
Supplies policy-based user and access rights provisioning.

eTrust Single Sign-On
Provides complete enterprise single sign-on to both desktop and web-based applications.

eTrust Web Access Control
Enables secure intranet and extranet management.

Common Components

The eTrust IAM product suite uses a set of common components that create a central architecture with which each product integrates. The common components are installed onto one or more computers depending on the product you are installing and how you configure your computer roles.

The common components installation includes third-party software such as Sun J2SE 1.4.2, Apache Tomcat 4.1.29, and Inxight Star Tree applet that provide underlying services.

Some components in the product suite, such as Admin Server, are required as part of the common components installation. However, the common components installation only installs components that do not already exist on your computers. For example, if you already have the correct version of eTrust Admin installed, the common components installation wizard will detect this and only install items such as agents and legacy interfaces.

After the common components and point products are installed, you can configure the web-based IA Manager to manage your applications.

For more information about common components installation, see the *eTrust SSO Implementation Guide*.

Computer Roles

When you install eTrust IAM you need to designate the roles you want specific computers to assume. A computer assumes one or more eTrust IAM roles based on the components that are installed on that computer.

The following describes the purpose of each computer role:

Web Application Server
Provides several web applications including the IA Manager, IAM Self Service, IAM Self Service Configuration and SPML Web Service.

Provisioning Server
Provides the Admin Server and options, plus eTrust Directory as a router, if on a different computer than a Policy Server or Directory Server.

Directory Server
Stores and maintains the integrity of your identity information configuration.

Workflow Server
Provides business process management services for establishing and tracking business processes.

Policy Server
Controls access to the web, application programs, and workstation resources.

Each computer role requires several components working together. The roles define the groups of components that must be installed on the same computer. It is possible to install multiple roles on individual computers although large installations will realize performance gains by using different computers to share the processing load managed by the various roles.

For more information about computer roles, see the *eTrust SSO Implementation Guide*.

IA Manager

The IA Manager is the web-based management interface that provides a unified administrative view for the eTrust IAM product suite. The IA Manager provides an alternative to the specialized Windows-based graphical user interfaces (GUIs), such as the Policy Manager for eTrust SSO or the Admin Manager for eTrust Admin.

You can use the IA Manager to perform basic administrative tasks related to identity management, role management, provisioning policy management, resource access management, account management, endpoint management, session administration, workflow and enterprise view. For example, you can create and manage global users and their accounts, and set up global users to update their account and personal information.

Available Features

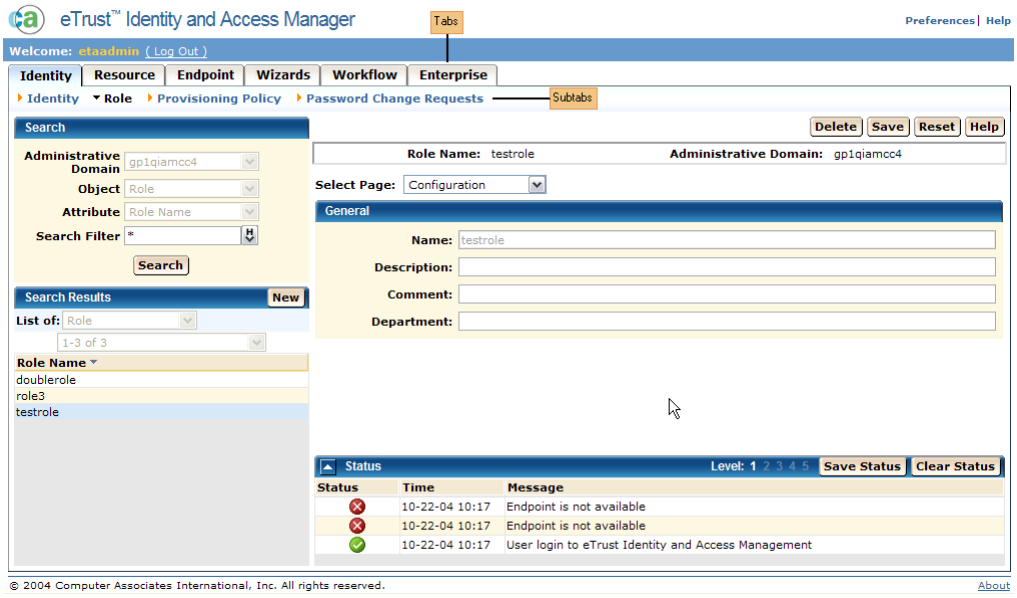
The available features of the IA Manager depend on which products you have installed. The eTrust IAM lets administrators and users perform basic administrative tasks related to:

- Identity-based user management
- Account-based user management
- Application management
- Session administration

For more information about how to use the IA Manager to perform basic tasks, see the "Basic Tasks Using IA Manager" chapter in this guide.

IA Manager Navigation

The IA Manager uses tabs as the main navigation mechanism. The tabs have sub-functions that use subtabs for navigation. The following is an example of the IA Manager showing the Identity tab and Role subtab (the arrow for the active subtab points down):



The features of the interface depend on the eTrust product(s) installed and which tabs and subtabs you select. In this example, there is a Search pane for roles. You select a role name from the Search Results pane, and configure the selected role in the Role - Configuration pane on the right.

Tabs and Subtabs

The IA Manager offers the following tabs and subtabs. Availability depends on which eTrust products are installed and configured.

Identity Tab

The Identity tab is the administrative area for eTrust Admin and manages the tasks related to global users.

The subtabs are:

Identity
Provides management of global users, global user groups, and administrative profiles. You can manage accounts, modify administrative settings, and set profile membership.

Roles
Provides management of roles. Roles are containers used for identity policies, which are executed when a role is assigned to a user. You can set roles membership, synchronize users with roles, and set workflow approvers.

Provisioning Policy
Manages provisioning policy management to explicitly define provisioning of accounts and account group membership on managed endpoints. Provisioning policies are executed when a role that contains the policy is assigned to a global user.

Password Change Requests
Lets the appropriate administrator review and approve requests for password changes received from global users. A request is made by a global user from the Self-Administration GUI and is sent to the IA Manager where the administrator can view and process it.

Resource Tab

The Resource tab handles objects that are protected on individual endpoints. It also lets you authorize and modify access to resources by accounts or account groups on the managed endpoint. This is an administrative area for eTrust Web Access Control, eTrust Access Control, and eTrust SSO.

The subtabs are:

Resource
Manages and defines protected resources and resource groups to be secured by the enforcement points of eTrust Access Control and eTrust Web Access Control. (Resources include files, login applications, surrogates, terminals, registry keys for eTrust Access Control, and URLs and EJBs for eTrust Web Access Control.) The SSO WAC or AC option to eTrust Admin is required.

Application
Manages and defines applications and application groups on desktops and the World Wide Web. It also grants access to accounts and account groups for applications. This is an administrative area for eTrust Web Access Control and eTrust SSO only. The SSO WAC option to eTrust Admin is required.

Access Policy
Defines rules granting or denying access to resources. These policies must be explicitly deployed to specific managed endpoints. This is an administrative area for eTrust Access Control, and only policies related to eTrust Access Control are supported. The ACP option to eTrust Admin is required.

Endpoint Tab

This tab handles objects that are specific to endpoints, with the exception of those objects under the Resource tab.

The subtabs are:

AC Account
Manages and defines accounts and account groups for specific AC managed endpoints. It only administers one managed endpoint at a time, and does not necessarily have a direct link to a user, global user, or role. The AC option to eTrust Admin is required.

SSO/WAC Account
Manages and defines accounts and account groups for specific SSO/WAC managed endpoints. It only administers one managed endpoint at a time, and does not necessarily have a direct link to a user, global user, or role. The SSO WAC option to eTrust Admin is required.

Session Administration
Manages sessions in eTrust SSO. You have the ability to view what sessions an account has established and to terminate individual sessions.

Endpoint
Defines managed endpoints to eTrust Admin and performs explore, correlate, and update functions that connect global users to accounts. This is an administrative area for eTrust Admin, but is required in order to manage other products using eTrust IAM. The AC, SSO WAC, or ACP options to eTrust Admin are required.

Wizard Tab

The only available subtab is Wizards. The wizard subtab offers a number of wizards that take you through multi-step processes with ease, such as creating roles, changing role policies, and changing role users.

Workflow Tab

The Workflow tab is available when you install the Advanced Workflow for Business Process Management (Advanced Workflow) option. It is an administrative area used only with eTrust Admin. Advanced Workflow is used to submit requests by users, and manage those requests by either approving or rejecting them.

The subtabs are:

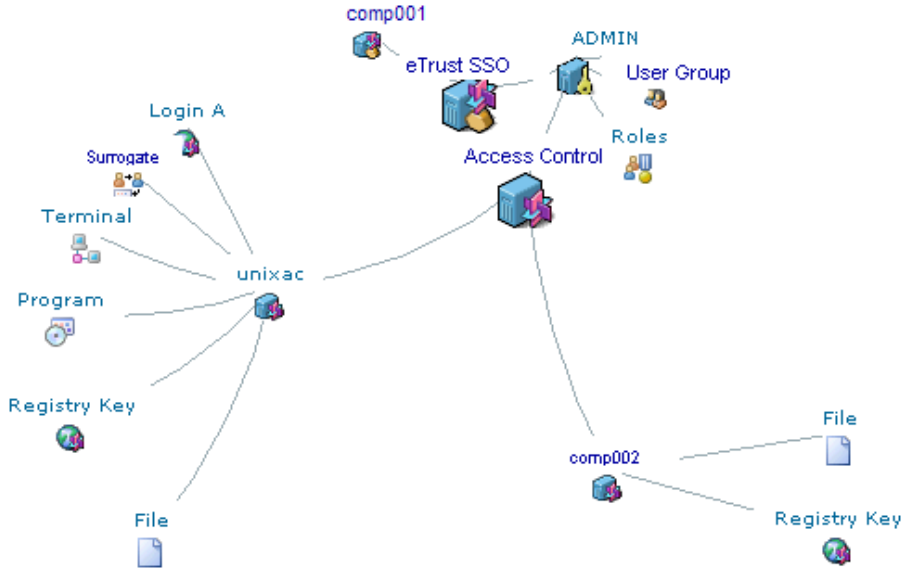
Requests
Permits a user submit a request to the workflow system, but it does not change any data. The Workflow Engine is required for this subtab.

Approvals
Lets workflow approvers view, approve, and reject requests awaiting response in the workflow system. (Workflow approvers are attributes set for specific global users). The Workflow Engine is required for this subtab.

Designer
Provides a launch point for a Java application that is used to design workflow procedures. Special permission is needed to access this subtab. The Workflow Engine is required for this subtab, and the Java application, including the Java JRE, must be installed on the local machine.

Enterprise Tab

The available subtab is Enterprise. This subtab shows a graphical view of the managed endpoints and object types that eTrust Admin can manage using the eTrust IAM. Here is an example of an enterprise view:



The enterprise view shows a complete view of eTrust IAM entities that are deployed in your enterprise. This includes eTrust Admin domains and correlated managed endpoints, and any eTrust Web Access Control or eTrust SSO policy servers, enforcement points, and eTrust Access Control installations. It does not display individual identities, roles, groups, or protected resources. Use this view to drill down into other management areas. A Java plug-in is required for the browser.

Chapter

3

Installing eTrust SSO

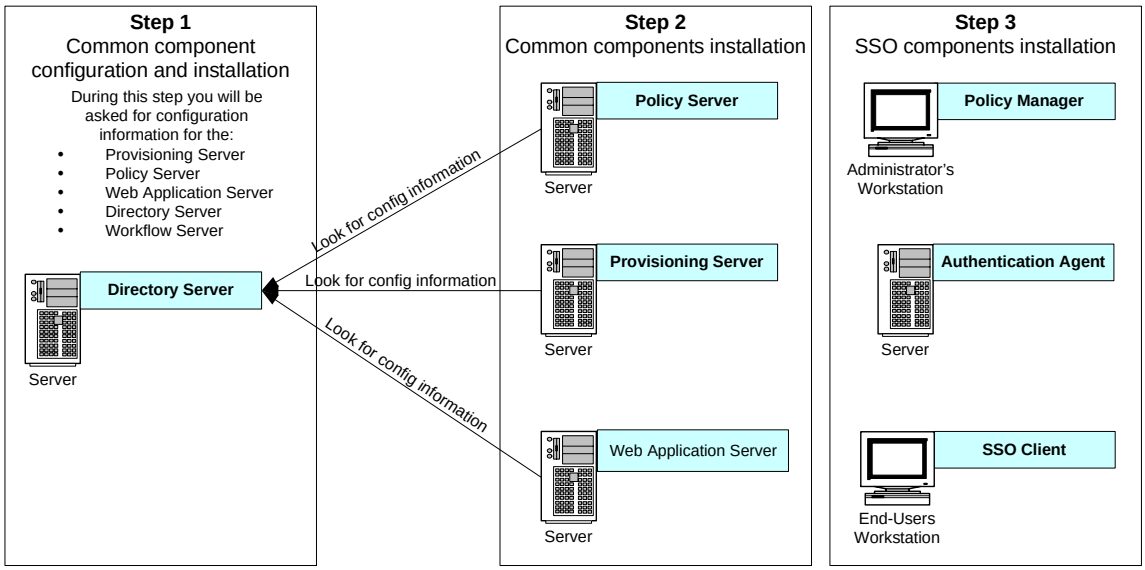
You must first install the IAM common components then the eTrust Single Sign-On (eTrust SSO) components. eTrust SSO is very flexible and can be installed in several different ways. This chapter describes a very simple installation.

