*e*Trust™ Single Sign-On

Implementation Guide

r8

Computer Associates®

Second Edition

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

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

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

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

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

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

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

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

© 2005 Computer Associates International, Inc.

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

Contents

Chapter 1: Understanding eTrust SSO

Chapter 2: Example Implementation

Chapter 3: Implementation Overview

Chapter 4: Planning The eTrust SSO Implementation

Chapter 5: Implementing the eTrust IAM Common Components

Chapter 6: Implementing the Policy Manager

Chapter 7: Implementing Authentication

Chapter 8: Implementing the SSO Client

Chapter 9: Adding Applications to SSO

Chapter 10: Implementing Session Management

Chapter 11: Implementing Password Agents

Chapter 12: Implementing Citrix Application Migration

Chapter 13: Implementing a Server Farm

Chapter 14: Upgrading

Chapter 15: Uninstalling

Chapter

1 Understanding 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. This includes some web browser-based 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.

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.

Quickly Updated Application Lists

You can configure the application list to automatically refresh. This means that if you want to add a new application to a user's eTrust SSO application list, the user does not have to log out, then log back on to eTrust SSO to have access to the new application.

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 now use the central administration GUI, the Policy Manager, to set and maintain the entire organization's access strategy. The Policy Manager saves time because you do not have to maintain multiple systems.

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. This is the primary interface for 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 *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 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

Because users no longer have to remember multiple passwords, 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 scanner) 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 existing 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 existing Windows screen lock

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 Session Administrator section in this chapter.

For information about how multiple concurrent eTrust SSO sessions can benefit users, see the Multiple eTrust SSO Sessions 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 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
Cert	Digital certificates
RSA SecurID	Secure ID card + PIN
SAFLINK	Biometric devices (for example iris, fingerprint, voice, proximity)
Politec	Biometric devices (for example iris scan, finger print)

If you want to use an authentication method not listed here, you can create your own authentication agent. Contact your CA representative for further details.

Enhanced Flexibility

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

Identity and Access Management

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 AC

Provides end-to-end platform and system resource security.

eTrust Web AC

Enables secure intranet and extranet management.

eTrust SSO

This product.

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 legacy 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 native authentication method that comes with eTrust SSO, SSO or LDAP, 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 eight external authentication methods, or you can 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

Example Implementation

The following scenario is designed to help get you started with eTrust Single Sign-on (eTrust SSO) as quickly as possible. This scenario guides you through the steps it takes to set up eTrust SSO in a specific configuration. We suggest that you set up the scenario in a test environment before you install this in a live environment.

Configuration Scenario

The following is a description of a typical eTrust SSO installation. This scenario does not require access to any live systems. For example, you will not need access to the domain controller to set up this test scenarios.

This is one of the most common eTrust SSO configurations.   The key points of the scenario are:

- **Data Stores - User Information**
  Store users in Active Directory. In this example, the company has existing users that are stored in a hierarchical structure and they want to configure SSO to use the existing user repository.

- **Data Stores - Application Access Information**
  Store users in Active Directory. Users and/or groups will determine which applications each end-user has single sign-on access to.

  Store application access information in eTrust Access Control.

- **Data Stores - Logon Information**
  Store logon information in eTrust Directory embedded on the Policy Server (supplied with eTrust SSO).

- **Authentication**
  Use LDAP authentication against Active Directory data store.

eTrust SSO with Active Directory

Before You Begin

The Before You Begin Section is designed to guide you through what you need to know before you implementing this scenario.

Operating Systems You Will Need

To set up this scenario in a test environment you will need the following software.

Software Required	SSO Components That Will Use It
Windows 2000 Server	Policy Server Provisioning Server GUI Server Directory Server
Windows 2000 Server	Policy Server
Windows 2000 Server or Windows XP SP 2	Policy Manager
Windows XP SP 2	SSO Client
Windows 2000 Server	LDAP Authentication Agent (This should be on a separate computer to the other components)

Understanding the Implementation

This section is a summary of the steps that you need to perform to set up the example scenario for eTrust SSO. The rest of this chapter explains each step in detail. We recommend that you work through this chapter in the order it is written until you understand the process fully:

1. Configure Windows 2000 as a domain controller with Active Directory
2. Create a number of test users within Active Directory
3. Install the common components (SSO only) into a server farm
4. Install the Policy Manager
5. Configure the Policy Server
    - Set Policy Server to use Active Directory as a user data store
    - Setup Directory DSA to use Active Directory
    - Verify User Data Store Configuration
6. Install and configure the LDAP Authentication Agent
7. Install and configure the SSO client
8. Create and test an application

Step 1: Configure Windows 2000 As A Domain Controller

This procedure explains how to set up a Windows 2000 Server as a Domain Controller.

Note: You may need the Windows 2000 installation CD during the setup.

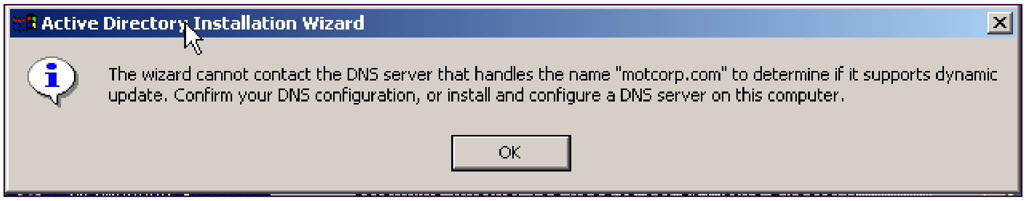
1. From the Start menu on your Windows 2000 Server, select Programs, Administrative Tools, Configure Your Server.

   The Windows 2000 Configure Your Server dialog appears.

2. From the left hand menu select Active Directory.
3. Scroll down and select the Start link.

   The Active Directory Installation Wizard appears.

4. Click Next, then select "Domain Controller for a new domain" option.
5. Follow the prompts to configure the Domain Controller. You can accept the defaults.
   - When prompted to enter the New Domain Name (full DNS), enter a domain name. For example, "acmecorp.com".
   - When you get the following warning, just click OK



The wizard cannot contact the DNS server that handles the name "motcorp.com" to determine if it supports dynamic update. Confirm your DNS configuration, or install and configure a DNS server on this computer.

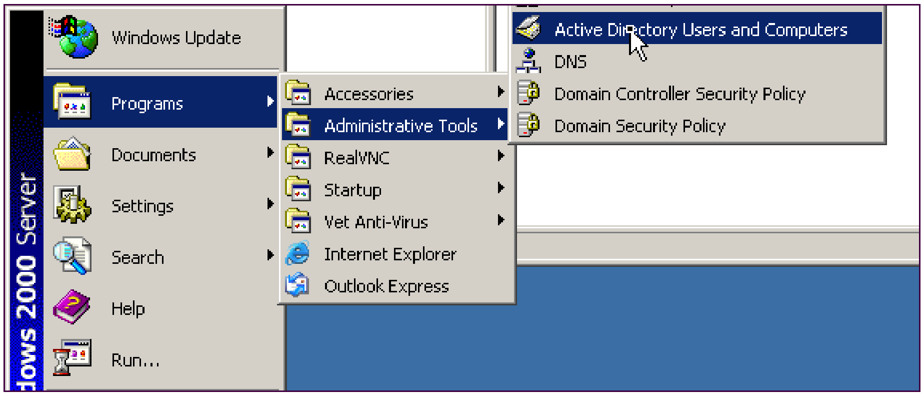
6. When you are finished, restart the computer as prompted.

Step 2: Create Test Users Within Active Directory

This procedure tells you how to set up some test users in Active Directory in a hierarchical structure. The examples in this procedure will be referred to throughout this scenario.

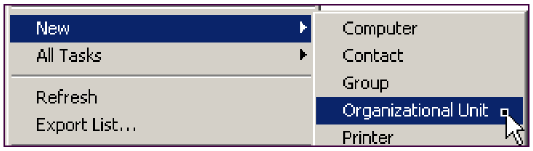
1. Logon to the Domain Controller as a Windows user with administrative privileges (i.e. is a member of the 'Administrators' group), preferably as a built-in 'Administrator' account.

2. From the Start menu select, Programs, Administrative Tools, Active Directory Users and Computers.



The Active Directory Users and Computers dialog appears.

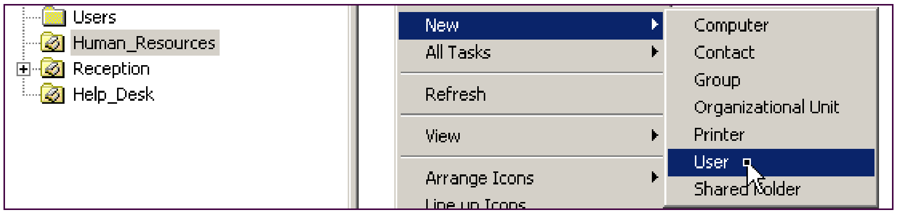
3. Select the domain (AcmeCorp.com) in the left pane, then right-click in the right pane and select New, Organizational Unit from the menu.



4. Create three new organizational unit folders:

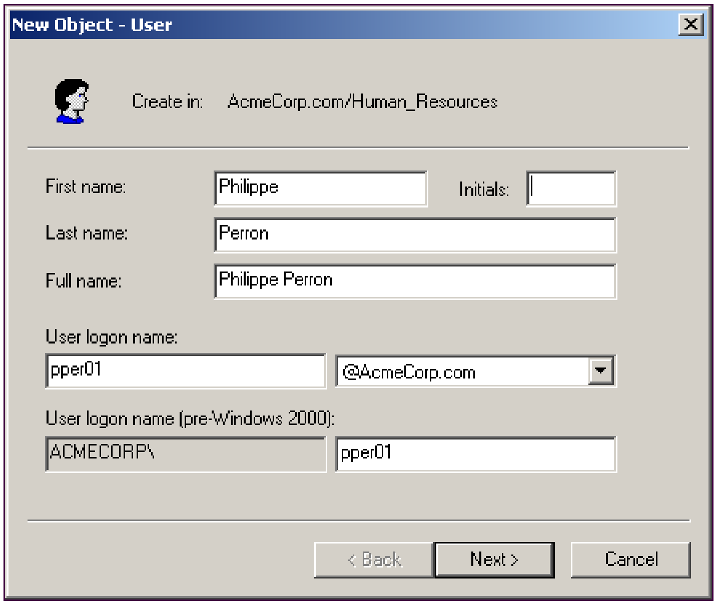
   - Human_Resources
   - Help_Desk
   - Reception

5. Select the Human_Resources folder from the tree in the left pane, then right-click in the right pane and select New, User from the menu.



The New Object – User dialog appears.

6. Fill in the necessary fields to create a test user called Philippe Perron, then click Next.
   First name: Philippe
   Last name: Perron
   User logon name: pper01



New Object - User

Create in: AcmeCorp.com/Human_Resources

First name: Philippe

Initials:

Last name: Perron

Full name: Philippe Perron

User logon name: pper01 @AcmeCorp.com

User logon name (pre-Windows 2000): ACMECORP\ pper01

7. Enter and confirm the user password, leaving the checkboxes empty. Click finish to create the user object in Active Directory.

   Remember the password. You will need it later in the chapter.

8. Repeat steps 5, 6 and 7 to create two other test users:

   Organizational group: Help_Desk
   First name: Prani
   Last name: Patil
   User logon name: ppat01

   Organizational group: Reception
   First name: Penelope
   Last name: Price
   User logon name: ppri01

9. Select the Users folder from the tree in the left pane, then right-click in the right pane and select New, Group from the menu.

10. Enter the Group name as ssoUsers and click OK.

11. For each of the three users created, right click on the user name and select ‘Add members to a group’ from the menu. Add each user to the ssoUsers group.

Step 3: Install the Common Components (Server Farm)

For information about installing the IAM Common Components, including the Policy Servers in a server farm configuration, see the “Implementing the IAM Common Components” chapter of this guide.

Step 4: Install the Policy Manager

To install the Policy Manager component of eTrust SSO using the graphical wizard, follow these steps:

1. Insert the product installation CD into your CD-ROM drive.

   If you have Autorun enabled, the Product Explorer automatically displays. Otherwise, navigate to the CD-ROM drive and double-click the PE_i386.EXE file.

2. From the Product Explorer main menu, select Policy Manager for Windows, and click Install.

3. Follow the wizard prompts and when you are done, click Install to start the Policy Manager installation.

   You can accept all the default settings when you install the Policy Manager.

   Note: If you previously installed the Policy Server on this computer, you need to stop eTrust Access Control when prompted to do so.

Step 5: Configure the Policy Server

Step 5a: Create a DSA Router to Active Directory

To create an eTrust Directory DSA that routes LDAP traffic from the local eDirectory server to AD (a DXlink in eDirectory terms) follow these steps:

1. Using Windows Explorer, go to the following directory:

   `C:\Program Files\CA\eTrust Directory\dxserver\config\knowledge`

2. Create an empty text file named "AD_ACMECORP_Router.dxc". Substitute ACMECORP for the actual AD domain name.

   Note: If Windows Explorer is set to hide extensions, the file may incorrectly be created with the extension ".dxc.txt". This is not correct and you must change the Windows Explorer setup and rename with just the extension ".dxc".

3. Using notepad, copy the following into the file and change :

   - "svrpol01" to the Active Directory computer name
   - "acmecorp" to your domain name

   Note: The domain components in the last parameter are in reverse order from usual.

```
# Computer Associates DXserver/config/knowledge
# AD_ACMECORP_Router.dxc
# Routes to Active Directory on ACMECORP domain
# Refer to the Admin Guide for the format of the set dsa command.
set dsa AD_ACMECORP_Router =
{
     prefix          = <dc "com"><dc "acmecorp">
     native-prefix   = <dc "com"><dc "acmecorp">
     dsa-name        = <o AD_ACMECORP><cn AD_ACMECORP_Router>
     dsa-password    = "secret"
     address         = tcp "svrpol01" port 389
     auth-levels     = clear-password, ssl-auth
     dsa-flags       = read-only
     trust-flags     = allow-check-password, no-server-credentials, trust-
                       conveyed-originator
     link-flags      = dsp-ldap, ms-ad
};

set transparent-routing = true ;
```

   Note: Please note the following points that affect this file:

   - In the address line, replace "svrpol01" with the host name (machine name) of the Domain Controller.
   - The "read-only" dsa-flag prevents updates to AD from the Policy Server (even if the account used by the user data store has domain admin privileges).

4. Using notepad, open PS_Servers.dxg and add above to end the file.

   ```
   source "AD_ACMECORP_Router.dxc";
   ```

   For example:

   ```
   # Computer Associates DXserver/config/knowledge/
   #
   # PS_Servers.dxg written by eTrust PS Installation
   #
   # Description:
   #   Use this file to group and share DSA knowledge.
   #   PS DSA's source this file
   #   from its initialization file.
   #
   source "../knowledge/PS_ACMECORP.dxc";
   source "../knowledge/PSTD_ACMECORP.dxc";
   source "AD_ACMECORP_Router.dxc";
   ```

   You must now restart the eTrust Directory service.

5. Go to the Windows Start menu and select Programs, Administrative Tools, Services.

6. Find the service called “eTrust Directory – PS_ACMECORP”

7. Right-click and select Restart from the menu.

Step 5b: Configuring the Directory Access Controls to allow the DXlink to Active Directory

To be able to successfully dxlink to the Active Directory you will need to update the Directory Access Controls.

1. Using Windows Explorer, go to the following directory:

   ```
   C:\Program Files\CA\eTrust Directory\dxserver\config\access
   ```

2. Open the PS_Access.dxc file in a text editor.

3. Add the following information to the group section at the top of the file:

   ```
   set group = {
       name = "AD_Group"
       users = <dc "com"><dc "acmecorp"><ou "Help_Desk"><cn "Prani
       Patil">
   };
   ```

   This adds the user ‘Prani Patil’ from the Active Directory data store to a group name ‘AD_Group’

4. In the “Give Admin users access to PS and PSTD tree's” section add the following:

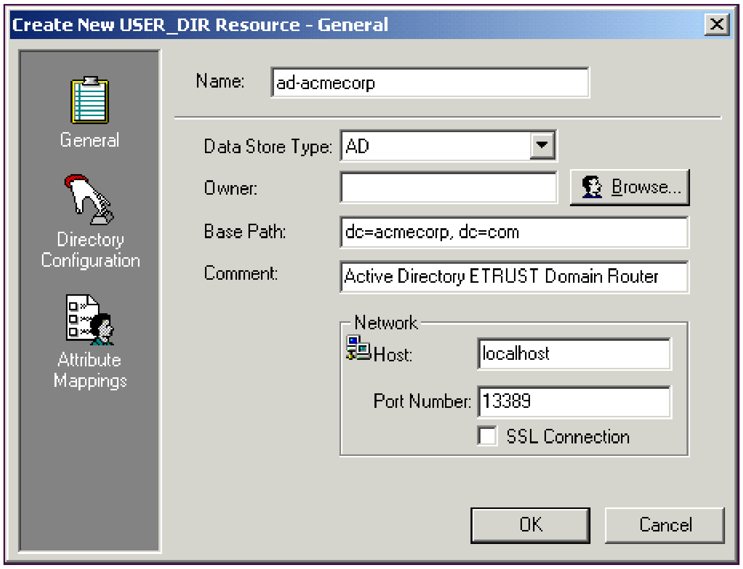
   ```
   set admin-user = {
       group = "AD_Group"
       subtree = <dc "com"><dc "acmecorp">
   };
   ```

   The configures the Directory to allow a connection to read the Active Directory tree as long as the user trying to access it through the policy server DSA is listed in the AD_Group Access Controls group.

Step 5c: Create a User Data Store on the Policy Server to use Active Directory

Create a user data store that points to AD for user records and local LDAP for the user's login variables.

1. Log on to the Policy Manager.
2. Go to Resources, Single Sign-On Resources, Data Stores, User Data Stores.
3. Right-click in the right pane and select New from the menu.
4. Enter the following in the dialog box:
   - Name: ad-acmecorp
   - Data Store Type: AD
   - Owner: [blank]
   - Base Path: dc=acmecorp, dc=com
   - Comment: Active Directory ETRUST Domain Router
   - Host: localhost
   - Port: 13389



Create New USER_DIR Resource - General

Name: ad-acmecorp

Data Store Type: AD

Owner:

Base Path: dc=acmecorp, dc=com

Comment: Active Directory ETRUST Domain Router

Network

Host: localhost

Port Number: 13389

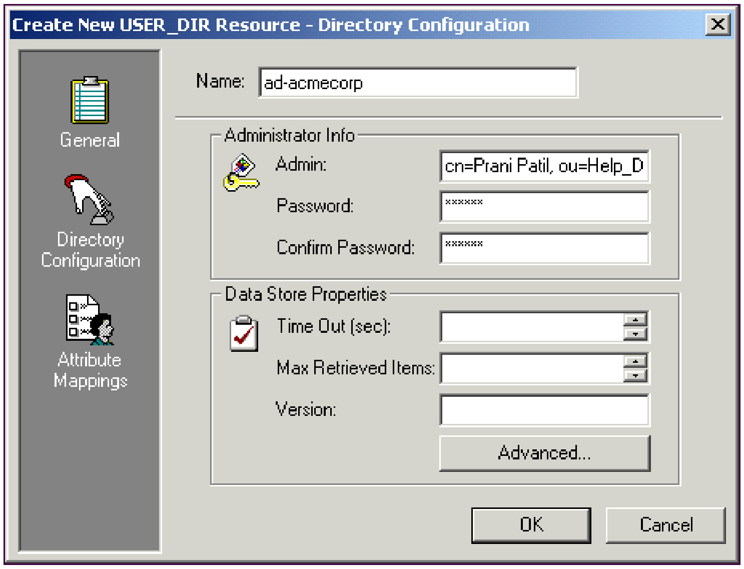
□ SSL Connection

5. Click the Directory Configuration icon on left.

6. Configure the datastore using the following dialog. You should use a permanent user, but they do not need to be an administrator. For example,

   Admin: cn=Prani Patil, ou=Help_Desk, dc=acmecorp, dc=com

   Password: whatever you assigned to this user when creating it.



Create New USER_DIR Resource - Directory Configuration

Name: ad-acmecorp

Administrator Info

Admin: cn=Prani Patil, ou=Help_D

Password: ******

Confirm Password: ******

Data Store Properties

Time Out (sec):

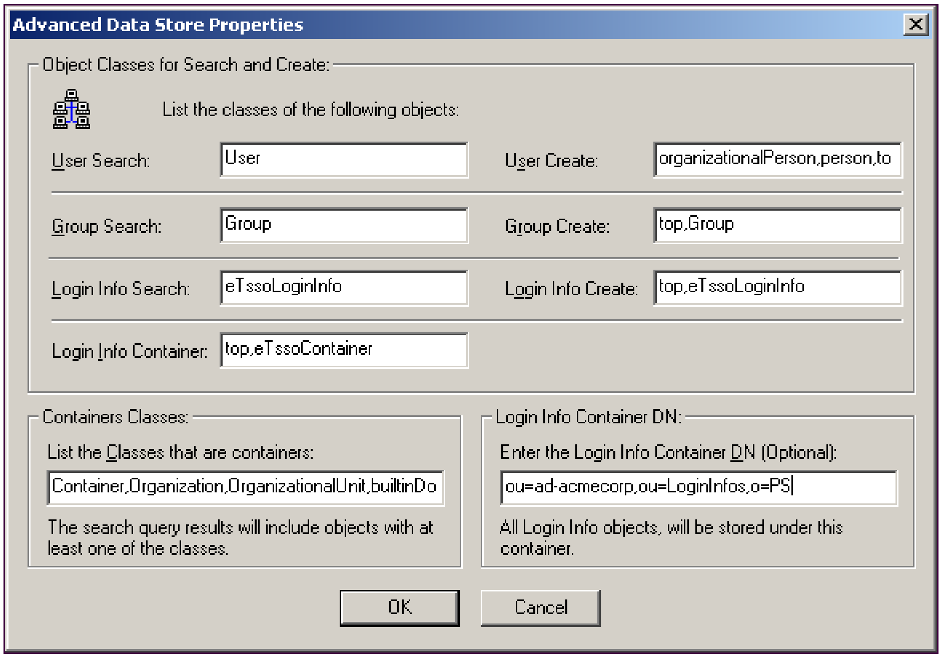
Max Retrieved Items:

Version:

7. Click the Advanced button on lower right.

8. Keep all defaults except modify/add the following:

   Container Classes:
   ```
   container,organization,organizationalUnit,builtinDomain,country
   Login Info Container DN: ou=ad-acmecorp,ou=LoginInfos,o=PS
   ```



Advanced Data Store Properties

Object Classes for Search and Create:

List the classes of the following objects:

User Search: User

User Create: organizationalPerson,person,to

Group Search: Group

Group Create: top,Group

Login Info Search: eTssoLoginInfo

Login Info Create: top,eTssoLoginInfo

Login Info Container: top,eTssoContainer

Containers Classes:

List the Classes that are containers: Container,Organization,OrganizationalUnit,builtinDo

The search query results will include objects with at least one of the classes.

Login Info Container DN:

Enter the Login Info Container DN (Optional): ou=ad-acmecorp,ou=LoginInfos,o=PS

All Login Info objects, will be stored under this container.

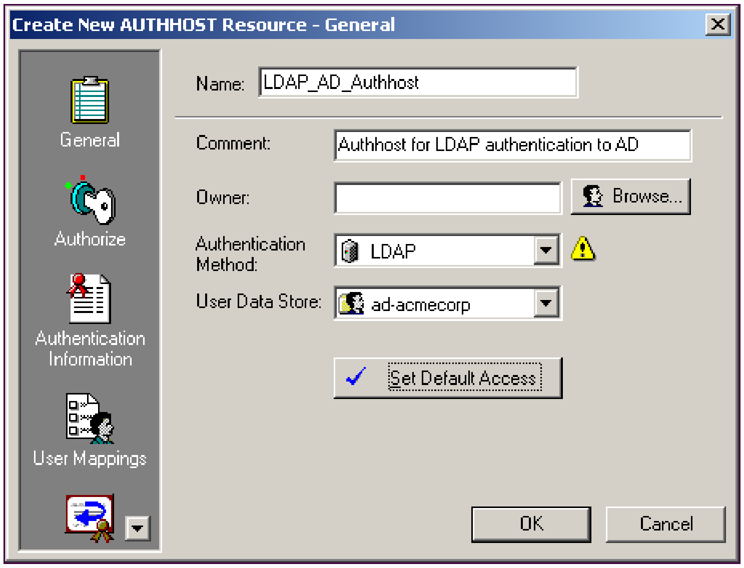
Tip: The Containers Classes field determine which classes the Policy Manager interprets as containers. Any typos will cause problems or some containers may not appear in the user data store when viewed with Policy Manager.

9. Click OK twice to create the user data store.
10. When asked, restart the Policy Server service.
11. Also restart the PS_SVRPOL01 Directory service

Step 5d: Create a New LDAP Authentication Host

You must create a new LDAP authentication host to define which users can use LDAP authentication to this user data store. To create a new authentication host, follow these steps:

1. Go to Resources, Single Sign-On Resources, Configuration Resources, Authentication Host.
2. Right-click in the right pane and select New from the menu.
3. Enter the following in the dialog box:
   - Name: LDAP_AD_Authhost
   - Comment: Authhost for LDAP authentication to AD
   - Owner: [blank]
   - Authentication Method: LDAP
   - User Data Store: ad-acmecorp


Create New AUTHHOST Resource - General

Name: LDAP_AD_Authhost

Comment: Authhost for LDAP authentication to AD

Owner:

Authentication Method: LDAP

User Data Store: ad-acmecorp

You must add users or user groups who can authenticate to Active Directory.

4. Click on the Authorize icon in the left pane.

   The Create New Authhost Resource – Authorize dialog appears.

   a. Click the + button.
   The Add Access Control List Accessor dialog appears.

   b. Select the datastore = ad-acmecorp, select user, select Browse, select All.

   The User Selection dialog appears.

   c. Browse for Philippe Perron in Human Resources, click Add, click OK.

Philippe Perron can now authenticate to LDAP AD.

d. Repeat steps 4a to 4c add Prani Patil (Help Desk) and Penelope Price (Reception).

e. Or add the ssoUsers group.

5. Click on the Authentication Information icon in the left pane

a. Enter the information as shown:

Name: LDAP_AD_Authhost (automatic)

Provider = AD

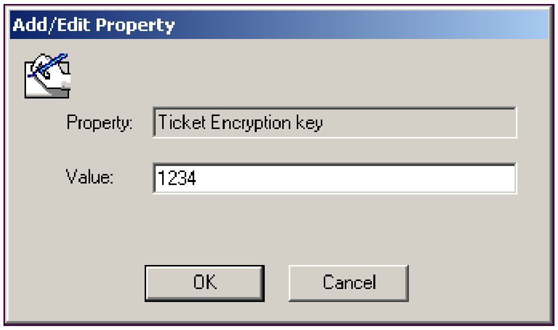
Authentication Data Store = ad-acmecorp

b. Click Advanced Authentication Information

The Advanced Authentication Information dialog appears.

c. Double-click Ticket Encryption Key

The Add/Edit Property dialog appears.



Add/Edit Property

Property: Ticket Encryption key

Value: 1234

d. Enter an Encryption Key value.

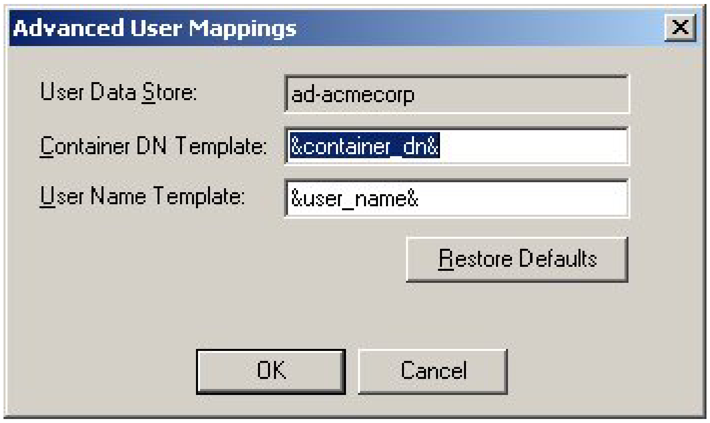
Keep a note of this value. This value must match the encryption key value that you enter when you install the LDAP authentication agent.

The encryption key is used by the auth agents to encrypt the SSO ticket. The Policy Server must have this value to decrypt the SSO ticket during authentication.

6. Click on the User Mappings icon in the left pane

a. Select the Advance User Mappings button.

b. Make sure the user mapping information is the same as the screen below.



Advanced User Mappings

User Data Store: ad-acmecorp

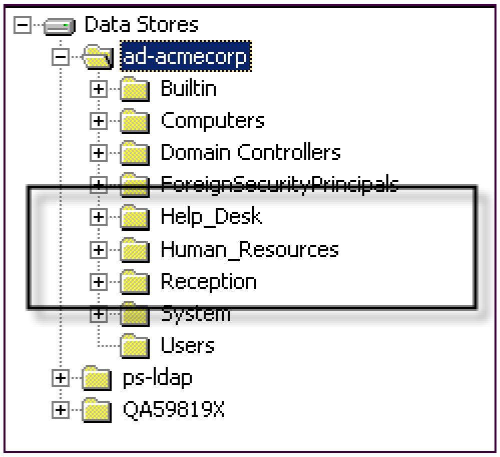
Container DN Template: &container_dn&

User Name Template: &user_name&

8. Click the OK button twice to save your settings.
9. Exit the Policy Manager.

Step 5e: Verify User Data Store Configuration

1. Restart the "eTrust Policy Server 8.0" service.
2. Login to Policy Manager.
3. Go to Users. Expand the "ad-acmecorp" data store and select the Users container. The AD users and groups should be displayed.