You would usually install each component on a separate computer, but for the purposes of a test installation, you can install all components on the same computer.

For more complex installations, including UNIX environments, see the *eTrust SSO Implementation Guide*.

Overview of the Installation

This overview explains the overall process for installing eTrust SSO. This diagram shows the basic components of the eTrust SSO system and the order to install them.



Step 1: From the IAM Common Components installation CD, install the Directory Server. This computer stores the common components configuration information which is accessed by the other computers included in the installation.

Step 2: From the IAM common components installation CD, install the:

- Policy Server
- Provisioning Server
- Web Application Server

The IAM installation wizard will connect to the Directory Server to retrieve the configuration information for these common components.

Step 3: From the eTrust SSO installation CD, install the:

- Policy Manager
- Authentication Agent
- SSO Client

For a full eTrust SSO installation with advanced functionality you would also need to install the eTrust SSO agents. For more information, see the *eTrust SSO Implementation Guide*.

Before You Begin the eTrust SSO Installation

This section explains what you need to install the eTrust SSO components.

Set Administrator Access Rights

You must have local administrator privileges to install eTrust SSO. In a Windows environment, you can do this from the Start menu, Control Panel, User Accounts.

To install the Policy Server on a UNIX environment you must have root access and privileges.

Install an Authentication Server

If you are *not* using the native authentication method that comes with eTrust SSO, you must set up the third party authentication server and install the appropriate eTrust SSO authentication agent. You may already have this in operation.

For more details about how to install an authentication server and authentication agent, see the *eTrust SSO Implementation Guide*.

Install the IAM Common Components

This section outlines the three steps to installing eTrust SSO r8. The first two steps cover how to configure and install the Common Components. The final step covers how to install the components that are specific to eTrust SSO r8.

Step 1: To Install the Directory Server and Configuration Information

To complete the first part of the eTrust SSO installation, follow these steps:

1. Insert the first eTrust IAM Common Components installation CD into your CD drive.

   The eTrust IAM Product Explorer appears.

   Note: If the Product Explorer does not automatically appear, use Windows Explorer to access the CD drive and double-click the setup.exe file.

2. Click Install.

   The installation wizard starts loading and appears after a short delay.

3. Click Next.

   The Starting the Installation panel appears, asking if you have already started your installation of eTrust IAM Common Components elsewhere.

4. Select No and click Next.

5. Follow the Installation Wizard instructions and enter the configuration information for each of the common components.

   For more detailed instructions on how to install the common components, see the "Implementing the Common Components" chapter in the *eTrust SSO Implementation Guide*.

Step 2: To install the Policy, Provisioning and Web Application Servers

To complete the second part of the eTrust SSO installation, follow these steps:

1. Insert the first eTrust IAM Common Components installation CD into your CD drive.

   The eTrust IAM Product Explorer appears.

   Note: If the Product Explorer does not automatically appear, use Windows Explorer to access the CD drive and double-click the setup.exe file.

2. Click Install.

   The installation wizard starts loading and appears after a short delay.

3. Click Next.

   The Starting the Installation panel appears, asking if you have already started your installation of eTrust IAM Common Components elsewhere.

4. Select *Yes*, enter the name of the machine where you started your eTrust IAM installation and your IAMConfig password, and click Next.

   If the installer can connect to the machine and load your configuration successfully, the Configuration Information Progress panel will appear..

5. Follow the Installation Wizard instructions to complete common components installation.

Step 3: To Install the SSO-Specific Components

To complete the third part of the eTrust SSO installation you need to install the following components in the following order:

1. Policy Manager
2. Authentication Agent(s)
3. SSO Client

Install the Policy Manager

To install the Policy Manager, which is the GUI interface that lets you administer the eTrust SSO system and the Policy Server, follow these steps:

1. Open the eTrust Single Sign-On r8 Product Explorer window.

   This window should appear automatically when you insert the eTrust SSO disk. If not, open Windows Explorer, navigate to the CD-ROM directory, and double-click the PEi386.exe file.

2. Select Policy Manager for Windows.

   The Install button becomes active.

3. Click Install.
4. Follow the prompts to complete the installation.

Install the Authentication Agent

To install an Authentication Agent, follow these steps:

1. Open the eTrust **Single Sign-On r8 Product Explorer** window.

   This window should appear automatically when you insert the eTrust SSO disk. If not, open Windows Explorer, navigate to the CD-ROM directory, and double-click the PEi386.exe file.

2. Expand the eTrust Single Sign-on Authentication Agents folder .

3. Select the authentication agent that matches the authentication method you want to use.

   The **Install** button becomes active.

   Note: For UNIX authentication agents, this button is not active so you should click System Requirements which contains the command for running the installation on a UNIX platform.

4. Click **Install**.

   The Welcome dialog appears.

5. Follow the prompts to complete the installation.

Install the SSO Client

This procedure explains how to install the SSO Client, which is the component installed on the end-user's workstation.

1. Open the eTrust Single Sign-On r8 Product Explorer window.

   This window should appear automatically when you insert the eTrust SSO disk. If not, open Windows Explorer, navigate to the CD-ROM directory, and double-click the PEi386.exe file.

2. Select Single Sign-On Client 8.0

   The Install button becomes active.

3. Click Install.

   The Welcome dialog appears.

4. Follow the prompts to complete the installation.

Chapter 4

Concepts Behind eTrust SSO

This chapter gives you an overview of eTrust Single Sign-On (eTrust SSO) concepts including:

- End users
- Primary authentication
- Scripts
- Applications (accessed through eTrust SSO)
- Session profiles
- Resources
- Policies

End Users

End users are individuals (usually employees of your company) who are using eTrust SSO to access their applications. The eTrust SSO system must identify each individual as unique. Each user has specific information recorded against them including:

- How they should be authenticated
- What applications they need access to
- What groups they belong to
- Application logon credentials

End-User Experience

From an end user's perspective, eTrust SSO is designed to help them log on to multiple software applications without having to identify themselves every time. However, end users must identify themselves when they first log on to eTrust SSO. This is called primary authentication. For more information, see the Primary Authentication section in this chapter.

Primary authentication usually uses a combination of a username and either a password, a smart card, an ID card or a biometric device. The term *biometric* refers to technology that uses biology such as a fingerprint or iris scanner.

Once an end user successfully authenticates and logs on to eTrust SSO, they see a list of applications that they can access. Users can select these applications either from the Start menu in Windows, or from an eTrust SSO application list. These applications typically require the user to provide identification. These applications can be from any company.

Ways to Manage End Users

When implementing eTrust SSO in your organization, the implementation team typically uploads a large number of users at once. This is not usually a regular administration task.

After eTrust SSO has been implemented in your organization you usually only need to add or remove users individually as staff are hired or leave the company. This is done through the Policy Manager or using the IA Manager. This is a regular administration task.

Groups of End Users

Assigning users to groups and setting the access permissions by group eliminates the need to create and remove access rules for each user.

For example, you can create a user group for the Payroll department and grant only members of that group access to sensitive payroll information. As employees leave or join the Payroll department, you can add or remove them from the group to automatically grant or deny them access to the correct resources.

Primary Authentication

Primary authentication is the method by which users identify themselves to the eTrust SSO system. For primary authentication to occur, a user must enter unique credentials (such as a user name and password) and the system must verify that those credentials correspond to a valid user in the system.

The eTrust SSO system is designed to use several different systems to verify those credentials, including third-party authentication methods.

Customers and third-party vendors can also integrate additional authentication methods using the eTrust SSO API.

Authentication Methods Developed and Supported by CA

eTrust SSO comes with two native authentication methods that you can use immediately out-of-the-box. The eTrust SSO native authentication methods are:

Authentication Software	Authentication Method
eTrust SSO	Username and Password
LDAP	Username and Password

Authentication Methods Supported by CA

eTrust SSO also comes with the ability to integrate quickly and easily with several third-party authentication vendors, using authentication agents. For more information about authentication agents, see the Authenticating Users section in the "Common eTrust SSO Processes" chapter in this guide. You may already have this software implemented within your company. These are:

Authentication Software	Authentication Method
Certificate	Digital certificates
Entrust	Digital certificates
Novell	Username and password
Windows	Username and password
RSA SecurID	Secure ID card + PIN
Safeword	Token

Applications in eTrust SSO

When we talk about applications in eTrust SSO or *secure applications*, we are referring to any application that has been added to eTrust SSO and is ready to allocate to users. These can be Windows, mainframe, or web-based applications that you want your users to have access to after they have authenticated.

The eTrust SSO applications are located on either the user's computer or on a computer connected to the network.

Application Lists

Every user has an application list. This list contains all the applications that the user is authorized to use that are started by eTrust SSO. If the user is a member of a group, all the applications that the group can access appear on the user's eTrust SSO application list when they log on to eTrust SSO.

In Windows 98SE/NT/2000/XP/2003, the application list can be displayed in:

- The Start menu
- An eTrust SSO toolbar
- An eTrust SSO window (launched from an icon)

The eTrust SSO administrator or implementation team can also customize how users access their application lists.

For an application to appear in a user's eTrust SSO application list, the administrator must write an eTrust SSO logon script and must assign it to the user (or user group). For more information about scripts, see the Scripts section in this chapter.

Scripts

In the context of eTrust SSO the term *scripts* refers to Tcl programs that perform tasks for the user. Scripts can be used for a wide variety of tasks. A *logon* script, for example, is written to automatically log a user in to an application (automatically insert the correct user's name and password in the relevant fields of the logon screens).

eTrust SSO logon scripts are written in a special extended version of the Tcl scripting language. Prior experience with Tcl is not required to be able to write these, but some programming experience is an advantage.

The security or system administrator in charge of eTrust SSO is responsible for preparing the logon scripts. These scripts are written during implementation and typically do not affect the day-to-day administration of eTrust SSO.

Scripts to Launch Applications

The most obvious function of a script in the single sign-on environment is to launch applications and insert the user's logon credentials so that the user does not have to remember passwords or enter any data.

You must write a logon script for each application you add to the eTrust SSO system. The logon scripts must conform exactly to the specific logon requirements of each application in your environment.

Other Functions for Scripts

Scripts can do more than simply launch applications and enter user credentials.

Scripts can also be used to:

- Close applications
- Change and synchronize passwords
- Automate repetitive tasks
- Automate long navigation trails

Example

Ken, a busy doctor, must access an application that permits him to enter patient data. Each time Ken logs in to this application, he must navigate through four windows and enter default data before reaching the screen he actually needs. A Tcl script can be written to automate this process and thereby assist productivity.

Session Profiles

You can define a session as the period of time a user is logged in to the SSO Client.

By default, eTrust SSO lets users have multiple concurrent sessions. Using eTrust SSO, you can set automatic session management rules to limit the number of concurrent sessions a user has open. You can also work with sessions manually using the Session Administrator.

You can use eTrust SSO to:

- Limit the maximum number of sessions a user can have open simultaneously
- Define what happens when a user attempts to exceed this number of sessions
- Manually terminate any sessions

To protect sensitive information, you can use the Policy Manager to set the following:

- An idle time-out for logging the user out of the eTrust SSO session as well as logging out the underlying Windows user
- An idle time-out for logging the user out of the session

What is a Session Profile?

Using the eTrust SSO management GUI, the Policy Manager, you can set **profiles** that define how user sessions work. Profiles are groups of settings applied to users or groups of users.

Profiles include the following settings:

- How many sessions the user can have open simultaneously
- What happens when the user reaches their maximum number of sessions
- What happens when the system is not used for a length of time

Resources

In the context of eTrust SSO the term *resource* refers to software, hardware, and settings managed by the Policy Manager. Users and authentication agents are not included in the *resources* category.

Different Types of Resources

The Policy Manager can manage different types of resources.

Resources	Explanation
Data Stores	**User Data Stores:** Computers that store user details **User Attributes:** Categories of extra information that can be recorded for each user, such as the country they work in.
Configuration Resources	**Terminal:** All computers that run the Policy Manager. **Authentication Host:** Computers that run the authentication agent. **Authentication Method:** The method used to authenticate users. **Password policies:** The rules that apply to the strength of the password. **Response Table:** Table that defines additional information returned with an authorization request. **Token Directory:** An LDAP directory in which the Policy Server stores the users' session information.
Web/Generic Resources	**URLs:** Web addresses of secure web pages that users can log on to using eTrust SSO. **EJBs:** Enterprise Java Beans (EJB) can not be used with eTrust SSO, only eTrust Web Access Control.
Application Resources	Applications that users can log on to using eTrust SSO.
Session Resources	Session Profiles that can be applied to users. For more information, see the Session Profiles section in this chapter.

Policies

A policy is a set of rules that defines behavior. In eTrust SSO, you can define a policy for passwords.

This password policy controls the password that users enter to log on to the eTrust SSO system.

You can set the following password rules:

- Minimum and maximum length
- Alphanumeric/upper and lower case requirements
- Upper and lower case combination
- Password change interval
- Password history (how many password changes required before reuse is allowed)
- Grace logons

For more information about setting up password policies, see the Password Policies section of the "Basic Tasks Using the Policy Manager" chapter in this guide.

Chapter 5

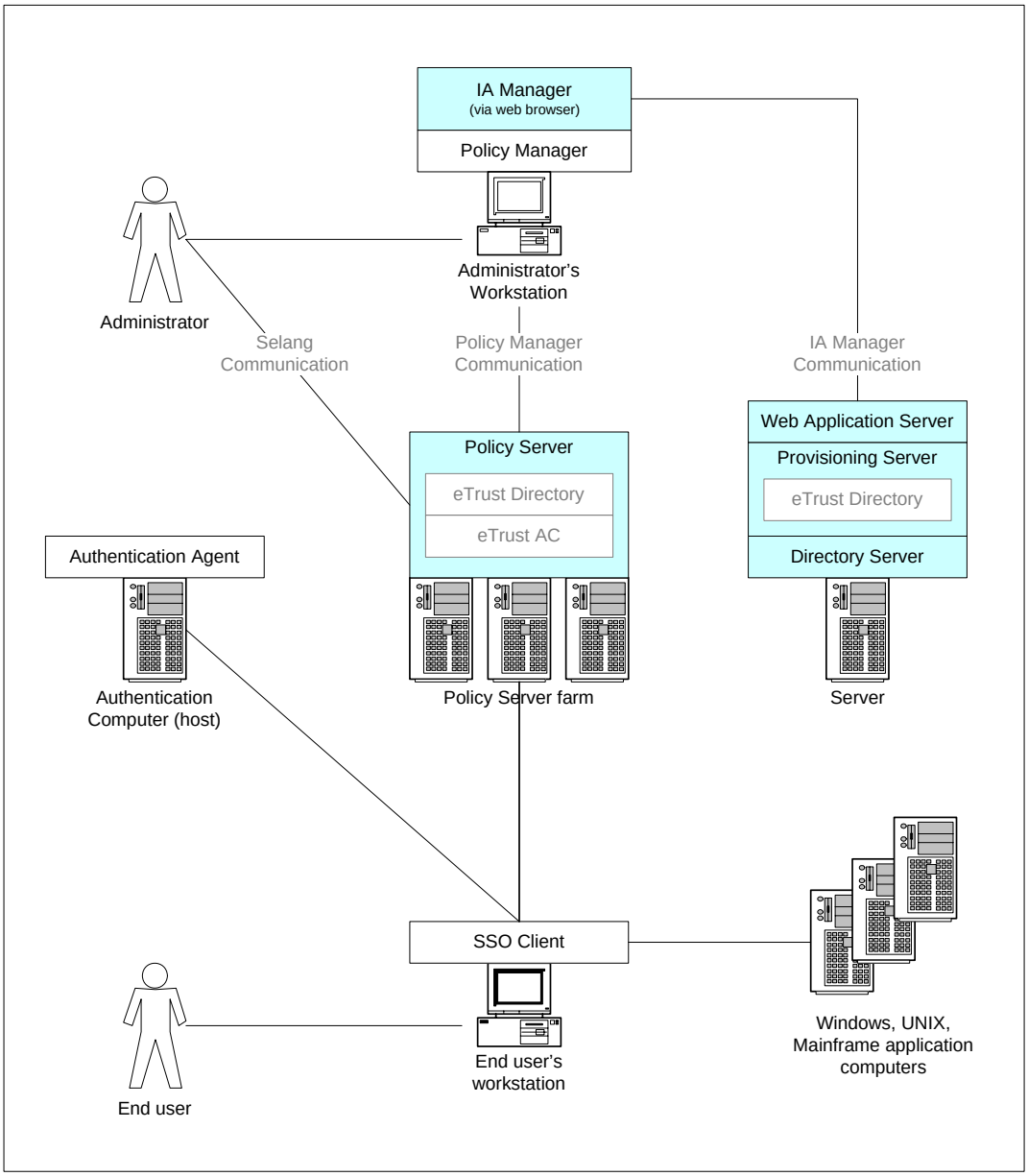
Tour of eTrust SSO Components

This chapter introduces the main architectural components of the eTrust Single Sign-On (eTrust SSO). This chapter will give you a simple look at the following:

- Architectural Overview
- SSO Client
- Policy Manager
- IA Manager
- IAM Common Components
  - Policy Server
  - Provisioning Server
  - Directory Server
  - Web Application Server
- Data Stores
  - eTrust Access Control
  - eTrust Directory (LDAP)

Architectural Overview

This architectural overview shows how each of the eTrust SSO components fit into the product architecture. The rectangles in the diagram represent the software components. The shaded rectangles represent the IAM Common Components.



SSO Client

The SSO Client runs on every workstation that uses eTrust SSO desktop services. You can run the SSO Client software on the user workstation, or it can be run on the workstation from a network file server.

The SSO Client is a small application that lets users in your enterprise work with eTrust SSO. This is the only eTrust SSO component that the end user sees and works with.

The SSO Client software:

- Communicates with primary authentication agents to verify the user's primary authentication, and then stores an authenticated ticket for that session
- Displays a list of the applications that the user is authorized to use
- Sends the authenticated ticket to the Policy Server to gain access to applications
- Executes a logon script and logs the user in to the selected application
- Sends the results of the logon attempt to the Policy Server (when instructed by the logon script)

Policy Manager

The Policy Manager is a Windows GUI for managing the Policy Server and the data stores. It is usually installed on an administrator's workstation with TCP/IP communication to the Policy Server. You can use the Policy Manager to communicate with both UNIX and Windows Policy Server computers.

As an administrator, you must perform a number of tasks regularly using the Policy Manager. These include:

- Configuring and connecting all the eTrust SSO components
- Adding and grouping users
- Allocating applications and web resources to users and user groups
- Establishing access rights

The Policy Manager also controls other eTrust products including eTrust Access Control and eTrust Web Access Control.

IA Manager

IA Manager is the web-based management interface that provides a unified administrative view for the product suite. It as an alternative to the existing management interfaces that are provided with each product in the suite, which are the Policy Manager for eTrust SSO, eTrust Web AC, and eTrust AC, and the Admin Manager for eTrust Admin. The IA Manager does not fully replace the functionality of your product's management interface with this release.

You can use IA Manager to perform basic administrative tasks related to identity management, role management, provisioning policy management, resource access management, account management, session administration, and self-administration. For example, you can create and manage users and their accounts, and set up users to update their account and personal information. Available features depend on which products you have installed.

IAM Common Components

Every product in the IAM suite, which includes eTrust SSO, uses a set of common components that forms the central architecture with which each product can integrate. The common components include the following:

- Policy Server
- Provisioning Server
- Web Application Server
- Directory Server

Additionally, the common components installation includes third-party software, such as Java JRE 1.4.2 and Apache Tomcat 4.1.29, that provide underlying services.

Policy Server

The Policy Server is one of the IAM Common Components. The Policy Server is the heart of eTrust SSO. It resides on a central UNIX or Windows server, and completely manages eTrust SSO. You can control the Policy Server from the command line or by using the Policy Manager.

The Policy Server performs the following functions:

- Provides authentication
- Manages data in the eTrust Access Control data store
- Manages data in the eTrust Directory data store
- Builds the list of applications that a user is permitted to access and sends it to the SSO Client
- Retrieves the logon scripts and the user-specific logon data for each application
- Determines which web resources users can access

Provisioning Server

The Provisioning Server is one of the IAM Common Components. It forms a link between the Web Application Server and the Policy Server. The Provisioning Server is used extensively by eTrust Admin, which is one of the other products in the IAM suite.

Web Application Server

The Web Application Server is one of the IAM Common Components. The Web Application Server hosts the IA Manager infrastructure. The IA Manager is a GUI that lets administrators manage eTrust SSO, and other products in the IAM suite if they have them installed, from a central web-based interface using their web browser.

Directory Server

The Directory Server is one of the IAM Common Components. The main purpose of this server is to store configuration information for the other IAM Common Components.

The Directory Server has eTrust Directory installed on it. eTrust Directory is also installed on the Policy Server and the Provisioning Server, but each installation contains different information.

Data Stores

The *data stores* are the software that stores the data associated with eTrust SSO. eTrust SSO comes with two data stores, eTrust Access Control and eTrust Directory, that each give slightly different benefits. You can also integrate third-party LDAP data stores.

eTrust Directory

eTrust SSO comes with eTrust Directory. eTrust Directory is designed to efficiently manage thousands of users, which significantly enhances the performance and scalability of eTrust SSO. The eTrust Directory data store is perfect for large enterprise installations.

eTrust Directory is the default data store for:

- Users
- User groups
- Logon information

You can populate this database with user and group information from existing databases in your organization after product installation. You can conveniently import information by running a utility, or by using the command line interface.

Other eTrust products also use eTrust Directory. Once you load information in the data store, these products can all read and update the shared database for their separate and common purposes.

eTrust Access Control

eTrust SSO comes with eTrust Access Control. eTrust Access Control is the required data store for all information about:

- Administrators
- Resources
- Applications
- Access control rules

You can also use eTrust Access Control to store information about users, user groups, and logon information, but we recommend that you use eTrust Directory or another LDAP directory to store this information.

You can populate this database with resource and application information from existing databases in your organization, during or after product installation. You can conveniently import information by running a utility, or by using the command line interface.

Other eTrust products also use the eTrust Access Control database. Once you load information in the database, these products can all read and update the shared database for their separate and common purposes.

Chapter

6

Common eTrust SSO Processes

This chapter introduces the following common processes performed by eTrust Single Sign-On (eTrust SSO):

- Authenticating users
- Launching applications
- Synchronizing passwords

Each description includes a diagram that shows how the component fits into the architecture of eTrust SSO. The gray boxes in the diagrams represent the software components.

Authenticating Users

Primary authentication is how users identify themselves to the system.

After the user has entered their credentials, the SSO Client sends those credentials to the authentication agent. The authentication agent acts as a *go-between*, it passes those credentials to the relevant authentication software and receives confirmation back. The authentication agent then produces a *ticket* and sends it back to the SSO Client.

What Is the Authentication Agent?

An agent is a program that performs some information gathering or processing task, and typically interfaces with another software component. Many of the eTrust SSO processes require an agent.