4. Select the Human_Resources folder.

   The View or Set User Properties – General dialog appears.

5. Check that Philippe Perron is listed. If you had linked Philippe to a group, you can click the Groups icon in the left pane to see which groups he was linked to.

   Note: The Policy Manager should only be used to view users or read attributes. To create or modify users, you should use the AD tools.

Step 5f: Authorize SSO resources to Active Directory user groups

Various SSO resources need to be linked to the SSO-specific users or groups in AD. This authorizes AD users to access appropriate authentication methods, authentication host groups, application groups, and session profiles.

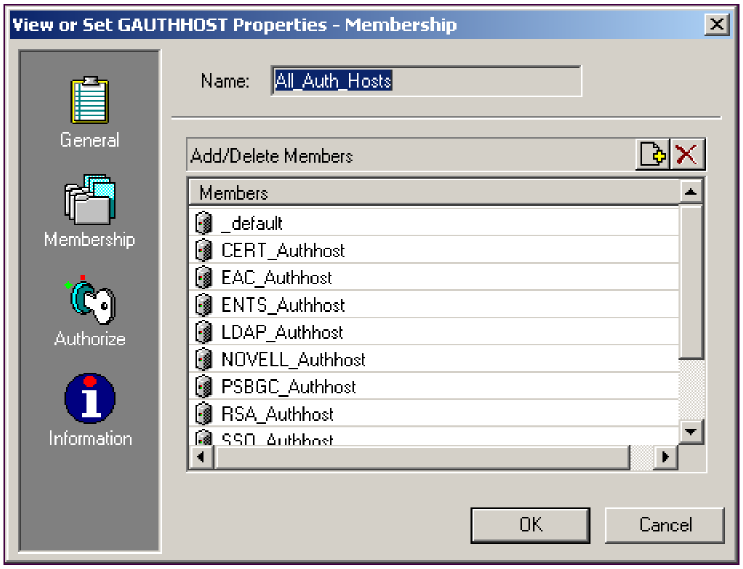
1. Login to Policy Manager.
2. Go to Resources, Single Sign-on Resources, Configuration Resources, Authentication Host Group
3. Right-click in the right pane and select New.

   The Create New GAUTHHOST Resource – General dialog appears.
4. Enter the name All_Auth_Host.

Name: All_Auth_Host

5. Click the Membership icon in the left pane.

   The Create New GAUTHHOST Resource – Membership dialog appears.
6. Add all the existing Auth Hosts, one by one, using the "+" button. You can select multiple hosts at once using either the shift or ctrl key. It works the same way as selecting multiple files in Windows Explorer.



View or Set GAUTHHOST Properties - Membership

Name: All_Auth_Hosts

Add/Delete Members

Members
- _default
- CERT_Authhost
- EAC_Authhost
- ENTS_Authhost
- LDAP_Authhost
- NOVELL_Authhost
- PSBGC_Authhost
- RSA_Authhost
- SSO_Authhost

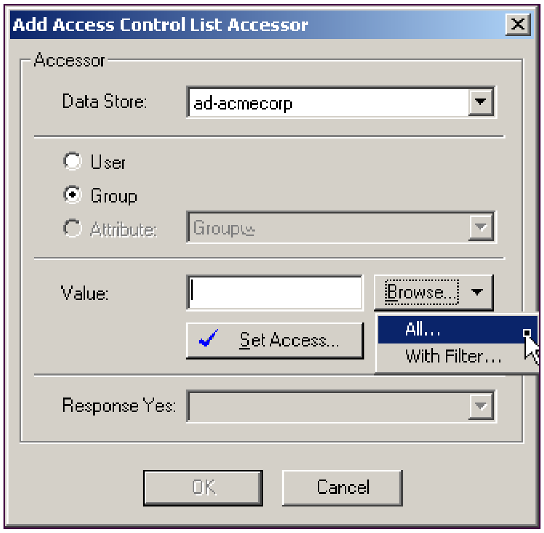
7. Click the Authorize icon in the left pane

   The View or Set GAUTHHOST Properties – Authorize dialog appears.
8. Click the "+" button.

   The Add Access Control List Accessor dialog appears.
9. From the Data Store drop down, select ad-acmecorp

Select the Group radio button

Click Browse, All



Add Access Control List Accessor

Accessor

Data Store: ad-acmecorp

○ User

● Group

○ Attribute: Groupw

Value:

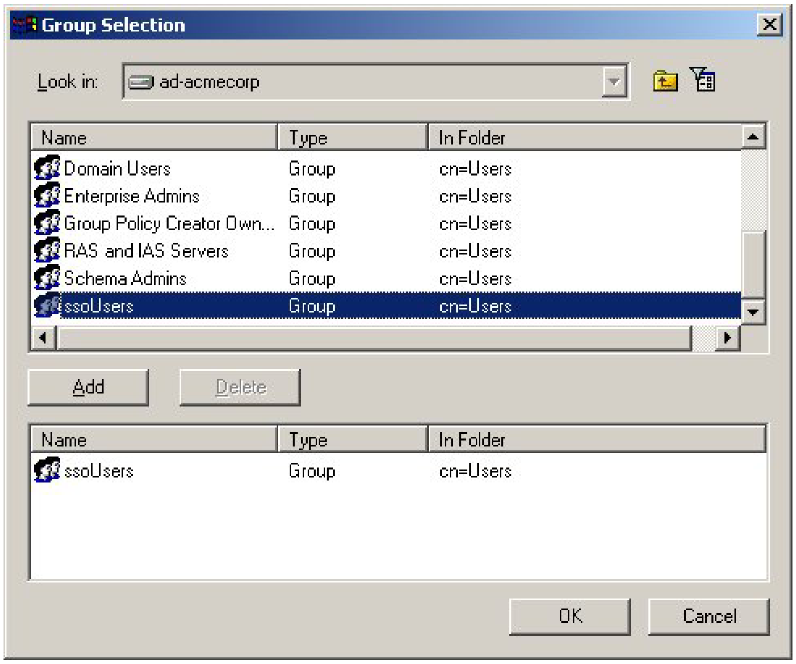
Response Yes:

The Group Selection dialog appears.

10. Select the Users folder.

    All Groups in the Users folder appear in the top pane.

11. Select ssoUsers and click the Add button.



Group Selection

Look in: ad-acmecorp

Name	Type	In Folder
Domain Users	Group	cn=Users
Enterprise Admins	Group	cn=Users
Group Policy Creator Own...	Group	cn=Users
RAS and IAS Servers	Group	cn=Users
Schema Admins	Group	cn=Users
ssoUsers	Group	cn=Users

Name	Type	In Folder
ssoUsers	Group	cn=Users

12. Click OK three times to save.

Step 5g: Apply Resources

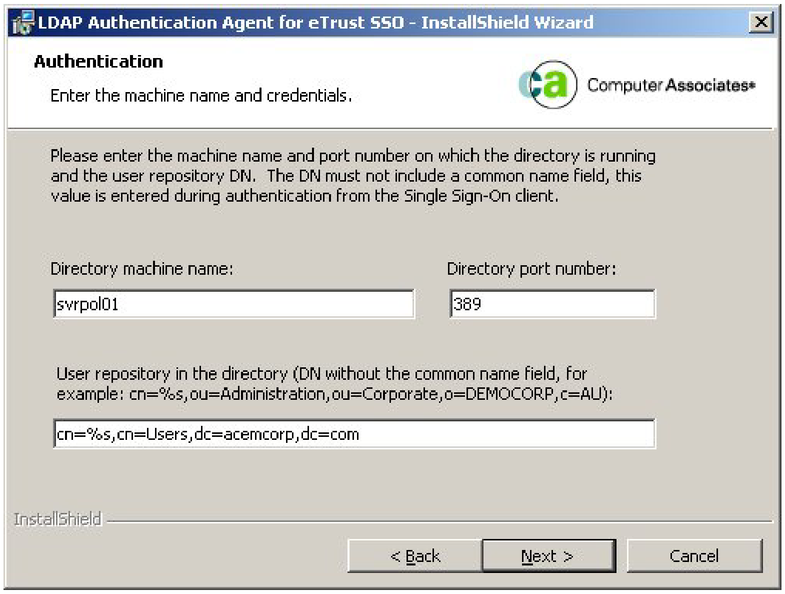
1. Go to Resources , Single Sign-On Resources, Application Resources, Application Group
2. Create an application group
   a. Right-click in the right pane and select New
   b. Enter “Trial Apps” as the Name
   c. Click OK.
3. Similar to Authentication Host Groups, authorize the SSO specific user groups in AD to the appropriate application groups.
4. Go to Resources, Single Sign-On Resources, Configuration Resources, Authentication Method
5. Similar to Authentication Host Groups, authorize the SSO-specific user groups in AD to the appropriate authentication methods. For now, authorize NT and LDAP authentication methods.

> **Tip:** In SSO 6.5, authentication methods were linked within the user record. In SSO 7.0 and 8.0, authentication methods can now be linked to user groups as well. This feature was added since the AD user record doesn’t know anything about authentication methods..

6. Similar to Authentication Host Groups, authorize the SSO-specific user groups in AD to the appropriate Session Profiles. Skip this step if Session Management isn’t going to be used.

Step 6: Install and Configure LDAP Authentication Agent

1. On a different machine from where you've configured Active Directory, commence an installation of eTrust SSO LDAP Authentication Agent.



LDAP Authentication Agent for eTrust SSO - InstallShield Wizard

Authentication

Enter the machine name and credentials.

Please enter the machine name and port number on which the directory is running and the user repository DN. The DN must not include a common name field, this value is entered during authentication from the Single Sign-On client.

Directory machine name: svrpol01

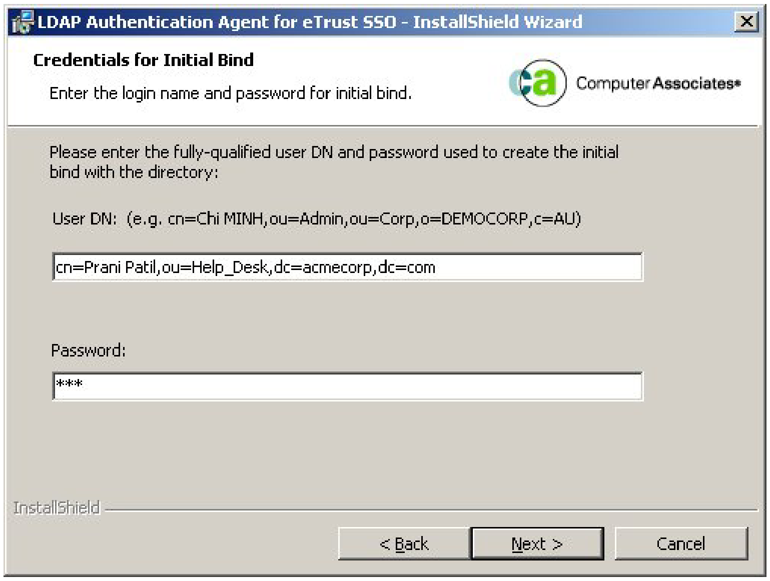
Directory port number: 389

User repository in the directory (DN without the common name field, for example: cn=%s,ou=Administration,ou=Corporate,o=DEMOCORP,c=AU):

cn=%s,cn=Users,dc=acemcorp,dc=com

2. In the 'Authentication' dialog, enter the name of the machine where the Active Directory service was installed, port number on which Active Directory is listening for communication queries (389 is the default), and cn=%s,cn=Users,dc=acmecorp,dc=com in the last field (see screenshot above).

3. In the 'Credentials for Initial Bind' dialog, enter the full distinguished name of the 'Prani Patil' user in Active Directory and the password that you specified.


LDAP Authentication Agent for eTrust SSO - InstallShield Wizard
Computer Associates
InstallShield
< Back
Next >
Cancel

Credentials for Initial Bind

Enter the login name and password for initial bind.

Please enter the fully-qualified user DN and password used to create the initial bind with the directory:

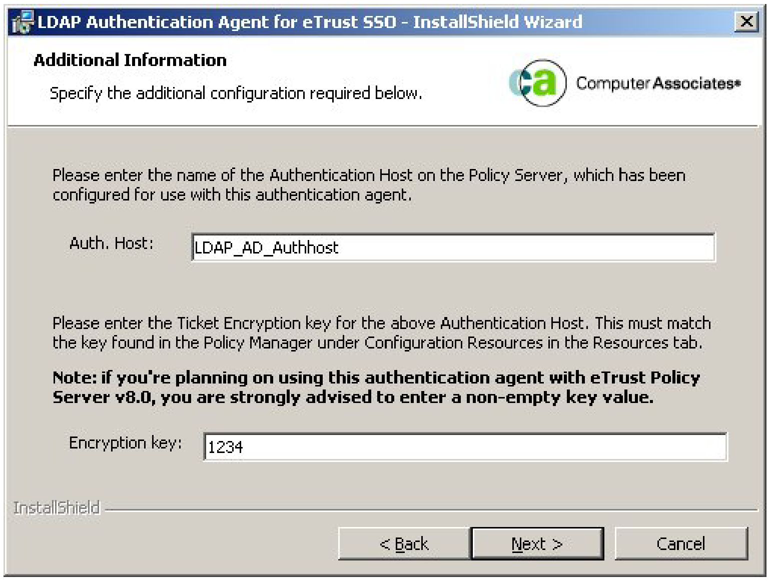
User DN: (e.g. cn=Chi MINH,ou=Admin,ou=Corp,o=DEMOCORP,c=AU)

cn=Prani Patil,ou=Help_Desk,dc=acmecorp,dc=com

Password:

***

4. When prompted in the following dialog, enter value of the Auth Host that was created before. You will also need to enter the key value you want to use to encrypt tickets created by the LDAP Auth Agent.


LDAP Authentication Agent for eTrust SSO - InstallShield Wizard
Computer Associates
InstallShield
< Back
Next >
Cancel

Additional Information

Specify the additional configuration required below.

Please enter the name of the Authentication Host on the Policy Server, which has been configured for use with this authentication agent.

Auth. Host: LDAP_AD_Authhost

Please enter the Ticket Encryption key for the above Authentication Host. This must match the key found in the Policy Manager under Configuration Resources in the Resources tab.

Note: if you're planning on using this authentication agent with eTrust Policy Server v8.0, you are strongly advised to enter a non-empty key value.

Encryption key: 1234

This key value must match the Key field value defined for the LDAP_AD_Authhost Auth Host entry in the Policy Manager.

5. In the post-install completion screen, ensure the ‘Start LDAP Authentication Agent service’ checkbox is checked.

6. Select ‘Start -> Run’, enter ‘regedit’ in the text field and press ‘OK’.

7. Navigate to the following key: HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ sso_tga_ldap_Agent1 \ Parameters \ sso_tga_ldap_Agent1, and set the value of 'AuthMethod' to be 'Bind' (if it is not already set to this value) – using Bind is a requirement for Active Directory, other LDAP repositories may use a value of 'Compare'.

8. Add the following Name Mapping information in the tga_ldapPolicy.ini file

```
[NameMapping0]
BaseDN=ou=Help_Desk,dc=acmecorp,dc=com
Filter=sAMAccountName=%s
Scope=Subtree

[NameMapping1]
BaseDN=ou=Help_Desk,dc=acmecorp,dc=com
Filter=cn=%s
Scope=Subtree

[NameMapping2]
BaseDN=ou=Human_Resources,dc=acmecorp,dc=com
Filter=sAMAccountName=%s
Scope=Subtree


[NameMapping3]
BaseDN=ou=Human_Resources,dc=acmecorp,dc=com
Filter=cn=%s
Scope=Subtree

[NameMapping4]
BaseDN=ou=Reception,dc=acmecorp,dc=com
Filter=sAMAccountName=%s
Scope=Subtree

[NameMapping5]
BaseDN=ou=Reception,dc=acmecorp,dc=com
Filter=cn=%s
Scope=Subtree

[NameMapping6]
StaticName=cn=%s,cn=Users,dc=acmecorp,dc=com
```

9. Select the Services menu item from Start, Settings, Control Panel, Administrative Tools list.

10. From the list of services, select 'eTrust SSO – LDAP Authentication Agent – Agent1', and restart it, either by right-clicking and selecting 'Restart', or by using the ■▶ button from the toolbar.

11. Check the %ProgramFiles%\eTrust SSO\LDAP Agent\LDAPAgent.log file to ensure you do not see any error message. If so, please consult the Troubleshooting section of this document. If not, the LDAPAgent.log file should look something like the following:-

```
#############################################################################
#
# Created Appender on: 02-15-04 22:47:15
#
#############################################################################
2004-02-16 09:47:15 INFO tga_ldap [] - File version: 325,0,0,0
```

```
2004-02-16 09:47:15 INFO tga_ldap [] - Product version: 7,0,0,0
2004-02-16 09:47:15 INFO tga_ldap [] - Build description: Beta Build; Build
date: Fri Jan 23 01:10:28 AUSEDT 2004
2004-02-16 09:47:16 INFO tga_ldap [] - eTrust SSO - LDAP Authentication Agent
- Agent1 is installed.
#############################################################################
#
# Created Appender on: 02-15-04 22:47:25
#
#############################################################################
2004-02-16 09:47:25 INFO tga_ldap [] - File version: 325,0,0,0
2004-02-16 09:47:25 INFO tga_ldap [] - Product version: 7,0,0,0
2004-02-16 09:47:25 INFO tga_ldap [] - Build description: Beta Build; Build
date: Fri Jan 23 01:10:28 AUSEDT 2004
2004-02-16 09:47:25 INFO tga_ldap [] - Using PortNumber 17979
2004-02-16 09:47:25 INFO tga_ldap [] - ChildLimit: 3
2004-02-16 09:47:25 INFO tga_ldap [] - IdleFreq: 20
2004-02-16 09:47:25 INFO tga_ldap [] - TimeOutConnect: 60
2004-02-16 09:47:25 INFO tga_ldap [] - TimeOutRecv: 60
2004-02-16 09:47:25 INFO tga_ldap [] - TimeOutSend: 30
2004-02-16 09:47:25 INFO tga_ldap [] - SendBuffSize: 131072
2004-02-16 09:47:25 INFO tga_ldap [] - RecvBuffSize: 131072
2004-02-16 09:47:25 INFO tga_ldap [] - TicketKey: 1234
2004-02-16 09:47:25 INFO tga_ldap [] - PolicyFilePath: D:\Program
Files\CA\eTrust SSO\LDAP Agent\tga_ldapPolicy.ini
2004-02-16 09:47:25 INFO tga_ldap [] - AuthHostName: LDAP_ps-ldap
2004-02-16 09:47:25 INFO tga_ldap [] - UserNamePrefix:
2004-02-16 09:47:25 INFO tga_ldap [] - UserNameSuffix:
2004-02-16 09:47:25 INFO tga_ldap [] - StandbyConnections: 5
2004-02-16 09:47:25 INFO tga_ldap [] - MaxConnections: 10
2004-02-16 09:47:25 INFO tga_ldap [] - SearchTimeout: 120
2004-02-16 09:47:25 INFO tga_ldap [] - OfflineTimeout: 120
2004-02-16 09:47:25 INFO tga_ldap [] - ConnectionLifetime: 3600
2004-02-16 09:48:51 INFO tga_ldap [] - service_ctrl calling ServiceStop
#############################################################################
#
# Created Appender on: 02-15-04 22:48:52
#
#############################################################################
2004-02-16 09:48:52 INFO tga_ldap [] - File version: 325,0,0,0
2004-02-16 09:48:52 INFO tga_ldap [] - Product version: 7,0,0,0
2004-02-16 09:48:52 INFO tga_ldap [] - Build description: Beta Build; Build
date: Fri Jan 23 01:10:28 AUSEDT 2004
2004-02-16 09:48:52 INFO tga_ldap [] - Using PortNumber 17979
2004-02-16 09:48:52 INFO tga_ldap [] - ChildLimit: 3
2004-02-16 09:48:52 INFO tga_ldap [] - IdleFreq: 20
2004-02-16 09:48:52 INFO tga_ldap [] - TimeOutConnect: 60
2004-02-16 09:48:52 INFO tga_ldap [] - TimeOutRecv: 60
2004-02-16 09:48:52 INFO tga_ldap [] - TimeOutSend: 30
2004-02-16 09:48:52 INFO tga_ldap [] - SendBuffSize: 131072
2004-02-16 09:48:52 INFO tga_ldap [] - RecvBuffSize: 131072
2004-02-16 09:48:52 INFO tga_ldap [] - TicketKey: 1234
2004-02-16 09:48:52 INFO tga_ldap [] - PolicyFilePath: D:\Program
Files\CA\eTrust SSO\LDAP Agent\tga_ldapPolicy.ini
2004-02-16 09:48:52 INFO tga_ldap [] - AuthHostName: LDAP_ps-ldap
2004-02-16 09:48:52 INFO tga_ldap [] - UserNamePrefix:
2004-02-16 09:48:52 INFO tga_ldap [] - UserNameSuffix:
2004-02-16 09:48:52 INFO tga_ldap [] - StandbyConnections: 5
2004-02-16 09:48:52 INFO tga_ldap [] - MaxConnections: 10
2004-02-16 09:48:52 INFO tga_ldap [] - SearchTimeout: 120
2004-02-16 09:48:52 INFO tga_ldap [] - OfflineTimeout: 120
2004-02-16 09:48:52 INFO tga_ldap [] - ConnectionLifetime: 3600
```

Step 7: Install and Configure the SSO Client

This procedure describes how to install the SSO Client using the Product Explorer Wizard. To install the SSO Client component of eTrust SSO using the graphical wizard, follow these steps:

1. Insert the product installation CD into your CD-ROM drive.

   If you have autorun enabled, the Product Explorer automatically displays. Otherwise, navigate to the CD-ROM drive and double-click the PE_i386.EXE file.

2. From the Product Explorer main menu, select Single Sign-On Client 8.0, and click Install.

3. Follow the wizard prompts to:
   - Accept the license agreement
   - Select the Custom Installation
   - Select only the WIN and LDAP Authentication Methods to be installed.

4. On the Configuring Server Set #0 dialog, create a server set using the following information:

Server Set Name:	Scenario 1
Policy Servers:	svr_dom_01
Failover Interval:	30 minutes
Auth Methods:	LDAP
Authentication Hosts:	svr_auth_01

   Note: You must select the Auth Method before you enter the Authentication Hosts for that authentication method.

5. On the second Configuring Server Sets #0 next dialog, select LDAP as the default authentication method.

6. On the Ready to Install the Program dialog, select Add a shortcut to the “eTrust SSO Client” in the Startup folder.

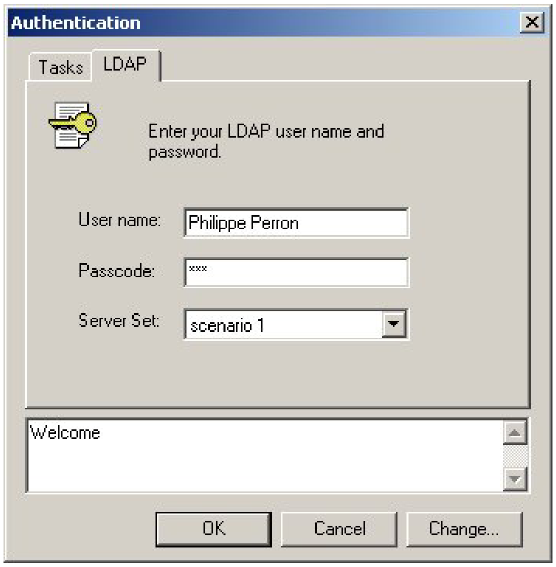
7. Click Install.

Tip: When the message InstallShield Wizard Complete appears, you have successfully installed the SSO Client. Be sure to review the Readme file, and then click Finish to complete the process.

Step 8: Authenticate to Active Directory From the SSO Client

1. Launch the eTrust SSO Client and ensure that the:

   - LDAP tab is selected in the authentication dialog
   - Auth Server pull-down menu contains the entry that matches the name of the computer where the eTrust SSO LDAP Authentication Agent is running.



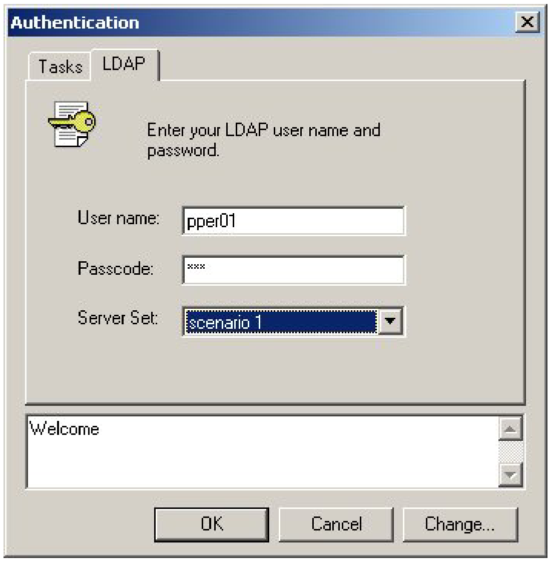
Enter your LDAP user name and password.

User name: Philippe Perron

Passcode: ***

Server Set: scenario 1

Welcome



Enter your LDAP user name and password.

User name: pper01

Passcode: ***

Server Set: scenario 1

Welcome

2. Enter ‘Philippe Perron’ or ‘pper01’ in the user name field and the appropriate password, then click OK.

   The eTrust SSO Client authenticates and logs on to the SSO Policy Server using LDAP authentication.

The SSO Agent icon appears in the tray menu on the bottom right-hand corner of the screen. The user can double-clicked this icon to access their list of SSO-enabled applications. The list will either appear in the SSO Tools view or the SSO Toolbar depending on which mode SSO is defined to run in by the [Toolbar] Enabled property in the SsoClnt.ini file).

Step 9: Create and Test An Application

This section gives you a basic tcl script that can be used to launch an application from the SSO Toolbar.

Step 9a: Create a Logon Script

Here is a logon script that will launch Notepad and enter type out the name of the user currently logged in.

```
sso run -path "notepad.exe"
sso window -titleglob "*Notepad*"
sso type -text "Logged in as user $_USERNAME"
```

Create a file named note.tcl at C:\Program Files\CA\Policy Server\Scripts\ that contains the above example.

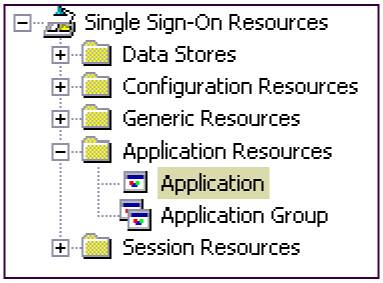
For more information about writing Tcl scripts to log users in and out of applications and documents, see the following documentation:

- *Implementation Guide* "Adding Applications to eTrust SSO"
- *Administrator Guide* "Launching Applications with eTrust SSO"
- *Tcl Scripting Reference Guide*

Step 9b: Define Logon Script to the Policy Server

This procedure tells you how to define a logon script on the Policy Server.

1. Launch the Policy Manager
2. In the Program Bar navigate to Single Sign-On Resources, Application Resources, Application.



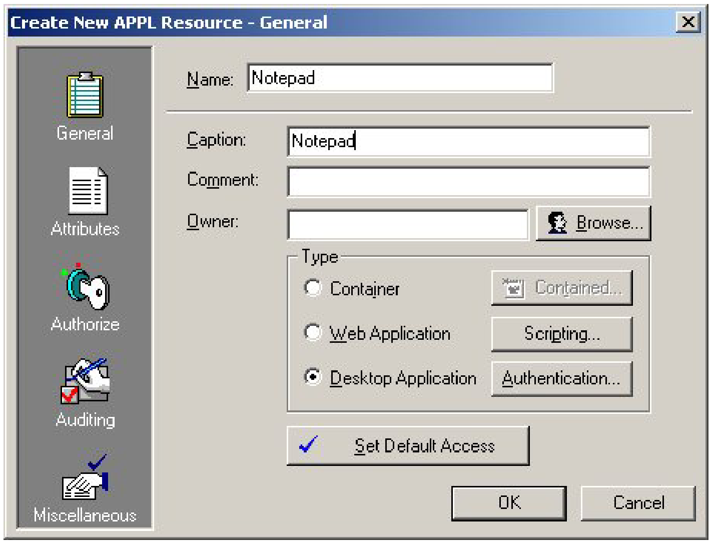
Single Sign-On Resources
- Data Stores
- Configuration Resources
- Generic Resources
- Application Resources
  - Application
  - Application Group
- Session Resources

3. Right-click in the Application Window and choose New.
   The Create New APPL Resource – General dialog appears.
4. Fill in the details of the application.

   For example:

   Name: Notepad
   Caption: Notepad
   Type: Desktop Application

   Note: The caption is what the user sees in their eTrust SSO Application List.



Create New APPL Resource - General

Name: Notepad

Caption: Notepad

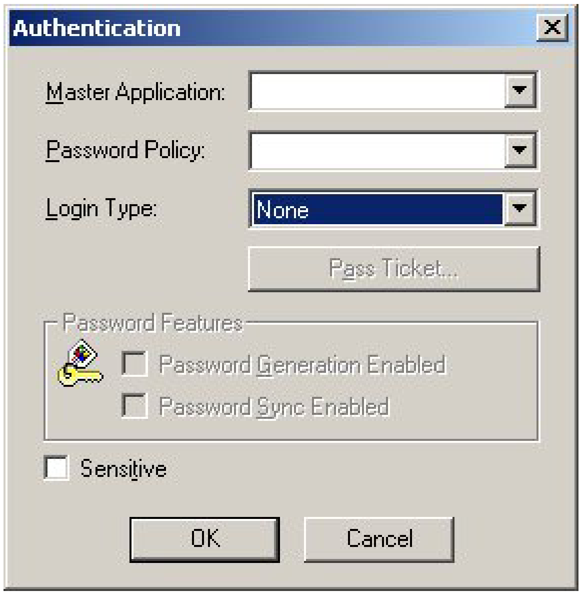
Comment:

Owner:

Type
○ Container
○ Web Application
● Desktop Application

5. Click the Scripting button.
   The Scripting dialog appears.
6. Enter note.tcl in the Script File field, and then click OK.