Every authentication method requires a corresponding authentication agent to relay information between the eTrust SSO system and the authentication software.

eTrust SSO has two ready-made authentication methods: native SSO authentication and LDAP authentication. If you use native SSO authentication, you do not need to install a separate Authentication Agent, because the Policy Server can performs the necessary authentication functions. eTrust SSO is also compatible with a number of third-party authentication methods, so you can select the authentication method that best meets your company's needs. For more information about authentication methods, see the Primary Authentication section in the "Concepts Behind eTrust SSO" chapter in this guide

Where to Install the Authentication Agent

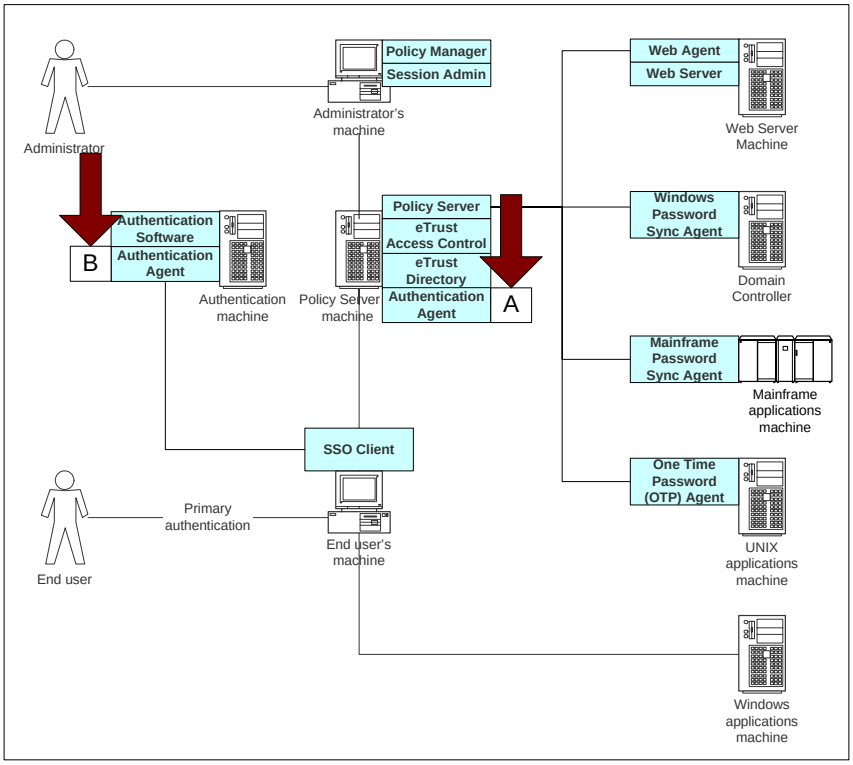
The location of the authentication agent depends on the method of authentication (authentication software) and the level of security you require.

The server where the authentication agent resides is called the *authentication host*. The corresponding authentication software is usually also located on the authentication host, but can be located on another computer for security reasons.

You can configure your system in different ways and install your authentication agent in different places. The following table and diagram show where you might *typically* install the authentication agent for the different authentication methods. It is rare that you need the authentication agent in more than one location.

Authentication Method	Authentication Agent Location	Diagram Reference
SSO	Policy Server	A
Novell	Domain member	B
Windows	Domain member	B
LDAP	Separate authentication computer	B
Entrust	Separate authentication computer	B
Certificate	Separate authentication computer	B
RSA SecurID	Separate authentication computer	B
Safeword	Separate authentication computer	B

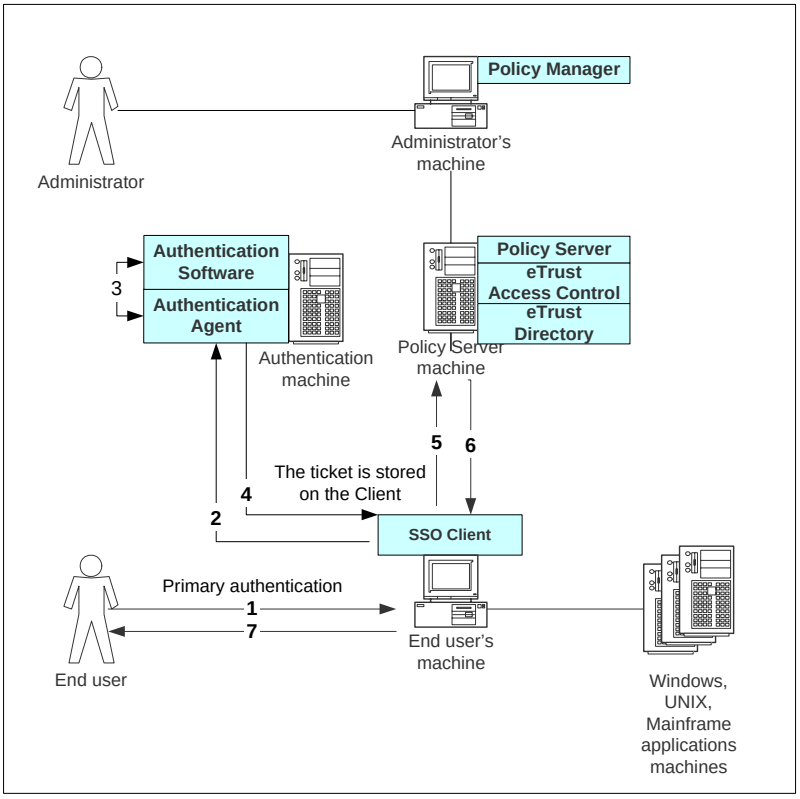
The following diagram shows the location of the authentication agents in relation to the authentication methods in the previous table.



The boxes marked *A* and *B* in this diagram correspond to the authentication agent location specified in the previous table.

The Authentication Process

The following diagram shows how the authentication process works using a third-party authentication method as an example (option B in the previous section).



1. The user enters their primary authentication credentials in to the SSO Client.
2. The SSO Client sends the credentials to the authentication agent for verification.
3. The authentication agent connects to the authentication software for verification and produces a ticket if the credentials are correct.
4. When approved, the authentication agent sends the ticket back to the SSO Client. This ticket is time stamped and expires after a set period, or persists until the eTrust SSO session is terminated, depending on the expiration settings on the Policy Server.
5. The SSO Client sends the ticket to the Policy Server to check which applications are allocated to that user.
6. The Policy Server sends a list of the applications available to the user to the SSO Client.
7. The user is presented with a list of all the applications that have been allocated to them within the eTrust SSO framework.

Launching Applications

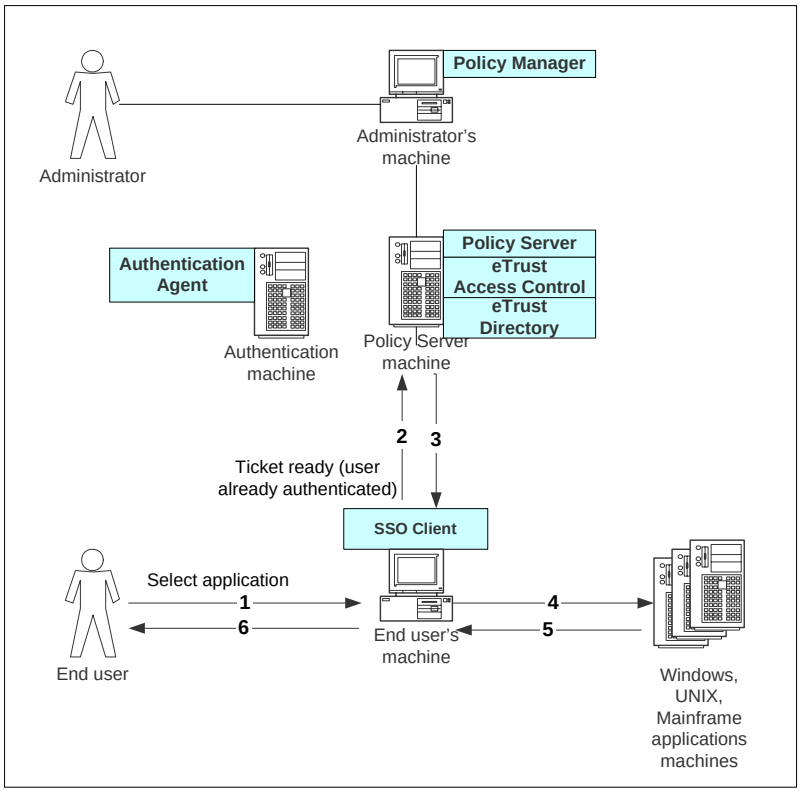
Once end users have been authenticated, they can select and launch any application that has been added to their eTrust SSO application list.

Each application must have a Tcl script to perform the logon functionality and any other tasks required to help the user. For more information about Tcl, see the Scripts section in the "Concepts Behind eTrust SSO" chapter.

You can configure eTrust SSO to let you launch applications from different platforms including Windows, the Web, mainframe, and UNIX. This section shows an example of how to launch a Windows application and how to access a Web resource.

Launching Windows Applications

You can store and configure Windows applications to work in different ways across different environments. Here is an example of how to launch a Windows email application from eTrust SSO.



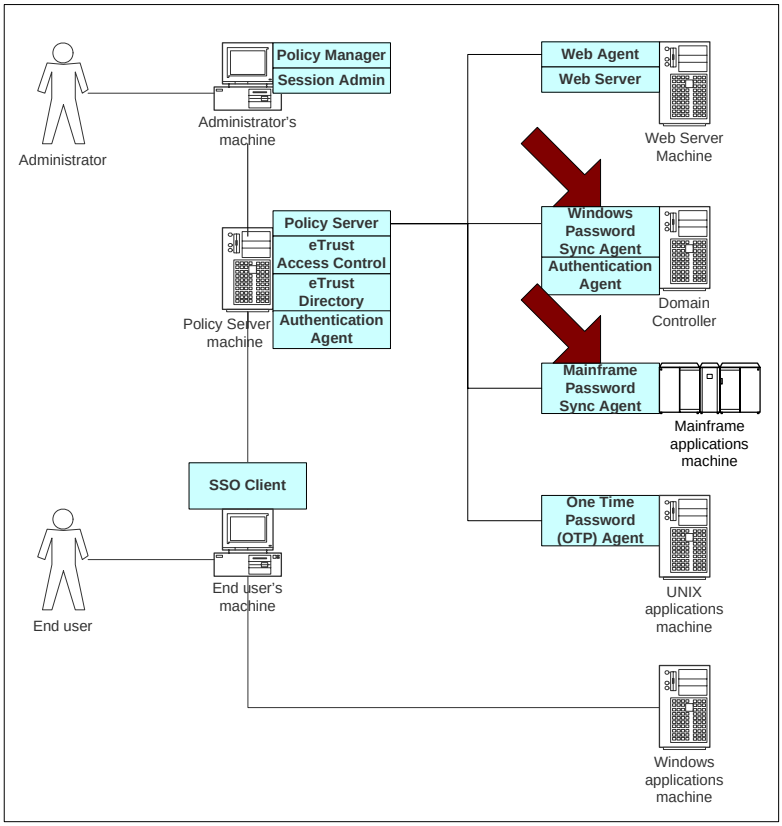
Before this process begins, the user was successfully authenticated.

1. The user launches the email application from their eTrust SSO list.
2. A request to launch the application is sent to the Policy Server together with that user's SSO ticket. For more information about SSO tickets, see The Authentication Process section in this chapter.
3. The Policy Server checks whether the user is permitted to access that application. If they are, the Policy Server sends back a script to launch the application.

   In this example, the application is installed on the user's computer and the script launches the application and enters the relevant username and password.
4. The email application checks for emails on the Windows server.
5. The emails download on to the user's computer.
6. The user is now logged in and able to access their email.

Synchronizing Passwords

It is important that the eTrust SSO system keeps passwords up-to-date on all computers. Sometimes a user's password changes on a system and that change must be updated on the Policy Server. A user's password may change when a user changes their domain logon or when a password automatically changes.



To record the new password on the Policy Server, you can install a password synchronization agent on the domain controller to constantly listen for any password changes. When the password synchronization agent receives notification of a password change, it sends the new password back to the Policy Server to be stored and used in the future.

There is also a mainframe password synchronization agent that works in a very similar way to the Windows domain password synchronization agent. The difference is that the mainframe password synchronization agent sends changed passwords to eTrust Access Control, which then records the change on the Policy Server.

Chapter 7

Basic Tasks Using IA Manager

This chapter introduces basic tasks you can perform using the IA Manager. For more information about how to use the IA Manager, see the IA Manager Online Help.

Manage Accounts

The following topics give procedures for performing basic tasks for managing user accounts and user account groups.

Create an SSO WAC Account

The user account object contains information such as the user's full name, the times the user is allowed to log in, and the authentication methods that the user is allowed to use. The user account object also contains a list of account groups to which the user account belongs.

Note: eTrust SSO and eTrust Web Access Control (eTrust Web AC) accounts are defined on a specific eTrust SSO or eTrust Web AC managed endpoint. You can only administer one managed endpoint at a time.

To create an eTrust SSO or eTrust Web Access Control account, follow these steps:

1. Select the Endpoint tab from the navigation bar to display the Endpoint Search Pane.
2. Click the SSO WAC Account sub-tab.

   The SSO WAC Account Search pane appears.
3. From the attribute fields in the Search pane, select Account from the Object field, and select the managed endpoint, user data store, and container (if you have any in your LDAP user data store) where you want to create the new account.
4. Click New from the SSO WAC Account Search pane.

   The Create New Account pane appears.
5. Complete the fields for the new account and click Save.

   The account is created.

Delete an SSO WAC Account

You can delete an eTrust SSO or eTrust Web AC account for an employee who has left the company.

To delete an eTrust SSO or eTrust Web AC account, follow these steps:

1. Select the Endpoint tab from the navigation bar to display the Endpoint Search Pane.
2. Click the SSO WAC Account sub-tab.