   Select the Authentication button and set the Login Type to None.



Master Application:

Password Policy:

Login Type: None

☐ Password Generation Enabled

☐ Password Sync Enabled

☐ Sensitive

7. Select the Authorize icon.
   The Create New APPL Recourse – Authorize dialog appears.
8. Right-click and choose Add.
   The Add Access Control List Accessor dialog appears.
9. Add the ssoUsers group to the authorized list.

Step 9c: Launch the Application

This procedure tells you how to test the script. This is the procedure that end-users would follow.

1. Using the Philippe Perron user, logon and authenticate to SSO.
   This means that you will have a current SSO ticket.
2. Choose the Notepad application from the list of SSO-enabled applications.

Chapter

3

Implementation Overview

This chapter gives you a step by step overview of what order to deploy the eTrust Single Sign-On (eTrust SSO) components in your organization.

Implementation Of Components

In many cases, the most efficient implementation strategy will be a sequential process. Here are the suggested implementation steps in order of components.

Step 1. Install the eTrust IAM Common Components

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

Step 2. Install the Policy Manager (administrator workstations)

Step 3. Populate the Data Stores

Step 4. Install the authentication agent(s)

Step 5. Write the logon scripts (and other scripts)

Step 6. Install the SSO Client (end-user workstations)

Step 7. Install the Session Administrator (optional)

Step 8. Install the Password Sync Agent (optional)

Step 9. Install the One Time Password (OTP) Agent (optional)

Tip: You may want to start development on **Step 5. Write the Logon Scripts** early, in parallel with the other steps, to make sure they ready in good time.

After each installation and configuration step, we strongly recommend that you verify that the component added is working as expected. For example, after performing step 3, use the Policy Manager to perform an ad-hoc verification that User and Application data is assigned as expected.

Note: All operating system clocks must produce a reliable and correct timestamp for the time-zone where each machine hosting any SSO components are located. For example, a machine located in New York hosting a Policy Server must have it's OS clock set to US Eastern Daylight Time (EDT) whilst a machine located in San Francisco hosting a LDAP Auth Agent must have it's OS clock set to US Pacific Daylight Time (PDT).

Step 1. Install the eTrust IAM Common Components

eTrust Identity and Access Management (eTrust IAM) is a suite of products and services that enforce secure access to information assets and facilitate management of those assets. eTrust IAM's web-enabled interface (IA Manager) lets administrators quickly and comprehensively establish and maintain access privileges to computers, services, and applications across the enterprise.

eTrust IAM consists of a core set of common components that support a suite of specialized identity and access management products. The common components provide a backbone of identity and access management functionality. As you identify additional specific access control needs, you can select and integrate products from the eTrust IAM suite to meet those needs.

eTrust IAM Product Suite

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

The *e*Trust 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 *e*Trust 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.

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.

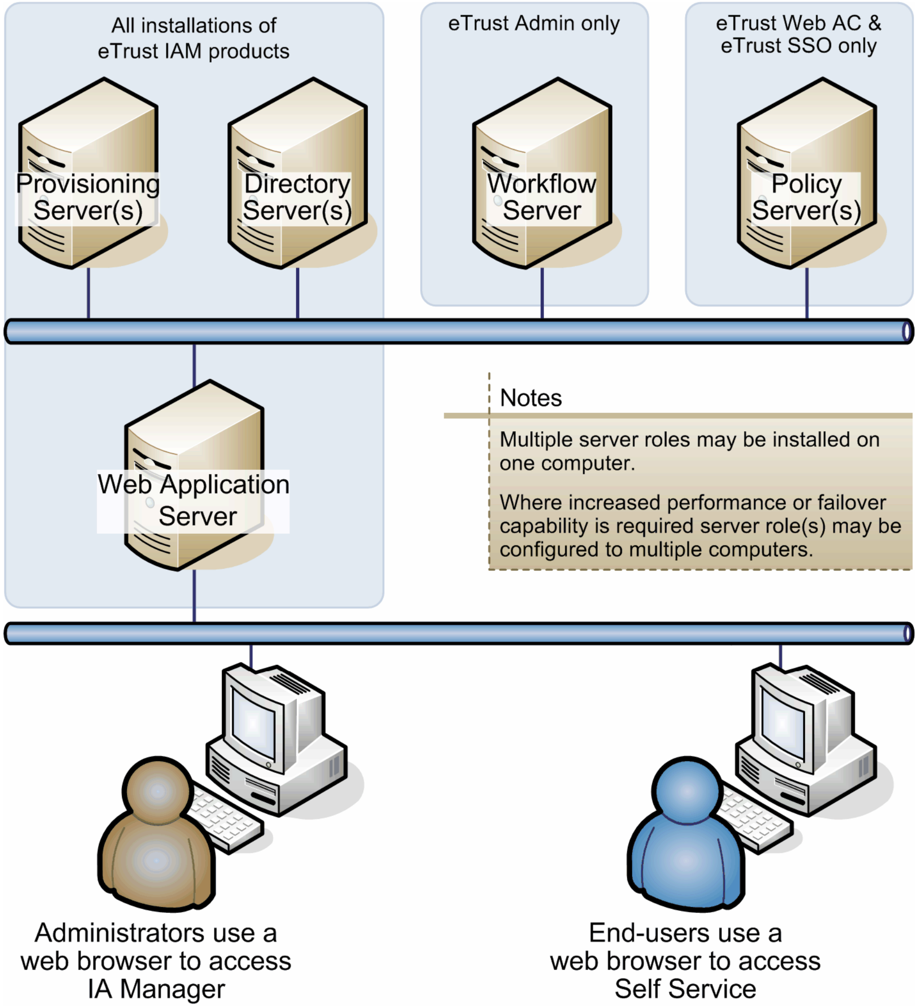
Workflow Server
Provides business process management services for establishing and tracking business processes.

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

Computer Role	Required for Point Product	Scalability	Installed Components
Directory Server	Admin, Web AC, SSO, AC	Fully scalable for failover and load sharing	eTrust Directory Advantage Ingres JRE for JXPlorer
Policy Server	Web AC, SSO	Scalable for load sharing	Policy Server eTrust AC eTrust Directory Advantage Ingres
Provisioning Server	Admin, Web AC, SSO, AC	Scalable for load sharing	Provisioning Server + Options eTrust Directory
Web Application Server	Admin, Web AC, SSO, AC	Single computer	Apache Tomcat JDK IA Manager IAM Configuration IAM Self Service IAM SPML Service
Workflow Server	Admin (optional component)	Single Windows computer	Admin Object API Apache Tomcat JDK Advanced Workflow

Where:

- eTrust Access Control = AC
- eTrust Admin = Admin
- eTrust Single Sign On = SSO
- eTrust Web Access Control = Web AC


All installations of eTrust IAM products
eTrust Admin only
eTrust Web AC & eTrust SSO only
Provisioning Server(s)
Directory Server(s)
Workflow Server
Policy Server(s)
Web Application Server
Notes
Multiple server roles may be installed on one computer.
Where increased performance or failover capability is required server role(s) may be configured to multiple computers.
Administrators use a web browser to access IA Manager
End-users use a web browser to access Self Service

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 *e*Trust SSO or the Admin Manager for *e*Trust 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.

Step 2. Install the Policy Manager

The Policy Manager is a Windows GUI for managing 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.

You should install the Policy Manager on all computers that your administrators' use to control the Policy Server. Once you have installed the Policy Manager on an initial machine, you must set access rights for any other machines that will be authorized to access the Policy Manager. For more information about setting up the Policy Manager for administrators for the first time, see the "Basic Tasks in eTrust SSO" chapter of the *eTrust Getting Started* guide.

Step 3. Populate the Data Stores

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.

You should use the eTrust Directory data store for storing user information and the eTrust Access Control database to store all other information relating to resources, applications, and administrators.

You should plan how to populate the data stores. The eTrust SSO database includes the following entities:

- Users (USER records) or eTrust Directory entries (typically iNetOrgPerson)
- User groups (GROUP records) or eTrust Directory entries (typically eTrust SSOGroup)
- Applications (APPL records)
- Application groups (GAPPL records)
- Authentication hosts (AUTHHOST records)
- Authentication host groups (GAUTHHOST records)

- Password policies (PWPOLICY records)
- Terminals (TERMINAL records), which are the computers that will be used to administer eTrust SSO.

You can populate these data stores in two ways. If you are importing a large amount of data to either of these data stores, you might want to use a Command Line command, such as a selang script to import data into the eTrust Access Control data store or a Directory utility, such as Jxplorer to import data into the eTrust Directory data store. Selang is a CA-proprietary security language that can be used to control the eTrust Access Control data base. If you are just entering small amount of information you might use the Policy Manager.

Based on the implementation decisions, the implementation team should define these entities and the relations among them, together with the associated access rules.

eTrust Directory (LDAP Data Store)

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

You should use eTrust Directory, or another third-party LDAP directory, to store:

- Users
- User groups
- Logon information

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.

You must use the eTrust Access Control data store for all information that does not relate to users, user groups and logon information.

eTrust Access Control (Data Store)

eTrust SSO comes with eTrust Access Control. The eTrust Access Control is a database that stores all information about:

- Resources
- Applications
- Access control rules

- Administrators

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.

Step 4. Install the Authentication Agents

If third-party software is to be used for either primary authentication (the user identifying them self to the SSO system) or application authentication (the method of identifying the user to the application they wish to access), it must be already installed at the site before eTrust SSO primary authentication agents are installed, however, each primary authentication agent will define their own installation requirements that you must follow. For further information about installing Authentication Agents, see the "Implementing Authentication Agents" chapter of this guide. Your CA representative can help you with your specific application requirements.

eTrust SSO primary authentication agents are installed on an Authentication Host. This is typically on the computer where the third-party authentication server is installed.

Authentication hosts have to be defined in the Policy Servers in order to grant users the authority to log into eTrust SSO having passed primary authentication on the authentication host.

Step 5. Write Logon 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.

Application logon scripts should be written in the order planned and then tested. You may also need to use JavaScript to launch Web applications using eTrust SSO. For more information about launching Web applications see the Launching Web Applications section in the “Common eTrust Processes” chapter in this guide.

Tip: For a detailed explanation of how to write eTrust SSO logon scripts, see the guide called *eTrust SSO Scripting Reference guide*

Step 6. Install the SSO Client

The eTrust SSO Client is installed on every end-user workstation. The only exception to this, is some thin-client environments, where eTrust SSO is only used to facilitate web access.

You can install the SSO Client on each user's computer using the eTrust SSO product explorer wizard from the eTrust SSO CD, which is very straightforward, but also time consuming if you have to roll the SSO Client out to large numbers of users. Alternatively you can roll the SSO Client out to a large number of end users machines on a network using appropriate software.

The SSO Client can be configured to work in a number of different ways. The SSO Client behavior is controlled by the SsoClnt.ini file. You must install the SSO Client at least once, using the product explorer wizard to get a copy of the SsoClnt.ini file. You can then customize this INI file and distribute it so that when you roll it the SSO Client to a large number of users, using the silent installation, the SSO Client is already customized.

You should plan what functionality you want from the SSO Client and what you want your users to experience from the eTrust SSO system. Decisions you need to make, include:

- What method of authentication are you planning to implement.
- How you want users to access the SSO system and SSO-supported applications
- Whether you want shared workstation functionality
- Whether you want application migration (Citrix Metaframe environments only)

Users can access the their SSO applications in a number of different ways including: as menu items in a Windows Program Group, as icons on the desktop, or using the SSO Toolbar.

You also need to plan how you are going to install the SSO Client on end-user computers. Are you going to install it on individual computers using the installation wizard or are you going to do a silent installation on a large scale using a software distribution tool?

For more information about customizing the SSO Client, see the "Working with the SSO Client" chapter in this guide.

For a complete list of all SsoClnt.ini settings, see the "Configuring the SSO Client: SsoClnt.ini" appendix in this guide.

For more information about silent installation of the SSO Client, see the "Installing the SSO Client" chapter in the *Implementation Guide*.

Step 7. Install the Session Administrator (Optional)

The Session Administrator is a web-based application that lets you view and terminate eTrust SSO sessions. In addition to storing automatic session profiles on the Policy Server, you can also manually track and terminate sessions using the Session Administrator. The Session Administrator is a web-based tool that lets you:

- View and terminate users' sessions
- Check how long a session runs
- Check what computers a session is running on

The Session Administrator can be installed on any Windows computer on the network. It may be installed on the same computer as any other eTrust SSO component.

The computer on which you install the Session Administrator is referred to as the Session Administrator Server.

Step 8. Install the Password Synchronization Agent (Optional)

eTrust SSO provides you with a Password Synchronization Agent for both Windows and mainframe platforms. The Password Synchronization Agent keeps passwords synchronized between external systems and the Policy Server. When a user changes their domain password, for example, that change is detected by the Password Synchronization Agent and the new password is updated on the Policy Server.

The Password Synchronization Agent for Windows must be installed on a domain controller (DC) to enable password policy and password synchronization for Windows domain users. The Password Synchronization Agent for Windows and the Policy Server must communicate with each other. Therefore, TCP/IP software must be installed on the DC.

The Password Synchronization Agent for mainframe ensures password are synchronized from the mainframe via and DC, to the Policy Server.

Step 9. Install the One Time Password (OTP) Agent (Optional)

eTrust SSO comes with a built-in one-time password (OTP) agent for UNIX platforms only. The OTP authentication type can eliminate the security risk of sending passwords across a network in clear text. With OTP, passwords are still sent across the network, but they cannot be used to log on a second time, so they are useless to whoever intercepts them.

Once the OTP agent detects that a password has been used, it generates a new password and sends this to be stored on the Policy Server.

The OTP agent is installed on a UNIX computer that hosts SSO-supported applications.

Chapter

4

Planning The eTrust SSO Implementation

This guide will help you install the eTrust Single Sign-On (eTrust SSO) system. This chapter is designed to get you thinking about what Project Planning you need to do to help you implement eTrust SSO. For more information about the steps involved with the implementation, see “Component Installation Overview” in this guide.

The Implementation Teams

As with any other implementation project, the success of the eTrust SSO installation at your site will depend very much on human factors: the skills and performance of the implementation team and the cooperation of the end users.

Before any serious deployment of new technology can begin, it is imperative that you assemble the proper implementation teams to facilitate the rollout of eTrust SSO within the business. Although you may have the actual vendor or a contractor run the project for your company, you should always understand the implementation and have an internal team assigned to work with the deployment vendor.

We recommend that you have two implementation teams, one for the technical deployment of eTrust SSO, and the other for the rollout within the business.

The Technical Implementation Team

For best results the implementation team should include:

- A project manager
- A security administrator
- An application administrator
- A password administrator
- Script developers
- A technical support person (for software installation)
- An eTrust SSO administrator for day-to-day administration.