   The SSO WAC Account Search pane appears.
3. Select Account from the Object field and any other related attributes from the Search pane, and then click Search.

   The search is processed and the results are displayed in the Search Results list.
4. Choose the account you want to delete from the Search Results list.
5. On the right pane the selected user details will be displayed with the Delete button.
6. Click Delete.

   The account is deleted.

Add an Account Group to an SSO WAC Account

You can assign account groups to an eTrust SSO or eTrust Web AC account, so you can manage the specified account along with other accounts in the account group.

To add an account group to an eTrust SSO or eTrust Web AC account, follow these steps:

1. Select the Endpoint tab from the navigation bar to display the Endpoint Search Pane.
2. Click the SSO WAC Account link.

   The SSO WAC Account Search pane appears.
3. Select Account from the Object field and any other attributes you want from the Search pane, and then click Search.

   The search is processed and the results are displayed in the Search Results list.
4. Choose the account from the Search Results list.

   The Configuration Pane appears.
5. Select Group Membership from the Select Page drop-down list.

   The Group Membership pane appears.
6. Select the group's container from the account group search, and then click Search.

   The results of the search appear in the Available Account Groups list.
7. Select the account group that you want to add from the Available Account Groups list and click Add  .

   The account group is moved to the Included Account Groups list. The account is a member of all the account groups listed in the Included Account Groups list.
8. Click Save.

   The account group is added to the account.

Delete an Account Group

When you no longer use an account group, you can delete that account group without deleting the accounts that are members of the account group.

To delete an account group, follow these steps:

1. Select the Endpoint tab from the navigation bar to display the Endpoint Search Pane.
2. Click the AC Account link.

   The AC Account Search pane appears.
3. Select Group from the Object field and click Search.

   The search is processed and the results are displayed in the Search Results list.
4. Choose the account group you want from the Search Results list.

   The Configuration Pane appears.
5. Click Delete.

   The account group is deleted.

Manage Applications

The following topics give procedures about performing basic tasks for managing applications.

Assign Access Permission to an Account for an Application

You can grant access permission to an account or account group for a specific application. The access permission can allow or deny the account or group to execute the application.

To assign access permission to an account or account group for an application, follow these steps:

1. Select the Resource tab from the navigation bar to display the Resource Search Pane.
2. Click the Application link.

   The Application Search pane appears.
3. Select the type of application you want and any other attributes from the object drop-down list and click Search.

   The search is processed and the results are displayed in the Search Results list.
4. Choose the application from the Search Results list.

   The Configuration Pane appears.
5. Select Authorize Access from the Select Page drop-down list.

   The Authorize Access pane appears.
6. Select the attributes you want, such as User Data Store, Container (if you have any containers in your LDAP user data), and Account or Group object. Click Search from the account search.

   The results of the search appear in the Available Accounts list.
7. Select the account or group you want from the list and click Add  .

   The account or group is moved to the Included Accounts list.
8. Select the account or group from the Included Accounts list, then select whether to allow or deny access permission.
9. (Optional) When you want to specify compound rules, click View/Modify. The View/Modify Conditions window appears. Make your changes, and then click OK.

   You return to the Authorize Access pane.
10. Click Save.

    The access permission is saved to the account or group for the specified application.

Add a Script to an Application

You can add a script to be used with an application. The script allows the user to enter third-party or affiliated web sites without having to re-enter login information.

To add a script to an application, follow these steps:

1. Select the Resource tab from the navigation bar to display the Resource Search Pane.
2. Click the Application link.

   The Application Search pane appears.
3. Select a managed endpoint, and either Web Application or Desktop Application from the object list. Click Search.

   The search is processed and the results are displayed in the Search Results list.
4. Choose the application from the Search Results list.

   The Configuration Pane appears.
5. Complete the Script File field and click Save.

   The script file is saved to the application.

Specify an Account's Login and Password for an Application

You can specify the login information for an account to log into a specific application. The Policy Server sends the application login information to the Web Agent after the Policy Server gets the account's request to log into an application.

To specify an account's login and password for an application, follow these steps:

1. Select the Endpoint tab from the navigation bar to display the Endpoint Search Pane.
2. Click the SSO WAC Account link.

   The SSO WAC Account Search pane appears.
3. Select Account from the Object field and any other attributes you want from the Search pane, and then click Search.

   The search is processed and the results are displayed in the Search Results list.
4. Choose the account from the Search Results list.

   The Configuration Pane appears.
5. Select Application Password from the Select Page drop-down list.

   The Application Password pane appears.
6. Complete the Login, Password, and Confirm fields for the specific application and click Save.

   The account's login and password for the application are saved.

Chapter 8

Basic Tasks Using Policy Manager

The objective of this chapter is to help you get familiar with both the Policy Manager administration tool and the IA Manager administration tool. This chapter explains a bit about Policy Manager navigation and IA Manager navigation.

This chapter also takes you through your first tasks as an administrator of eTrust SSO using the Policy Manager and explains how to:

- Add and delete a user
- Add and delete a user group
- Add and delete an SSO Administrator
- Create and apply a session profile (and assign it to a user)
- Create and apply a password policy (and assign it to a user)

The Policy Manager is a windows based interface that provides a administrative view for the Policy Sever. The Policy Manager is ideal for advanced configuration.

You can use the IA Manager for many of the same tasks you can perform in the Policy Manager. For more information see the "Basic Tasks Using the IA Manager" chapter in this guide.

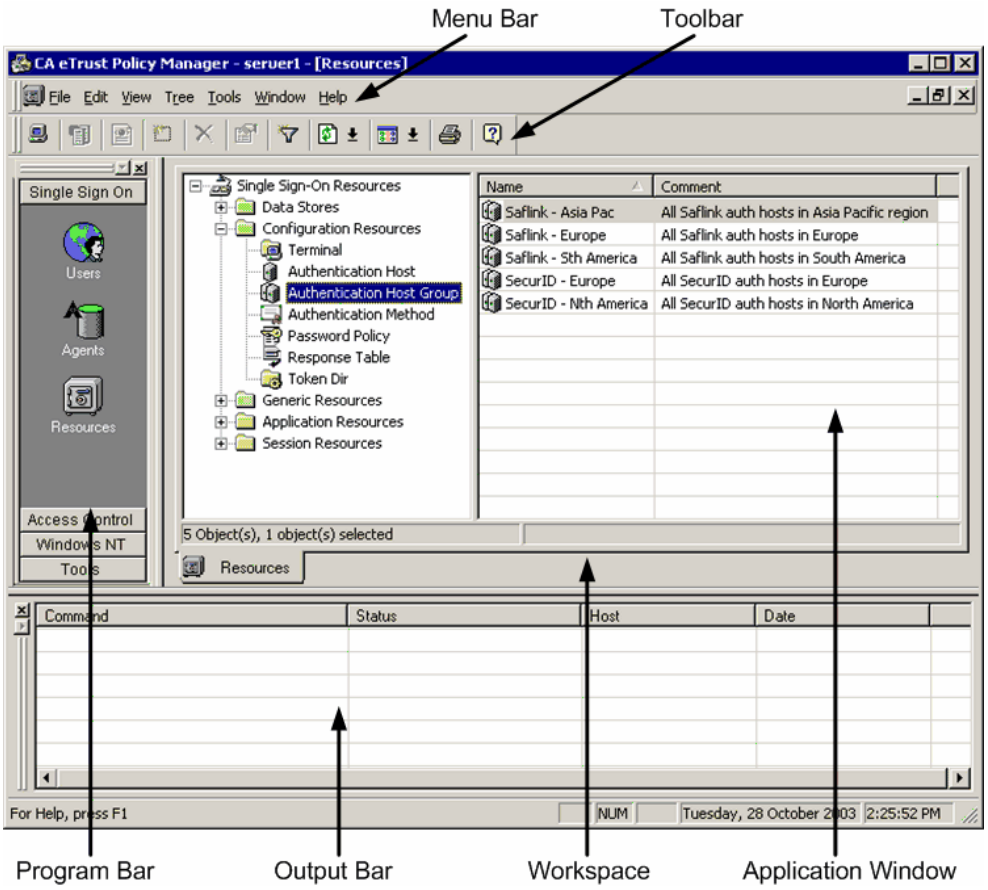
You can also use the Policy Manager to manage data in the following other eTrust IAM point products, by changing the operation mode:

- eTrust Access Control
- eTrust Web Access Control

Policy Manager Navigation

All data management begins at the main window of the Policy Manager. This window appears after you successfully complete the Login dialog.

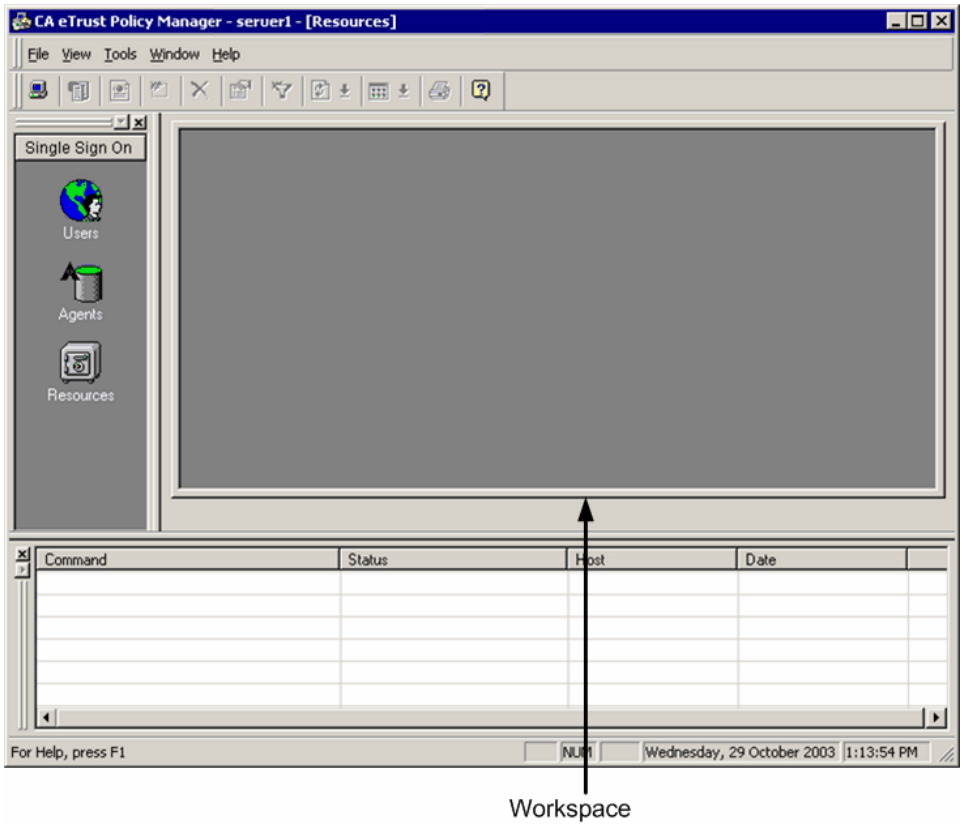
This is a sample Policy Manager window:



To increase the display area, you can use the View menu to hide any of the window areas except the workspace.

Workspace

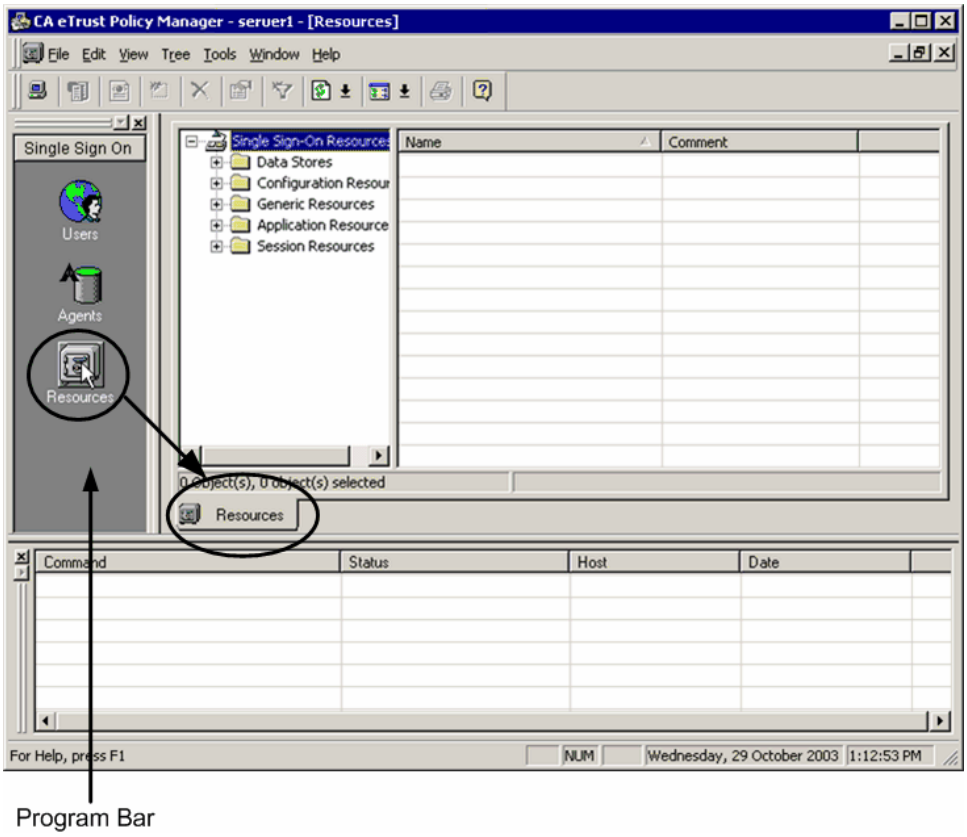
When the main window of the Policy Manager first appears, there is no application window section—only an empty workspace:



Program Bar

The program bar on the left shows an icon for each of the categories of entries you can manage with the Policy Manager.

Click an icon in the program bar to work with that category in the Policy Manager:



To display the panels on the program bar, click the buttons labeled SSO, Access Control, Windows NT, and Tools.

Users—Lets you add, remove, and edit users and user groups in your user data stores.

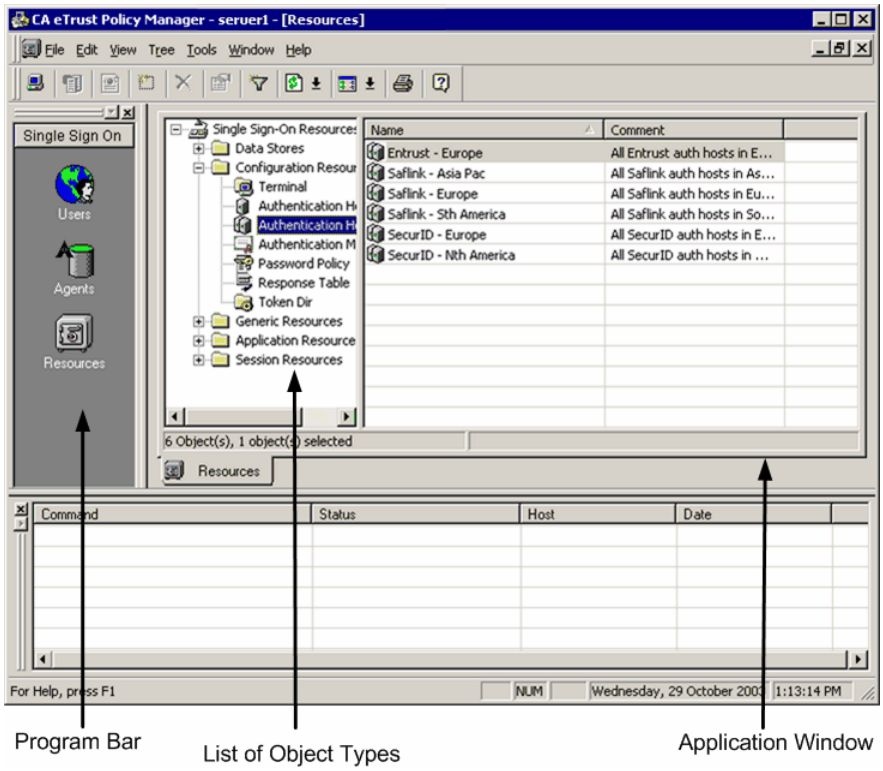
Agents—Lets you create and delete agents and agent types.

Resources—Lets you manage the data stores, configuration resources, generic resources, application resources, and agents in your policy data store.

Application Windows

The purpose of the workspace is to display application windows, which list users and resources.

To open an application window, click an icon in the program bar, or click an option in the File, Open menu.



When an application window is first opened, a list of entry types appears in the left pane of the application window. You can then click an entry type icon to see a list of all entries of that type in the right pane.

Users

eTrust SSO helps facilitate users' access to your system. It is therefore important that you know how to add and delete users from your system, and how to join users together to create user groups.

Creating a User

To create a new user:

1. Click the Users icon.

   A list of data stores appears.

   - The LDAP (eTrust Directory) data store is listed as *ps-ldap*. We recommend that you use the LDAP data store for user data.
   - The eTrust Access Control data store is listed as the name of the machine that the Policy Server is installed on.

2. Select the data store in which you want to create the new user.

   A list of any existing users in that data store appears.

3. From the Edit menu, select New, User. You can also right-click and use the pop-up menu.

   The Create New User - General dialog appears.

4. Enter the user details in the New User dialog. Use the icons in the left pane to open the other variables you can define for the user.

5. Select OK.

Deleting a User

Follow this procedure to delete a user from the data store using the Policy Manager.

1. Click the Users icon.

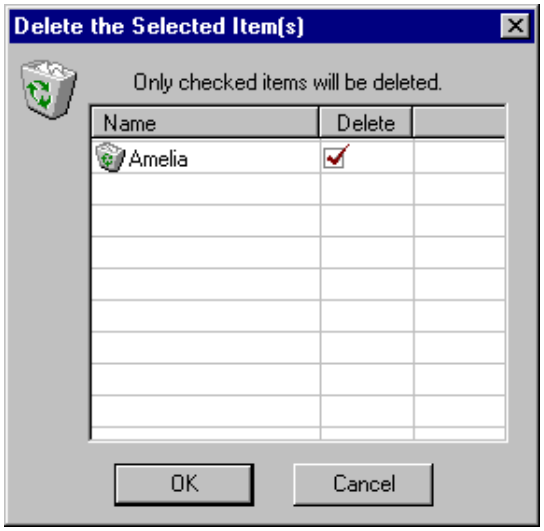
   A list of data stores appears.

2. Select the data store from which you want to delete the user.

   A list of any existing users in that data store appears.

3. Right-click on the user you want to remove, and select Delete from the pop-up menu.

   The Delete the Selected Items dialog appears.



4. Be sure a checkmark appears in the check box in the Delete column beside the user, and then click OK to delete the user.

User Groups

A group of users represents people who work together on specific projects or belong to a specific department or to the same division in the organization. How you group users depends on how your company is organized and how your users work.

Creating User Groups

Follow this procedure to create a user group in the data store using the Policy Manager.

1. Click the Users icon.

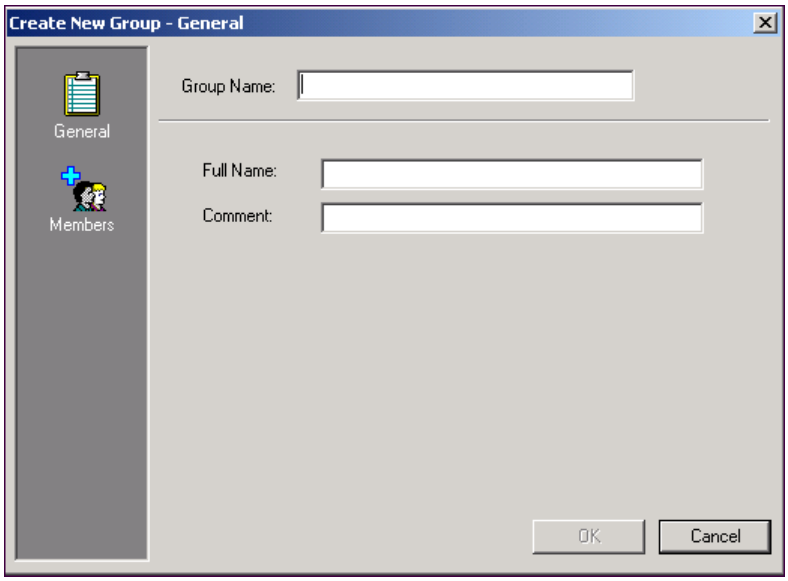
   A list of data stores appears.

2. Select the data store in which you want to create the new user group.

   A list of any existing users in that data store appears.

3. From the Edit menu, choose New, Group.

   The Create New Group - General dialog appears.



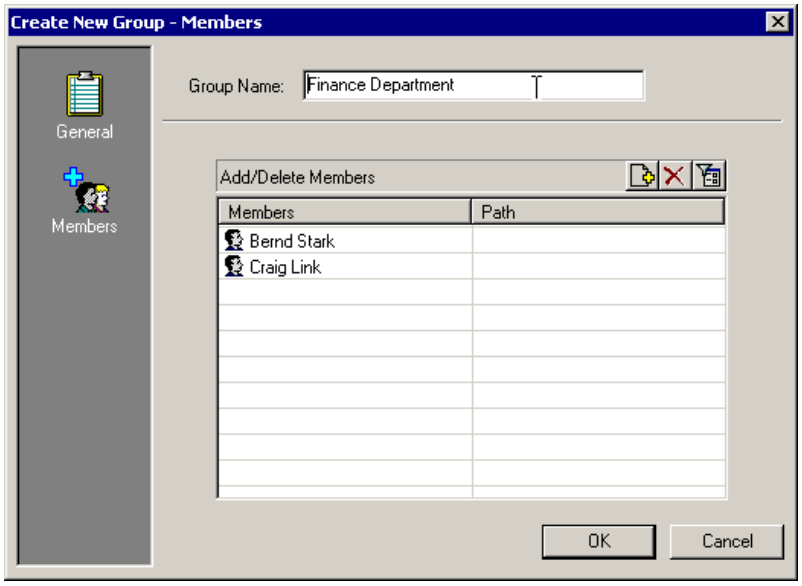
4. Enter the group name in the Group Name field.

   You can also enter a longer name and a comment about this group in this dialog.

5. Click the Members icon on the left.

   The Create New Group – Members dialog appears.

6. Use the Add and Delete and Filter buttons  to help you add users to the group.



7. Once you had added all the users you want to the group, select OK.

   The new User Group is saved and now appears in the list of users with a slightly different icon from individual users. 

Tip: The filter can help you organize and filter usernames. You can use an asterisk as a *wild card* character, for example, if you type *G** you will see all users whose username starts with a G.

Adding and Removing Group Members

There are three ways you can change the membership of a group:

- **Add members while creating a group**—Using the Members tab of the Create New Group dialog
- **Add or delete members from an existing group**—Using the Members tab of the View or Set Group Properties dialog
- **Add or remove group name from a user's record**—Using the Groups tab of the View or Set User Properties dialog

  When defining users, you can only add members to an existing group; if the group does not exist, you must create the group before you can add members to it.

Deleting a User Group

To delete a user group from the Policy Manager follow these steps.

1. Click the Users icon.

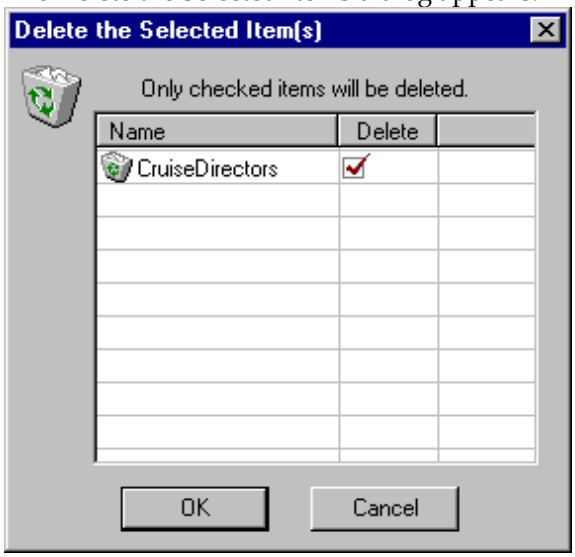
A list of data stores appears.

2. Select the data store from which you want to delete the user group.

   A list of any existing users in that data store appears.

3. Right-click on the user group you want to remove, and select Delete from the pop-up menu.

   The Delete the Selected Items dialog appears.



4. Be sure a checkmark appears in the check box in the Delete column beside the user, and then click OK to delete the user group.

Administrators

This section describes how to define eTrust SSO administrators and how to set their computer access rights.

Defining an eTrust SSO Administrator

The follow instructions describe how to set up an eTrust SSO administrator.

Please note that you can only define administrators in the eTrust Access Control data store. Normal eTrust SSO users should be created in the eTrust Directory LDAP (ps-ldap) data store, but administrators need to be defined in eTrust Access Control (name of the computer that the Policy Server is installed on).