Responsibilities of the Technical Implementation Team

The implementation team is responsible for:

- Defining eTrust SSO security objectives
- Mapping and documenting the computing environment, including users and applications
- Preparing the implementation plan, which includes defining the eTrust SSO database
- Installing and configuring servers and clients
- Defining security rules: primary authentication and application authentication
- Populating the eTrust SSO database
- Preparing logon scripts
- Testing the implementation
- Training end users to use the eTrust SSO Client

Preparing The Technical Implementation Team

All team members: All members should review eTrust SSO manuals, both the introductory chapters and the specific issues with which they will deal. They should also refresh their knowledge of the relevant aspects of the site's hardware and software.

Technical support personnel: Staff who will install eTrust SSO need to be familiar with migration considerations and with the steps required to install eTrust SSO. Users who maintain the SSO databases must be familiar with the material in *eTrust SSO Selang Command Reference Guide*. Knowledge of eTrust Access Control utilities is also advisable (see *eTrust Access Control / Utilities*).

Script developers: The staff responsible for writing logon scripts for eTrust SSO should become familiar with *eTrust SSO Tcl Scripting Reference Guide* and should begin writing practice scripts as soon as possible.

The Business Implementation Team

The following sections explain how to identify the members of your business implementation team and define their roles and responsibilities.

You business implementation team should include representatives from each of the following affected areas:

- Security administration
- Systems software
- Applications software
- Operations
- Auditors
- End users

Cooperation is Essential

It is important to note that a security implementation forces cooperation between corporate areas that may never have been forced to work together before. This cooperation, critical to the successful implementation of a security product, provides another reason why you need a clearly defined management commitment to the security implementation.

Responsibilities of the Business Implementation Team

Regardless of organizational responsibilities, the following roles should be considered and assigned to specific members of the implementation team:

Project Manager—Owns the overall project management tasks, deliverables, communications, and timetables.

Security Administrator—Responsible for the review and approval of design, architecture, and naming standards as they pertain to user IDs and resources. This team member is also responsible for the formation and distribution of audit reports. After the implementation is complete, the security administrator is responsible for the enforcement of the security policies and procedures established for eTrust SSO.

Operations Representative—Responsible for the day-to-day operation of eTrust SSO in terms of the hardware, software, and procedures required to maintain the service levels agreed on. The Operations group is also responsible for disaster recovery, business continuum, failover, and backups.

Network and Systems Representative—Responsible for maintaining the connectivity of the environment in which eTrust SSO runs. Since there are several components of eTrust SSO that can reside in multiple systems across the network, it is important to include these groups in the design and architecture phase of the implementation. During this implementation phase of eTrust SSO, you need to consider firewalls, protocols, DMZ, operating systems, authentication server, servers, and so on.

End User Liaison—A business person who represents the end user experience when it comes to interface decisions or user awareness issues. This person should have full voting rights when deciding what the user sees and what procedures get implemented that will directly affect the experience of an end user.

Business Representative—Responsible for the policies that will affect the end user's experience with certain business applications.

Management—The success of any project is the constant involvement and approval of senior management at every step of the way. This team member should be in a high enough position in the organizational structure to have jurisdiction over all the parties involved in the deployment of this technology.

Preparing the Business Implementation Team

All team members should be given a demonstration of eTrust SSO and should be familiar with the basic benefits of installing eTrust SSO. Stakeholders should also be reassured, where necessary, about the minimal impact on end-users. Members of this team should be encouraged to read the eTrust SSO Getting Started.

Objectives

Defining Project Objectives

To begin implementation, you must first define what you want eTrust SSO to do for your system. For instance, what is your primary aim: To increase the security of your data processing installation and data? Or, is it to simplify the work environment of your end users? The answers to these types of questions help define your objectives and aid in forming policy guidelines and priorities for eTrust SSO implementation and operations.

Formulating a Security Policy

eTrust SSO provides a solution for security and productivity problems that result from users having to work with many different passwords. Like any security solution, eTrust SSO will be most effective when it is integrated into a well-defined and comprehensive system security plan.

eTrust SSO implementation should conform to system security requirements regarding overall system security policies, password policies (either present policies or new, stronger policies that can take advantage of eTrust SSO features), physical protection of servers and backup servers, and auditing. In addition, general system requirements regarding response time and survivability should be considered when planning the number, location, and general configuration of Policy Servers and backup servers.

The initial assignment of the security implementation project team may be to develop and recommend the security policy or the document of security objectives for your environment. You may be able to use or borrow concepts from the established policies within your company with the same generic security requirements, such as authentication and authorization.

If the security policy or the document of security objectives has already been developed, the implementation team can use this document as its mandate. If these documents must be developed, the team is an ideal committee to do it since they can take into account the concerns of each affected area while developing the objectives. If each area agrees to the direction being set, which is more likely with active participation, then implementation can proceed smoothly without time-consuming discord among the business areas.

After the security policy has been formulated, upper management should issue a position statement to all internal employees and appoint a security officer (or at least a security administrator). The security officer can then ensure that employees are made aware of the security policies and procedures that they must adhere to and the consequences of any security violation.

Implementation Overview

Overview of implementation

You should always install the test a new system in a controlled environment. Here are the suggested steps involved with the eTrust SSO implementation.

- Plan the implementation
- Implement a Test bed installation
- Conduct a Pilot Test
- Prepare the Installation Area
- Deploy eTrust SSO
- Conduct End User training

Plan the Implementation

Although eTrust SSO installation is straightforward and flexible, it is affected by, and affects, much of the site's system. You need an implementation plan in order to schedule and control the properly paced introduction of eTrust SSO into the nodes of the network and into the procedures of the workplace. For efficiency, the plan has to provide step-by-step procedures, guidelines, and timetables.

The Initial Planning Session

An initial planning session should be convened to define the eTrust SSO configuration. All the relevant servers and clients should be identified, together with the users and the applications to be secured. Relationships between applications and users have to be mapped.

Once decisions have been made on configuration, the team has to detail each of the stages of implementation.

The plan should also take into consideration any other significant events, such as installation of new hardware or software, that is planned for the same period and that could affect implementation.

It is also advisable to define a pilot group that will have eTrust SSO installed first. A pilot group can provide valuable initial experience that can prevent problems in the full-scale implementation. You should make a decision about the size and location of the pilot group and the applications that you will include in the pilot study.

Once the implementation plan is finalized, the team should prepare a project schedule for the pilot and final implementation.

In a large computer system, it will probably not be practical to implement eTrust SSO for all applications and for all users in one stage. An advantage of eTrust SSO is that it allows for phased implementation, staggered by groups of users and/or groups of applications. The implementation team has to set priorities for adding user groups and application groups.

Project Management

Implementing eTrust SSO is a major project. As with any major endeavor, you need to follow good project management guidelines to ensure a successful implementation.

In addition to creating an implementation team, you need to:

- Hold regular meetings
- Establish an archive of all pertinent documentation relating to this project
- Review your corporation's security policies and procedures

Collect Data

Before a detailed plan can be formulated, the implementation team will have to collect considerable relevant information. The team has to map and document the computing environment, in particular those elements that directly affect eTrust SSO implementation.

It is essential that the data about system configuration, operating systems, applications, and authentication methods be detailed and up to date.

It is advisable to use a form or checklist to collect information in a systematic way.

Here is a list of the information that you will need to obtain. The scope and detail of initial database planning will depend on the scope of the final implementation project itself. It is important to define the entities shown in the following table.

Entity	Definitions must include
All the applications to be accessible using SSO	- Application name/identifier - Application host - Authentication method - The application group to which the application belongs, if any
All the application groups (if application groups are planned)	- Application group name - Application names/identifiers of the application that are to be linked to the application group
All the authentication hosts that will be used by eTrust SSO	- Authentication method - Authentication host names - The authentication host group to which the authentication host belongs, if any
All the authentication host groups (if authentication host groups are planned)	- Authentication host group name - Authentication host names of the authentication hosts that are to be linked to the authentication host group
User groups planned	- User group name - The names of users in the group - Application groups associated with the user group

Implement a Test Bed Installation

Before you move into the Pilot Testing Phase, you should install and configure the eTrust SSO system within a Test Bed environment, to make sure all the components are configured correctly. This step will facilitate the smooth introduction of eTrust SSO to users within your company and help with user-acceptance, as well as assisting the implementation from a technical perspective.

Conduct a Pilot Test

In large systems, installation of the SSO Clients on end-user workstations will generally begin with a pilot group.

When a pilot test is to be run, SSO Clients will first be installed on the pilot group's workstations. The implementation team has to work closely with the pilot group for testing and for obtaining end user feedback. It is important to prepare testing procedures and worksheets for recording results.

Every user has to be authorized to use the specific method of authentication. Generally, we recommend that you set the user's AuthMethod token value to SSO when first implementing eTrust SSO. This will enable you to test the validity of the records in the USER and APPL classes, without being affected by any problems in primary authentication installation.

However, once in production, the token must be set to its planned value. For example, to enable an end user to use Windows authentication, change the value of the AuthSSO token in the ServerSet section of the SsoClnt.ini file to Windows NT. If the Windows authentication agent is not installed on the primary domain controller, then change the value of the AuthNT token in the ServerSet section to be the actual name of the Windows authentication host, in uppercase letters.

Prepare the Installation Area

Before you begin the eTrust SSO installation, you should review and prepare the intended site. This stage, which can also be referred to as a walk-through, involves the implementation team arriving on site to review the equipment and facilities for the subsequent stages. Successful completion of this stage should be viewed as a prerequisite to continuing the implementation.

The site staff should provide information about the hardware and software on the site. The implementation team should check technical details of servers, end-user workstations, and primary authentication systems against the preliminary data already received and analyzed.

The team should look for potential obstacles and problems. Hardware and software prerequisites should be checked, including:

- All client workstations must have with the network and TCP/IP configured
- Each SSO component (clients, servers, authentication hosts) should be able to ping its peer by name
- If you are using Windows authentication, SSO users should have a domain account and logon rights
- If you are using UNIX hosts for the Policy Server they should have a supported OS version (AIX, HP-UX, Solaris) installed and sufficient disk space
- Any third-party authentication software to be used (for example, RSA SecurID), should be properly installed and configured

Deploy eTrust SSO

In the production phase, the eTrust SSO Client software is installed on all the end-user workstations group by group (either by geographical groups or by business function groupings). If there is no pilot testing phase, it may be advisable to check the work of the previous stages by installing the SSO Client on one or two workstations in each user group.

During each phase, auditing data and user feedback are collected and analyzed. This allows management to evaluate the success of the implementation and indicates what adjustments have to be made.

During this stage, the implementation team will begin transferring responsibility for routine administration of eTrust SSO to the site’s IT organization.

Conduct End User Training

In itself, eTrust SSO implementation will require only minimal end-user training.

Prior to implementation, end users should be told that changes in the network will automate their logging into password-protected applications. They need to be informed on how the specific implementation on the site will affect them in regard to system logon, first-time eTrust SSO logon, routine logon to applications, logon to sensitive applications, station lock release, re-authentication, and password change.

End users should also be informed that where they will still be asked for passwords (such as for sensitive applications and password changes), they will need only their user ID, a primary authentication password, and, where applicable, an additional biometrics or token authentication. In addition, end users should be informed that when they log onto applications for the first time using SSO, they might be required to provide their application password to the Policy Server.

Following installation of eTrust SSO Clients, end users will have to be told where they will find eTrust SSO's application list and the various ways of selecting applications.

If eTrust SSO is implemented together with new third-party authentication, new password rules and/or other security policies, then end users will have to be educated on these topics.

Chapter

5

Implementing the eTrust IAM Common Components

The following sections describe how to install the IAM Common Components, including, pre-installation considerations, methods of installation, and installation procedures.

Before You Begin

Before you install any eTrust IAM product, you must install the eTrust IAM Common Components.

The eTrust IAM Common Components Installer coordinates the installation of the eTrust IAM Common Components across multiple computers. During installation on the first computer, the configuration information is collected and stored in a networked data store. This configuration information is used in installations on additional computers to streamline the process.

Each computer included in the installation accesses the configuration information created on the first computer where the software is installed and also requires additional local configuration information.

After installing the eTrust IAM Common Components, you will need to additionally install the software components specific to the point product you purchased. These components can be installed from your eTrust product CD.

Plan Your Installation

A typical installation of the eTrust IAM suite may involve multiple servers being accessed by computers distributed across the organization. The configuration of the servers is crucial to obtaining optimal performance from your installation. Elements that must be taken into account when planning the software configuration for your unique needs are:

- The eTrust IAM software products you are planning to use.
- Network structure, bandwidth and traffic between individual servers.
- Location of client computers and the volume and types of network activities generated by these clients.
- Hardware specifications and workloads on available servers.
- Operating systems installed on available servers.

These factors will influence the optimal IAM architecture and best location for the computer roles you want to assign.

For more information about structuring your Policy Server farm see the:

- "Working with Server Farms" chapter of the *Administrator Guide*.

During the installation you will be able to select a custom or express install. If you choose an express install, all required IAM common components will be installed and configured to the current computer. Installation of the common components to additional computers is not available when using the Express install option.

Note: Installation of this software on multiple machines cannot be run concurrently. Installation must be successfully completed on each computer before moving to the next computer.

Notes on Possible Architectures

This section lists some points to keep in mind when choosing the architecture of your eTrust IAM product suite.

- The Provisioning Server role can be shared across multiple computers. If you have purchased eTrust Admin and have a very large and/or distributed user base, you may wish to configure multiple computers to this role. For more details about the Provisioning Sever, see the eTrust Admin *Implementation Guide*
- The Policy Server role can be configured as a server farm installed across multiple computers. If you have purchased eTrust SSO, you plan to install a Policy Server Farm those computers must all run the same operating system. See the IAM Readme for the operating systems supported by the Policy Server. See the “Working with Server Farms” chapter of the *Administrator Guide.*
- The Directory Server role will be installed on every computer performing the Provisioning Server or Policy Server roles. There is no performance benefit in installing the Directory Server to additional computers.
- The Web Applications and Workflow Server roles should not be installed on computers already running as web servers due to potential port conflicts. These roles can be installed onto the same computer.

Upgrading an Existing eTrust Product

Upgrades of existing SSO Server 6.5, or Policy Server 2.0 (SSO 7.0) computers are supported by the IAM Common Components installer. When running the install, assign the Policy Server role to the computers running these earlier versions of the software to upgrade the Policy Server. Some settings will revert to their default values so if there is special configuration (DXlink for example), this will need to be re-created after the upgrade.

eTrust Admin cannot be upgraded by the IAM Common Components installer. You will need to upgrade an existing eTrust Admin computer to version 8.1 before running the IAM Common Components installer. Existing eTrust Admin v8.1 computers will be integrated into the IAM suite by assigning the Provisioning Server role to these computers. See the eTrust Admin documentation if you are planning to upgrade existing eTrust Admin software as part of this installation.

Important! *Make a backup of all existing eTrust user data before upgrading your software.*

Methods of Installation

eTrust IAM Common Components can be installed by either the:

- Graphical User Interface to installation wizard
- Command prompt interface to installation wizard

Either method automates the installation of the eTrust IAM Common Components.