Important! *When defining an administrator, the name you enter in the User Name field cannot contain a space. For example, you cannot enter* ***John Smith*** *as the value for User Name, but you can enter* ***JohnSmith***, ***John-Smith***, ***jsmith*** *or* ***John_Smith***.

To define an administrator:

1. Create a new user (see Creating a New User)
2. Right-click on the user, and select Properties.

   The View or Set User Properties – General dialog appears.
3. Browse to add SSO to the user's Authentication Method, if this is not already set.

   Setting a new password for SSO authentication changes the password in the operating system.
4. Select User Options icon from the left pane.

   The View or Set User Properties – User Options dialog appears.
5. Check the Administrator check box, in the User Type section.

   When you designate a user as an administrator, this user is also created in the native OS environment.

   If the Administrator check box is not available, check which user data store you are working with. You cannot store administrators on the eTrust Directory (ps-ldap). You should use eTrust Access Control (Policy Server computer name) to store administrators.

Note: You should now grant the new administrator access rights for the machine on which they will use the Policy Manager to administer the Policy Server. For more information about granting computer access rights, see Setting the Administrator Computer Access Rights.

Setting the Administrator Computer Access Rights

After you have created an eTrust SSO administrator, you should grant the new administrator access rights for the machine on which they will use the Policy Manager to administer the Policy Server.

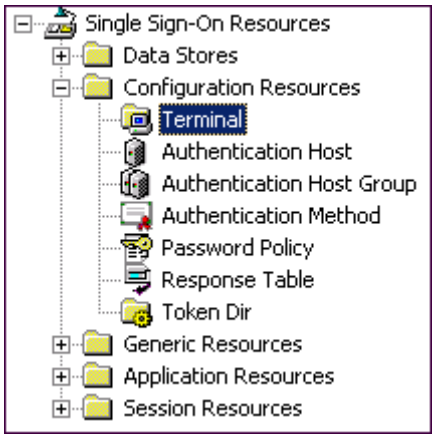
1. Select the Resources icon from the left hand pane.

   The Single Sign-On Resources folders appear.

2. Expand the Configuration Resources folder, if it is not already expanded.

   A list of the configuration resources is displayed.

3. Select the Terminal configuration resource.



   A list of computer names appears in the main window.

   These computers can all be configured to give the administrators access to the Policy Server, using the Policy Manager. You can configure each computer to either give all administrators who log on to that computer access to the Policy Server, or you can define specific administrators to have access to the Policy Server, and block all other administrators.

4. To add a computer to this list, right-click and select New.

   The Create New Terminal Resource – General dialog appears.

5. Enter the full name of the computer and click OK.

   The new computer or *terminal* has been added to the list.

6. To set access rights to the Policy Server, right-click the computer name that you want to configure. This computer must have the Policy Manager software installed.

   The View or Set Terminal Properties – General dialog appears.

To give *all* administrators who log onto the computer access to the Policy Server:

a. Click the Set Default Access button.

   The Set Default Access dialog appears.

b. Click the All button then click OK.

   To give specific administrators who log onto the computer access to the Policy Server:

a. Select the Authorize icon in the left pane.

   The View or Set Terminal Properties – Authorize dialog appears.

b. Use the Add, Edit and Delete buttons  to select administrators that you want to have access rights to the Policy Server from this computer.

Deleting an Administrator

eTrust SSO requires at least one administrator-level user.

This means that you cannot delete the last user who is defined as an Administrator.

You also cannot clear the Administrator check box on the User Attribute dialog for the last user.

Sessions

An eTrust SSO session is the period of time that a user is logged into eTrust SSO. During an eTrust SSO session, the user may be logged in to many other eTrust SSO-enabled applications.

By default, eTrust SSO lets users have multiple concurrent sessions on different computers. However, using eTrust SSO you can set up automatic session management rules to limit the number of concurrent sessions a user has open and the behavior of those sessions. You can also work with sessions manually using the Session Administrator.

To discourage user sharing logon IDs and to save system resources, the Policy Manager lets you:

- Set the maximum number of sessions a user can have open at the same time
- Define what happens when a user attempts to exceed this number of sessions
- Manually terminate any sessions

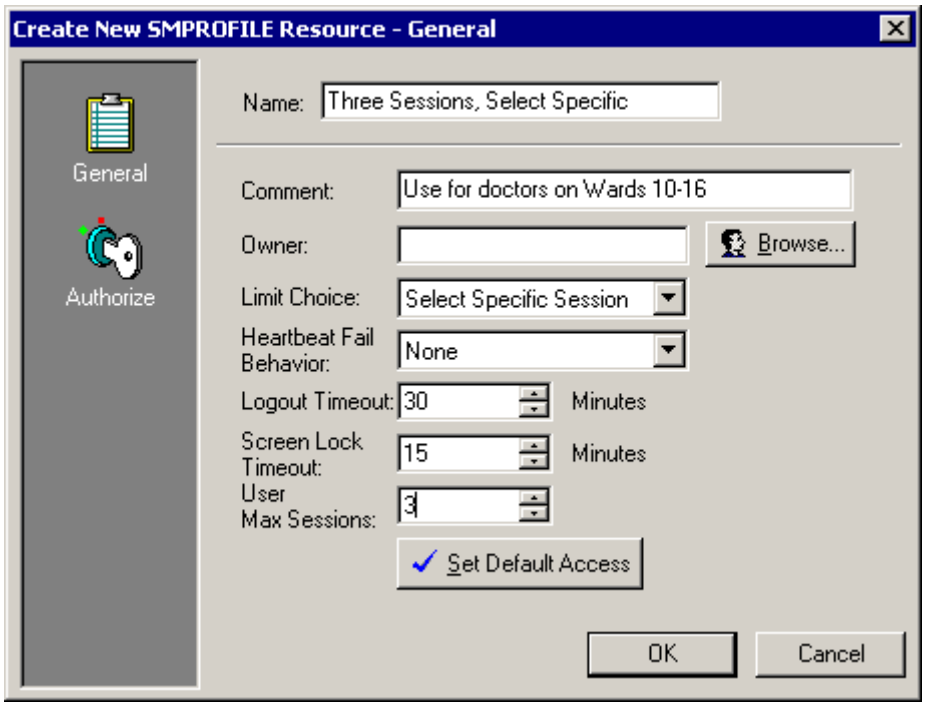
To protect sensitive information, you can use the Policy Manager to set the following:

- An idle time-out for logging the user out of the eTrust SSO session as well as logging out the underlying Windows user
- An idle time-out for logging the user out of the eTrust SSO session

Create a Session Profile

To create a session profile that can be applied to users to define their eTrust SSO session behavior, follow these steps.

1. From the Start menu, open the Policy Manager.
2. Click the Resources icon, then select Single Sign-On Resources, Session Resources, Session Profile in the tree.
   The list of existing session profiles appears.
3. Right-click anywhere in the list area, and select New.
   The Create New SMPROFILE dialog opens.



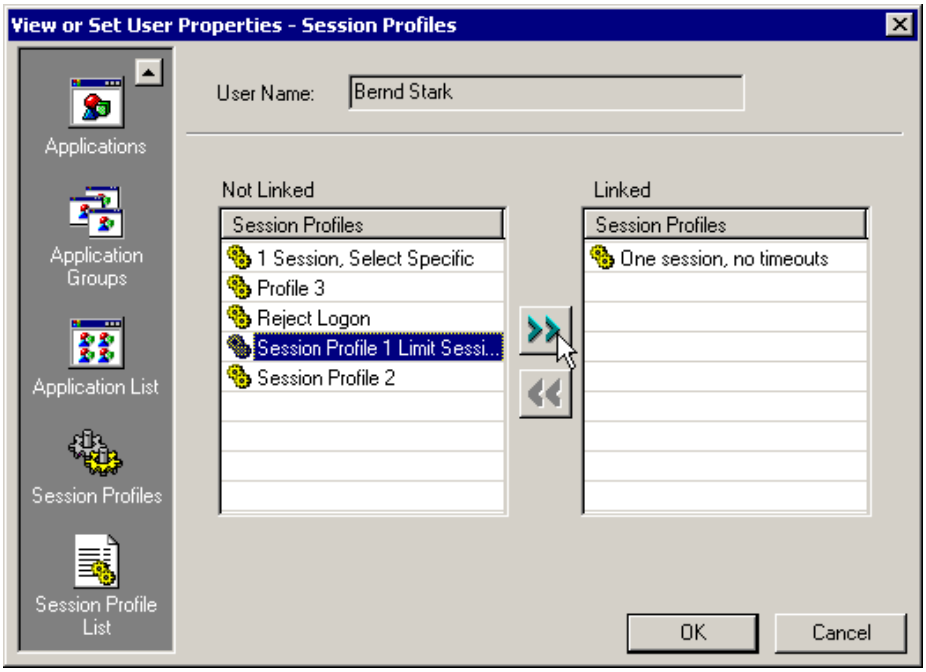
4. In the General dialog, set the behavior for the profile.
5. In the Authorize dialog, set permissions for users or groups to access the new session profile.
6. Click OK to save the new profile.

Apply a Session Profile to a Single User

To apply a session profile to a user to control their eTrust SSO session behavior, follow these steps.

To apply a session profile to a single user, follow these steps:

1. In the Policy Manager, open the Users section, and double-click a group or user name to open the User Properties dialog.
2. Select the Session Profiles section on the left of the dialog. The list shows the groups of which this user is a member.

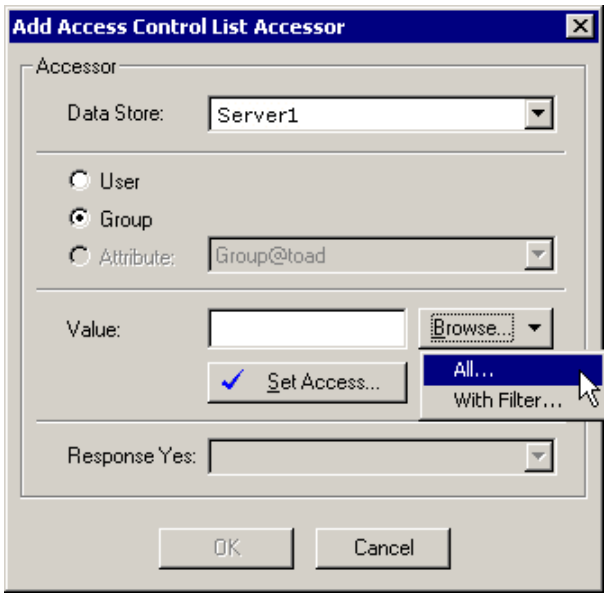


3. Select one or more session profile names in the list on the left, and click the  icon to apply the session profiles.
4. Click OK to close the dialog. The session profiles are assigned to the user.

Apply a Session Profile to a Group

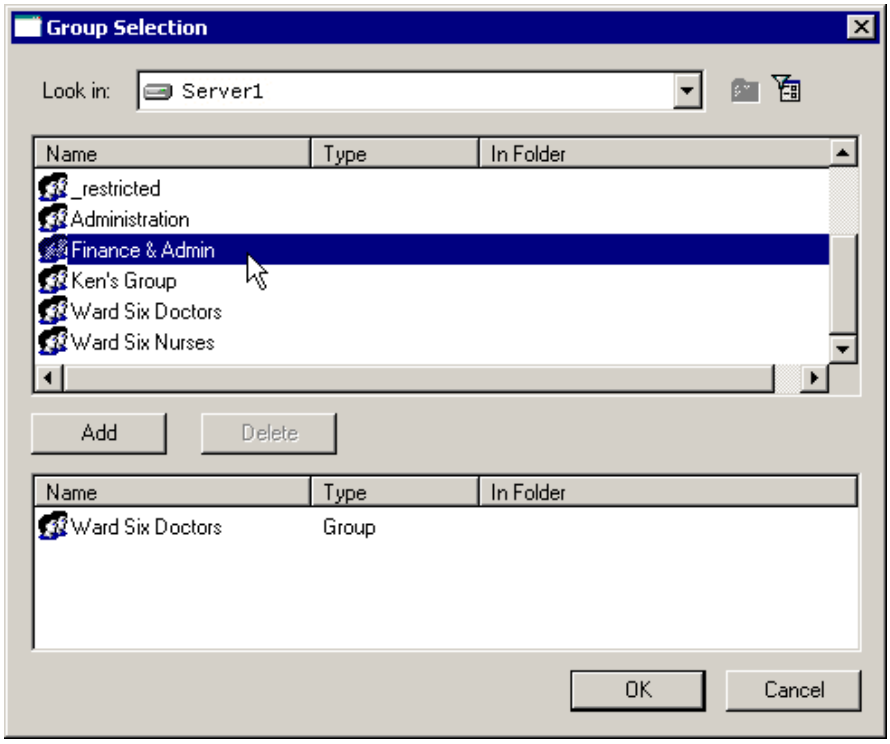
To apply a session profile to a user group to control their eTrust SSO session behavior, follow these steps.