Checklist

Prior to installation, you should ensure you have considered:

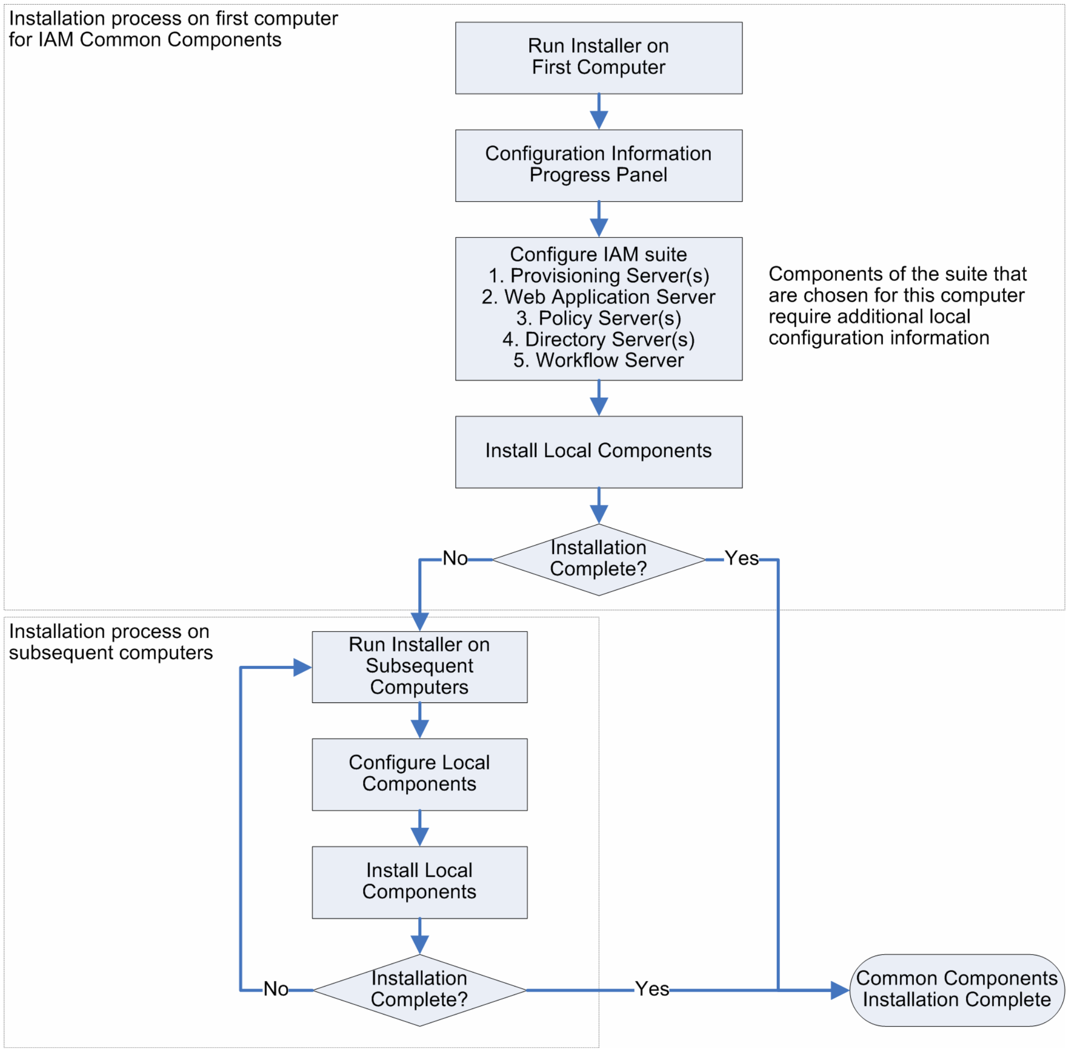
- The role or roles that will be assigned to each computer. At the very least, decide which computer the Provisioning Server will be installed on, and run the installer on that computer first.
- When assigning multiple provisioning server roles for eTrust Admin, if you choose to make the initial computer a Provisioning Server, it will be assigned the root Provisioning Server role. Therefore, you should commence the installation process on the computer which will either **not** play a role as a Provisioning Server or will be assigned the root Provisioning Server role.
- When you are upgrading a product, you need the computer names that currently perform that role and the administrative passwords for those computers.
- If you are upgrading any eTrust software you must backup all user data stores prior to installing the Common Components to avoid losing data. See the “Upgrading” chapter in this guide.
- SMTP server name.
- System administrator’s email address.
- List of Provisioning Server options for each Provisioning Server you wish to install. See the eTrust Admin Options Guides for more information on provisioning server options.

Installation Using the Installation Wizard

Installing the eTrust IAM Common Components can be done using the eTrust IAM Product Explorer to invoke the installation wizard.

The installation wizard installs (as a minimum) a directory server on the first computer where the common component software is installed. This computer stores the common components configuration information that is accessed by other computers included in the installation.

The complete installation process for the IAM Common Components is illustrated in the following graphic. Installing on the first computer requires you to provide a large amount of information which is used to streamline the installation on subsequent computers.


Installation process on first computer for IAM Common Components
Run Installer on First Computer
Configuration Information Progress Panel
Configure IAM suite
1. Provisioning Server(s)
2. Web Application Server
3. Policy Server(s)
4. Directory Server(s)
5. Workflow Server
Components of the suite that are chosen for this computer require additional local configuration information
Install Local Components
Installation Complete?
No
Yes
Installation process on subsequent computers
Run Installer on Subsequent Computers
Configure Local Components
Install Local Components
Installation Complete?
No
Yes
Common Components Installation Complete

Install the Common Components on the First Computer

You can install IAM Common Components on one computer, or on multiple computers. The following procedure describes the installation of IAM Common Components on the first computer.

To install the eTrust IAM Common Components on a computer running Windows, follow these steps:

1. Insert the first eTrust IAM Common Components installation CD in 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 eTrust IAM and then click the Launch the eTrust IAM Installer link.

   The Installation Wizard starts loading and appears after a short delay.

Elements in the Installation Wizard

During installation of the IAM Common Components you will be prompted for information which will be used to configure the suite for your organization.

This section provides background information for each screen you may encounter to help you provide the correct information.

The actual screens displayed and the order encountered depends on information provided. The information provided here (after the initial screen) is sorted into the alphabetical order of the screen titles.

Choose the setup type that best suits your needs

This option enables you to simplify the installation wizard by assigning all possible roles to the current computer with the default options.

- Select Custom to control the configuration of the eTrust IAM suite. This option will allow you to control more fully the installation and configure multiple computers to extend the functionality of your suite.
- Select Express to follow a simplified path through the installation wizard. On a Windows computer this option will install all common components onto this computer.

Configuration Information: Default Location

If you do not wish to use the default location, provide your preferred installation path or click Browse to navigate to your preferred installation path.

Configuration Information: Point Product Selection

Select the products you intend to install as part of eTrust IAM. These selections do not install the complete point product software; rather the common components will be tailored to the specific products that you select. After you have completed the installation of the common components you will need to run the installer on your separate point product CD to complete the installation of your software.

Configuration Information: Progress

This screen displays the current status of your installation.

Choose which set of questions you wish to (re)answer next

This field allows you to choose the set of questions you wish to answer next. In following a custom install the order that questions are answered is important. You are able to return to a section but cannot jump ahead across the order in which the sections are supplied. As sections are completed you can return to these or earlier sections by selecting the desired section and clicking on the Next button.

Directory Server: Assign Computer(s)

Select the computer(s) you want to perform the role of Directory Servers. Only computers in the list that have the check box selected will be configured to run as a Directory Server. The computer where the installation begins must act as a Directory Server. Any computer acting as a Policy Server or a Provisioning Server must also act as a Directory Server. You can select additional computers to run as Directory Servers.

If any computers you want to perform the role of Directory Server are not shown in the list, follow these steps:

- Enter the computer name(s) in the text box, and then click Apply. Each valid computer name is added to the list.
- Verify that each computer you want to assign as a Directory Server is selected.

Directory Server: Install Locations

Directory Server Install Location
Enter the installation location for the eTrust Directory software on this computer.

Advantage Ingres Install Location
Enter the installation location for the Advantage Ingres software on this computer.

Note: Due to a Windows path length limitation the path length supplied for the Advantage Ingres install location must not exceed 71 characters.

Documentation Options

The readme file contains important information relating to the installation of eTrust IAM common components.

- Select Yes to view the readme file at the completion of installation.
- Select No if you do not want to view the readme.

eTrust IAM Install DSA Password: Enter Password

Enter and confirm a password that will protect the configuration information for the common components. This password will be required later when installing common components onto additional computers or modifying the eTrust IAM suite.

Please read the following license agreement carefully

Answer 'I agree' if you agree with the terms of the license agreement.

Answer 'I disagree' if you do not agree with the terms of the license agreement. If you do not agree, this installation wizard will end without installing the software.

Note: You cannot change the selection until you have scrolled right to the bottom of the displayed license agreement.

Policy Manager Terminal Machines

Check the boxes next to the computer names you wish to add to the Terminal Machines list. Administrative accounts can connect to the Policy Server only from computers on the Terminals list. You will not be able to connect as an administrator to the Policy Server from any computer not listed as a Terminal Machine.

If any computers you want to add as Terminal Machines are not shown in the list, enter the computer name(s) in the text box, and then click Apply. Each valid computer name is added to the list.

Verify that each computer you want to assign as a Terminal Machine is selected.

Policy Server: Assign Computer(s)

Select the computers you want to perform the role of Policy Servers. Only computers in the list which have the check box selected will be configured to run as a Policy Server. You can select multiple computers to run as Policy Servers but all computers performing this role must be running the same Operating System.

If any computers you want to assign the role of Policy Server are not shown in the list, follow these steps:

- Enter the computer name(s) in the text box, and then click Apply. Each valid computer name is added to the list.
- Verify that each computer you want to assign as a Policy Server is selected.

When you install the IAM Common Components over an existing Policy Server, thus upgrading it, you must assign the role of Policy Server to your existing Policy Server computers.

Policy Server: Configuration

PS Admin Username
The name of the user who has administrative privileges on the Policy Server(s). You must choose a name that does not already exist as a user on the Policy Server computer(s).

PS Admin Password/PS Admin Password Confirm
The password for the new PS Admin account that will be created on the Policy Server(s).

LDAP Admin Username
The name of the user used by the Policy Server to authenticate to its internal LDAP directories. You must choose a name that does not already exist as a user on the Policy Server computer(s).

LDAP Admin Password/LDAP Admin Password Confirm
The password for the new LDAP Admin account that will be created.

Note: Make a record of the usernames and passwords that you assign on this screen. Store this information in a safe place.

Policy Server: Configure Session Management

This screen determines whether Session Management is enabled or not. Session Management enables limits to be placed on individual SSO clients connecting to the Policy Server. Refer to the *eTrust SSO Administrators Guide* for information on Session Management.

Disabled
Session Management will be disabled.

Enabled
Enables session management for SSO clients from eTrust SSO 7.0 and 8.0. Clients using eTrust SSO 6.5 will have unlimited sessions.

Required
All eTrust SSO users automatically have a default session profile. This setting will prevent eTrust SSO 6.5 clients from connecting to the Policy Server.

Policy Server: Install Location

Policy Server Install Location
Enter the install location for the Policy Server software on this computer.

eTrust Access Control Install Location
Enter the install location for the eTrust Access Control software on this computer.

Policy Server: Password Policy Check Failed

<Policy_Server_Admin_Name> Password / <Policy_Server_Admin_Name> Password Confirm
There was a problem validating the provided password on the target computer. Re-enter and confirm a password that complies with the password restrictions on this computer.

Provisioning Server: ACAS Option

This screen relates to the eTrust Access Control Policies (ACP) option when chosen for a Provisioning Computer.

ACAS Username
The username that can be used to administer the ACAS option on this Provisioning Computer.

ACAS Password/Confirm ACAS Password
The password that will be used with the ACAS Username.

Provisioning Server: ACC Option: Access Control Install Location

Access Control Install Location
Enter the installation location for the Access Control software on this computer.

Provisioning Server: Alternates for <computername>

Alternate Provisioning Servers provide load sharing for a Primary Provisioning Server without introducing a new domain.

Select the computer(s) you want to assign as an Alternate Provisioning Server to the indicated computer <computername>.

Note: Only computers running Windows can perform the Alternate Provisioning Server role.

To add computers not already listed, enter the computer names in the text box and click Apply. When the computer names are accepted as valid computer names, they are added to the list of alternates.

Computers already performing the role of Alternate Provisioning Servers are listed at the bottom of the page. If you select any of these computers, they will cease to perform the Alternate role for the computer they were previously assigned to and will become an Alternate for the indicated computer.

Provisioning Server: Assign Computer(s)

Select the computers you want to perform the role of primary Provisioning Servers.

Only computers in the list that have the check box selected will be configured to run as a Provisioning Server. You can select multiple computers if you want to run multiple provisioning domains.

You can add computers to this list by typing the computer names into the Enter Machine Names field and pressing the Apply button.

Note: When you are integrating an existing eTrust Admin Server you should assign the role of Provisioning Server to your existing eTrust Admin v8.1 Server. You will need to separately upgrade your provisioning server to v8.1 before installing with the IAM common components installer.

Provisioning Server: Configuration

This screen configures a single Provisioning Server.

LDAP Port
Fixed port number used by this Provisioning Server

Provisioning Server Administrator Username
The user name used by an administrator to manage the Provisioning Server administrator account on this computer

Domain Name
Defines the Admin domain created on the Provisioning Server. This defaults to the hostname of one of the computers listed as a Provisioning Server, but can be any string acceptable as a Directory common name. When you upgrade an existing Admin Server, you must enter the existing domain name.

Administrator Password/Administrator Password Confirm
Defines the administrative password for the current Primary Provisioning Server.

Administrator Description
Describes the administrative user on this computer, such as their name or position title.

Parent of <computername>
Defines the primary Provisioning Server relationship for this computer. Select the computer which is the parent of the currently listed primary Provisioning Server. Select 'None (Root)' if the currently listed computer is the root Provisioning Server.

Slapd Service Password/Slapd Service Password Confirm
Defines password required to administer the slapd service on this computer.

Enable Alternate Machines
Indicates whether you want to assign alternate Provisioning Servers to loadshare the role of Provisioning Server for the currently listed computer.

Provisioning Server: Install Locations

Provisioning Server Install Location
Enter the install location for the Provisioning Server software on this computer.

CA_APPSW Install Location
Enter the install location for the CA_APPSW software on this computer.

eTrust Common Services Install Location
Enter the install location for the eTrust Common Services software on this computer.

Provisioning Server: Options

Select the options you want to install on the currently indicated Provisioning Server (and its Alternates), and then click Next.

Note: Some options may be pre-selected and cannot be changed, depending on the products you previously selected to install.

Some options have prerequisites that must be met before the option is installed. The installation can fail if a prerequisite is not met. For more information about these options and their prerequisites, see the eTrust Admin Option Guides provided on the Documentation disk.