1. In the Policy Manager, navigate to the Resources, Session Profiles section.
2. Double-click a session profile name to open the View or Set SMPROFILE Properties dialog.
3. Click the Authorize icon in the bar on the left.
4. Click the Add icon. The Add Access Control List Accessor dialog appears.



5. In the Add Access Control List Accessor dialog, make the following selections:
   a. Select the data store that stores the group.
   b. Select the Group option.
   c. If you know the exact name of the group, enter the group name in the Value field, and click OK.

      Otherwise, click Browse to open the Group Selection dialog, which shows a list of group names. You can either view all group names, or you can filter the list.



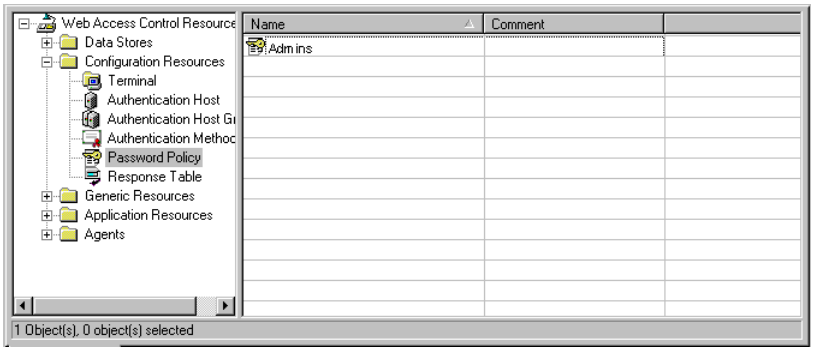
d. In the Group Selection dialog, select one or more group names on the top pane, and click Add.

6. Click OK on all open dialogs to return to the main Policy Manager window. The session profile is applied to the groups you selected.

Password Policies

A password policy is a set of rules used by eTrust SSO to ensure that users select reliable passwords. The password policy defines password parameters such as the minimum number of characters in a password and the maximum time until expiration.

To display a list of defined password policies, open the Configuration Resources folder and click the Password Policy entry. The created password policies will be listed.



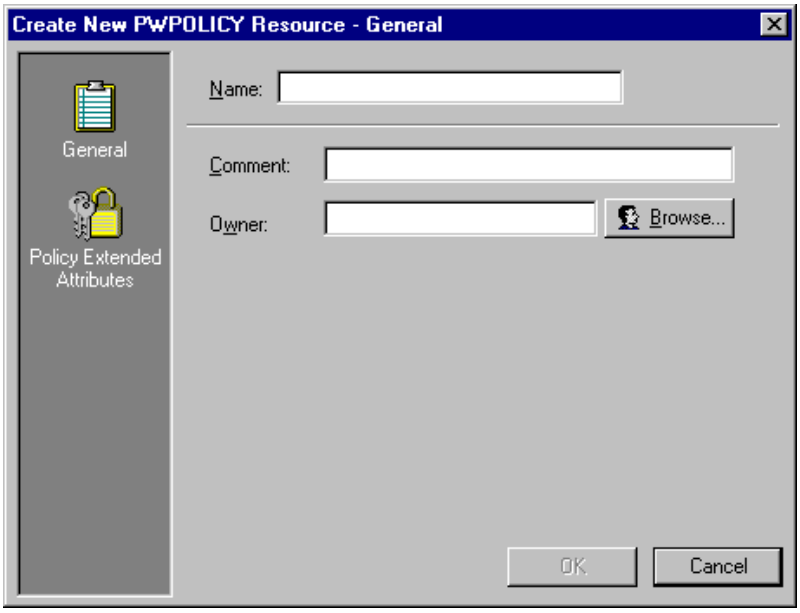
From the list of password policies you can:

- Add a new password policy
- Delete a password policy
- Locate a password policy in the list
- Change the properties of a password policy.

To perform any of these actions, select the appropriate command from the Edit menu or right-click in the list of password policies to display the pop-up menu and select the command from the command list.

Defining Password Policy Properties

Whenever you add a new password policy, you must specify its properties by completing a set of dialogs associated with the Create New PWPOLICY Resource dialog. The following example shows the Create New PWPOLICY Resource dialog; the bar on the left lists the associated dialogs.



The dialogs for defining a password policy's properties are:

General—Defines the password policy's name and owner.

Policy Extended Attributes—Defines specific password characteristics (such as minimum and maximum length of the password, what types of characters can be used in the password, how many days before the password expires, how many past passwords to retain, and other parameters).

When defining password policies, you must complete the General and Password Extended Attributes dialogs.

Updating Password Policy Properties

To change the properties of an existing password policy:

1. Display the list of password policies.
2. Locate the policy you want to change and double-click its entry in the list.

   This displays the View or Set PWPOLICY Properties dialog.
3. Make any changes that are necessary and click OK when you are finished.

Chapter 9

Frequently Asked Questions

This chapter contains answers to questions often asked about eTrust Single Sign-On (eTrust SSO).

Functionality and Benefits

The following are questions about the functionality and benefits of eTrust SSO. For additional information about the functionality and benefits of eTrust SSO, see the Advantages of Using eTrust SSO section of the "Introduction to eTrust SSO" chapter in this guide.

Question: What is eTrust Single Sign-On?

Answer: eTrust Single Sign-On (eTrust SSO) is a product that can be configured so that end users only have to authenticate (log on and identify themselves) once to gain access to all of their secure desktop applications. This includes some web browser-based applications.

Question: Who benefits from eTrust SSO?

Answer: Users benefit from eTrust SSO because it automates frustrating logon processes. Administrators benefit from eTrust SSO because it provides an efficient centralized administration system and gives greater control over user sessions. Security is increased with eTrust SSO because it provides secure logon and authentication processes and reduced written passwords.

Question: What makes eTrust SSO different from other solutions?

Answer: eTrust SSO is one of the most sought after solutions. Many early single sign-on solutions have either disappeared or have been reformulated to catch up with market requirements. eTrust SSO was conceived from the start with an open architecture and flexibility that has enabled it to stay ahead of fast-changing customer requirements by adjusting to the exact requirements of the customer environment, and allowing a phased implementation. eTrust SSO also supports a wide range of native and external authentication methods.

Question: How is communication secured between the SSO Client and the Policy Server?

Answer: The communication between the SSO Client and the Policy Server is fully encrypted using Triple-DES algorithm and El-Gamal key management. DES (data encryption standard) is a 112-bit encryption algorithm designed to secure data and information.

Passwords and Logon

The following are questions about passwords and logon within eTrust SSO. For additional information about passwords and logon within eTrust SSO, see the Advantages of Using eTrust SSO section of the "Introduction to eTrust SSO" chapter, and the "Common eTrust SSO Processes" chapter in this guide.

Question: Can an organization audit user logons?

Answer: Yes, eTrust SSO provides audit capabilities to record and store all logon activity. eTrust SSO auditing includes user logons, access to the Policy Server, requests for application lists, failed logon attempts, and more.

Question: Can eTrust SSO be used to log users into their operating system and connect to the domain?

Answer: Yes, you can configure eTrust SSO to appear as the first point of identification for a user when they log on to their computer. The user can log on using any of the supported authentication methods. The user is then automatically logged on to the operating system and domain using their Windows credentials.

Question: Do users have to restart their workstations at the start of each day?

Answer: Users are not forced to reboot their computers at any time. If a user needs to re-authenticate they are prompted to do so by the Client. You can set how long a session remains active. Also, you can use the eTrust SSO Station Lock facility to prevent access to applications by unauthorized users, and to force re-authentication for different users accessing the same computer.

Question: How does eTrust SSO handle password expirations?

Answer: eTrust SSO handles password expiration in several ways. eTrust SSO can:

- Accommodate user password expiration for target applications through error handling
- Enforce primary password expiration automatically through the Policy Server, if eTrust SSO native authentication is used
- Automatically generate new application passwords at regular intervals to prevent password expiration.

Question: Does eTrust SSO work in an environment where people share workstations?

Answer: Yes. eTrust SSO stores all logon information centrally on the *Policy Server*. This not only permits roaming users, it also facilitates the sharing of workstations. Also, eTrust SSO supports a feature called Station Lock that can prevent unauthorized access to applications and force different users to authenticate to the same workstation. eTrust SSO contains special logic to support the switching of user sessions without having to restart the computer.

These capabilities are useful in kiosk situations or in clinic environments at nurse stations.

Question: Can eTrust SSO manage multiple SSO sessions for a single user?

Answer: Yes. eTrust SSO lets organizations configure a permissible number of concurrent SSO sessions per user and can automatically log off the user after a preset time (in addition to the screen time-out).

Question: How does eTrust SSO let users move from workstation to workstation with an active session?

Answer: eTrust SSO can be configured to work within a Citrix Metaframe environment to return a user to the same place in an application on a different workstation. This is called Metaframe Session Migration. This can be used in conjunction with session management, to let users move to a new workstation and keep working even if they haven't logged off the previous workstation.

Question: Can eTrust SSO keep passwords consistent across all applications and systems in an organization?

Answer: Yes, eTrust SSO reduces the complexity of a user's logon process and saves them memorizing multiple passwords. Additionally, although this is not mandatory, eTrust SSO supports password synchronization that propagates a known password to any number of target applications.

Question: How does eTrust SSO relate to disaster recovery?

Answer: When implementing eTrust SSO, you should recognize that eTrust SSO is a mission-critical application and include it in your disaster recovery procedures. Also, the Policy Server supports failover and load balancing, making full use of available resources and providing redundancy in the event of computer failure.

Authentication

The following are questions about authentication within eTrust SSO. For additional information about authentication, see the "Common eTrust SSO Processes" and "Concepts Behind eTrust SSO" chapters in this guide.

Question: What authentication methods does eTrust SSO support?

Answer: For a complete list of supported authentication methods, see the "Concepts Behind eTrust SSO" chapter in this guide.

Question: Is it possible to set multiple authentication methods for different users?

Answer: Yes. You can authenticate using different methods or you can you can write your own authentication methods to suit your company's needs.

Implementation

The following are questions about implementation of eTrust SSO. For additional information about implementation, see the *eTrust SSO Implementation Guide*.

Question: How long does it take to implement eTrust SSO?

Answer: The length of time it takes to implement eTrust SSO depends on the size of your enterprise. You can implement eTrust SSO in phases to provide immediate benefits. A phased approach is often preferred when implementing eTrust SSO in a complex environment with a large number of applications and systems. For more information about implementation, see the *eTrust SSO Implementation Guide*.

Question: How do you determine the staffing numbers and skills required for a successful eTrust SSO implementation?

Answer: The minimum requirements for a successful implementation are:

- An implementation manager to set a strategy for implementing and organizing groups, setting policies, and managing the business issues.
- A programmer with basic programming skills who is dedicated to writing eTrust SSO logon scripts
- A systems administrator who has experience with network server platforms (Windows and/or UNIX).

For more information about the skills required to implement and maintain eTrust SSO, see the *eTrust SSO Implementation Guide*.

Integration

The following are questions about the integrations of eTrust SSO within your organization.

Question: What target applications does eTrust SSO support?

Answer: Tcl scripts are written individually for each target application, so eTrust SSO can support most applications and systems on Windows, UNIX, mainframe, or other legacy system.

Question: How can homegrown applications integrate with eTrust SSO APIs?

Answer: There are two ways that eTrust SSO can provide authentication to homegrown applications:

- Use Tcl Scripts to mimic the user actions to logon like any commercial application.
- Modify your homegrown application to use an eTrust SSO API, which eliminates the need to develop and maintain Tcl scripts for that application.

Question: Where does eTrust SSO keep user data?

Answer: eTrust SSO supports multiple identity repository options. It stores user data in the embedded copy of eTrust Directory that is installed with eTrust SSO. eTrust Directory is a secure and highly scalable X.500 directory with replication, shadowing and failover. Organizations with a large amount of user information in existing corporate directories can leave the data in place in their existing LDAP directories. Organizations may also choose to keep the user data in the embedded copy of eTrust Access Control that comes with the Policy Server. This is a highly secure repository with fine-grained permission on user data access. Organization may choose to keep the information about different parts of their user population in different repositories.

Question: What methods of application logons does eTrust SSO support?

Answer: Because eTrust SSO mimics keyboard and mouse input, it supports any logon method that uses mouse or keyboard input. eTrust SSO also supports mainframe pass-tickets and app-tickets.