Provisioning Server: Password Policy Check Failed

Slapd Service Password / Slapd Service Password Confirm
There was a problem validating the provided password on the target computer. Re-enter and confirm a password that complies with the password restrictions on this computer.

Starting the Installation

Have you already begun your eTrust IAM installation on another machine?

This option enables you to import the suite configuration settings provided on another computer.

- Select No if the eTrust IAM Common Components have not yet been installed on any other computers.
- Select Yes if you have already started installing eTrust IAM Common Components on another computer. Note: You will also need to provide the machine name and Install password used on that computer if you answer Yes.

If you have already started this installation on another computer, see *Complete the Installation on Subsequent Computers*.

Tomcat: Install Location

Tomcat Install Location
Enter the install location for the Apache Tomcat software on this computer.

Tomcat: Install Option

Apache Tomcat 4.1.29 is a required component of eTrust IAM and must be installed on the computer acting as the Web Application Server.

- Select Yes to install Apache Tomcat 4.1.29 on the Web Application Server.
- Select No if Apache Tomcat 4.1.29 is already installed on the Web Application Server and you wish to use this existing installation.

It is strongly recommended that you select Yes, even if you do have an existing installation of Apache Tomcat 4.1.29. If you choose to use an existing installation of Tomcat there is a possibility that it will not be configured appropriately for the eTrust IAM web applications.

Tomcat: JDK Install Location

JDK Install Location
Enter the installation location for the JDK software on this computer.

Tomcat: JDK Install Option

The Java™ 2 Software Development Kit (JDK) version 1.4.2_X must be present on the computer running Tomcat.

- Select Yes to install JDK 1.4.2_04 on the current computer.
- Select No if JDK 1.4.2_X is already installed on the current computer.

Note: If you already have JDK 1.4.2_04 installed on the current computer you must select No. Selecting Yes in these circumstances will cause the installation to fail.

Tomcat: Port Numbers

The following port numbers are required to configure Apache Tomcat on this computer.

SSL HTTP Port
Enter a port number to be used by Tomcat for accepting secure connections.

HTTP Port
Enter a port number to be used by Tomcat for accepting non-secure connections.

Shutdown Port
Enter a port number to be used to manually shutdown Tomcat.

Tomcat: Windows Service Name

Apache Tomcat is installed as a Windows Service.

Tomcat Windows Service Name
Enter the Windows Service Name to be used by Tomcat on this computer.

Web Application Server: Assign Computer

Select the computer you want to perform the role of Web Application Server.

Only the computer that has the check box selected will be configured to run as the Web Application server.

The Workflow Server must be installed before the Web Application Server. Accordingly, if you choose the current computer as the Web Application Server then you must also choose this same computer as the Workflow Server.

You can add a computer to this list by typing the computer name into the Enter Machine Names field and pressing the Apply button.

Web Application Server: Configuration

LDAP Hostname
Select which Provisioning Server will provide the LDAP information required by the Web Application Server.

ETA Server Domain
Displays the eTrust Admin Server Domain name associated with the selected LDAP host.

LDAP Port
Displays the unsecured port number (default 20389) that the Directory Server Agent (DSA) uses to connect with the Provisioning Server.

LDAP TLS Port
Displays the secured port number (default 20390) that the Directory Server Agent (DSA) uses to connect with the Provisioning Server.

SMTP Server
Enter the SMTP Server name which will provide email capability to the Web Application Server.

Administrator Email Address
Enter the administrator's email address. This address will be used by the system when configured to notify the administrator of certain events.

SPML Service Name
The SPML Service name used by the Web Server.

Web Application Server: Install Locations

IA Manager Install Location
Enter the installation location for the IA Manager software on this computer.

eTrust IAM Self Service Install Location
Enter the installation location for the eTrust IAM Self Service software on this computer.

eTrust IAM SPML Service Install Location
Enter the installation location for the eTrust IAM SPML Service software on this computer.

eTrust IAM Configuration Tool Install Location
Enter the installation location for the eTrust IAM Configuration Tool software on this computer.

Web Application Server: JRE Install Location

JRE Install Location
Enter the installation location for the JRE software on this computer.

Web Application Server: JRE Install Option

The Java 2 Runtime Environment (JRE) is a common component of eTrust IAM.

- Select Yes to install JRE 1.4.2_04 on this computer.
- Select No if JRE 1.3 or later is already installed on this computer.

Note: You must select No if you already have JRE 1.4.2_04 installed on this computer. If you do not have JRE installed but you do have a Java Plug-in (1.3 or later) installed you can select either Yes or No.

Workflow Server: Assign Computer

Select the computer to which you want to assign the role of Workflow Server. You do not have to assign the role of Workflow Server to any computer if you do not want to install this function.

If the computer you want to assign as Workflow Server is not shown on the list, follow these steps:

- Enter the machine name in the text box, and then click Apply. When the name entered is a valid computer name, it is added to the list.
- Select the computer name.

Note: If the role of Web Application Server was assigned to the first computer in the installation, then the Workflow Server role can only be assigned to this computer.

Workflow Server: Configuration

LDAP Hostname

Select the LDAP host computer from the list of available provisioning servers. The Workflow Server can be configured to connect to any of the provisioning servers.

Workflow Server: Install Locations

Workflow Install Location

Enter the installation location for the eTrust Directory software on this computer.

Advantage Ingres for Workflow Install Location

Enter the installation location for the Advantage Ingres software on this computer.

Note: This version of Advantage Ingres is different to the version of Ingres used by eTrust Directory.

Complete the Installation on Subsequent Computers

After you finish installing software on the first machine, you can install software on other computers that you listed during this installation. You must take the installation CDs to each of those computers to perform the required installations.

In these subsequent installations, the installation wizard pages are considerably simplified. This is because configuration settings you chose when installing on the first computer are imported for the installation on subsequent computers. Once settings are imported from the first computer, you are prompted only for installation locations relevant to the software being placed on each computer before proceeding with the installation.

To install eTrust IAM Common Components on additional computers, follow these steps:

1. Insert the first installation CD in your CD-ROM 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 eTrust IAM and then click the Launch the eTrust IAM Installer link.

   The Installation Wizard starts loading and appears after a short delay.

3. Click Next.

   The Starting the Installation page appears, asking if you have already started your installation of eTrust Identity and Access Management elsewhere.

4. Select Yes, and then enter the name of the computer where you started your eTrust IAM installation and your IAM Installation password.

5. Click Next.

When the installer connects to the computer and loads your configuration successfully, the Configuration Information Progress screen appears and you will be prompted for additional information depending on which role or roles you assigned to the current computer when performing the first installation. These screens ask questions related to the roles assigned to that computer. See Elements in the Installation Wizard for assistance in responding to these questions.

Once all the questions are answered, the installation will proceed on this computer. When the installation is complete a summary page appears and shows the results of the installation.

If other computers assigned roles have not yet had the software installed, a screen will appear listing the computers on which the eTrust IAM Installer needs to be run. If there are constraints on the order in which these computers should be visited, this screen describes them. Otherwise, the screen states that the eTrust IAM Common Components are fully installed.

Installation from the Command Prompt

The eTrust IAM Common Components can be installed using the command prompt if needed. This method of installation presents the same installation options as the installation wizard.

To initiate the command prompt installer:

1. Insert the CD into the CD-ROM drive.
2. Open a shell window. For example, on Windows choose Start, Run, and enter **cmd**.
3. Navigate to the Install directory on the CD.
4. Enter **setupwin32.exe –console** and press Enter.

The command prompt installation procedure follows the same steps as the installation wizard. For more information see *Installation Using the Installation Wizard*.

Reconfiguring the IAM Suite

The IAM Common Components installer allows you to reconfigure the computers running the components of the IAM suite. You are able to add (but not remove) point products and can also change the computer roles for individual computers.

To reconfigure the eTrust IAM Common Components on a computer running Windows, follow these steps:

1. Insert the first eTrust IAM Common Components installation CD in 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 eTrust IAM and then click the Launch the eTrust IAM Installer link.

   The Installation Wizard starts loading and appears after a short delay.

3. On the screen titled "Starting the Installation" you must select Yes and then provide the computer name of one of the Directory Servers and IAM Install DSA Password before clicking Next.

   The eTrust IAM: Reconfiguration screen appears.

4. Select either of the following and click Next.

   - "Reassign and add machines" to change the roles performed by computers in your IAM suite.
   - "Add supported Point Products" to add a point product to your suite and change the roles performed by computers in your IAM suite.

5. Follow the prompts to reconfigure your IAM suite. The Configuration Information: Progress screen allows you to select any computer roles to alter configuration.

At the completion of installation you may be prompted to perform additional installation or removal tasks on other computers.

Further information

For further information about the following aspects of eTrust IAM, see the "Maintenance" chapter of the Administrator Guide.

- Starting and stopping the IAM Web Application
- Securing the eTrust IAM Web Applications
- Resolving Port Conflicts Manually.

Chapter

6

Implementing the Policy Manager

This chapter explains how to install the Policy Manager.

Policy Manager is a tool that lets you manage the Policy Server and the data stores (eTrust Directory and eTrust Access Control). It is usually installed on an administrator's workstation with TCP/IP communication to the Policy Server.

The Policy Manager is the front-end graphical user interface (GUI) that allows you to manage your users and access control policies easily. You can install the Policy Manager on Windows computers only but you can use it to communicate with both UNIX and Windows Policy Server computers. The Policy Manager can also manage multiple Policy Servers that are deployed in a server farm.

The Policy Manager is an administrative tool and is designed for administrators of the eTrust SSO implementation. Before installing the Policy Manager, you should check whether some of the alternative administration tools available are more appropriate for at least some of your administrators.

selang

You can use the selang command line language to update the policy data store or an eTrust Access Control type of user data store.

IA Manager

Some of the functionality of the Policy Manager is also provided in the IA Manager Web administration interface. The IA Manager application can be accessed from any workstation with a web browser and access to the GUI Server. For more information on the IA Manager, see the *IA Manager online help*.

Before You Begin

The Before You Begin Section is designed to guide you through what you need to know before you install the Policy Manager. In addition to the information in this section, always make sure you review your implementation plan and take note of any specific requirements.

Decide on an Installation Location

The Policy Manager needs to be installed on the workstation of every eTrust SSO Administrator. The computer running the Policy Manager must have administrative access to the Policy Server computer. You can assign Policy Manager terminals with administrative access to the Policy Server computer during the eTrust IAM Common Components installation or, after installation using the Policy Manager. For more information, see the *Administrator Guide*.

You cannot install the Policy Manager to a location containing the % character in the folder path.

Some Policy Manager functionality is only available if you install the Policy Manager on the same computer as the Policy Server. For more information, see the *Administrator Guide*.

Policy Manager and Policy Server on One Computer

This sections lists what you need to know if you are installing the Policy Server and the Policy Manager on the same computer.

- If you install the Policy Manager on the same computer as the Policy Server, ensure that you install the Policy Server first. The Policy Server is installed as part of the eTrust IAM Common Components installation.
- When you install the Policy Manager on the same computer as the Policy Server, make sure that you stop the eTrust Access Control (eTrust AC) service before you install the Policy Manager.
  - This is particularly important with the silent install because no error will pop up
  - If you have a server farm configuration, you must do this for every computer in the server farm
  - If you have set up eTrust AC as your user data store, and the eTrust AC installation is on a separate computer to the Policy Server, you will need to stop the eTrust AC services on that machine

  For more information about stopping and starting the eTrust AC service, see the "Maintenance" chapter of the *Administrator Guide.*
- If you log onto the Policy Server, via the Policy Manager, where both components are installed on the same computer, your logon may fail if you were not the person who installed the Policy Server on that computer.

  For the log on to be successful the Windows user who is logged onto the computer, must have read/write access to the terminal in Policy Server. The Policy Server checks the user's Windows credentials. When a user installs the Policy Server, the installer checks the user's Windows logon credentials and automatically gives that user read/write access to the Policy Server.

  You can authorize a user to have read/write access in the Policy Manager, using Resources, Configuration Resources, Terminal, [select user], Authorize.

Decide on a Method of Installation

This section explains each type of installation to help you choose which method you should use.

The Policy Manager can be installed by one of three methods:

Graphical installation wizard

The graphical installation wizard leads you through the various steps required for installing the Policy Manager. Use this method to familiarize yourself with the installation options.

Graphical installation wizard with custom defaults

From the command line, you can pass defaults to the graphical installation wizard. Use this method to create a batch file that opens the wizard with the defaults you want to use.

Silent installation

Using the command line, you can silently install the Policy Manager rather than just pass defaults to the graphical installation wizard. Use this method to push the installation to remote computers.

Pre-Installation Checklist

Use this checklist to make sure you have performed all pre-installation review tasks:

❑ Ensure that you stop eTrust Access Control (eTrust AC) before you install the Policy Manager. For more information about stopping and starting the eTrust AC service, see the "Maintenance" chapter of the *Administrator Guide.*

❑ Ensure that all system requirements are met before you begin installing the Policy Manager. For a complete list of system requirements, see the product Readme file.

❑ Ensure that all the necessary prerequisite components have been installed and are functioning properly. Specifically, be sure that the eTrust IAM Common Components have been installed. Test each component to be sure that it works.

❑ Ensure that you know the name of the computer or computers that you are installing the Policy Manager on.

❑ Ensure that the computer you are installing the Policy Manager on has TCP/IP communications with the Policy Servers that you want to manage.

❑ Ensure that you have the names of the Policy Server computers that host the Policy Servers that you want manage. You do not need this information until after the installation when you need to connect to the Policy Server for the first time.

Install Using the Graphical Wizard

To install the Policy Manager component of eTrust SSO using the graphical wizard, follow these steps:

1. Insert the product installation CD into your CD-ROM drive.

   If you have Autorun enabled, the Product Explorer automatically displays. Otherwise, navigate to the CD-ROM drive and double-click the PE_i386.EXE file.

2. From the Product Explorer main menu, select Policy Manager for Windows, and click Install.

3. Follow the wizard prompts and when you are done, click Install to start the Policy Manager installation.

   Depending on the choices you make, you may need to specify the following options:

   Setup Type
   Specifies the type of installation you want to perform. Choose Complete if you do not require any specialized options, or choose Custom if you want to decide on where the installation should place the Policy Manager files.

   Policy Manager Modes
   Specifies which applications you can manage using the Policy Manager. Make sure that eTrust Single Sign-Onl is selected.

   Encryption Method
   Specifies the type of encryption used to encrypt communication between the Policy Manager and the Policy Server.

   Destination Folder
   Specifies where you want to install the Policy Manager files.

Tip: When the message InstallShield Wizard Complete appears, you have successfully installed the Policy Manager. Be sure to review the Readme file, and then click Finish to complete the process.

Command Line Installations

You can use the command line to:

- Pass defaults to the graphical installation wizard.
- Silently install the Policy Manager.

Install Using the Command Line to Set Custom Defaults

To install the Policy Manager component of eTrust SSO using the command line with custom defaults, follow these steps:

Note: If you previously installed the Policy Server on this computer, you need to stop the eTrust Access Control services before installing the Policy Manager.

1. Open a command prompt and navigate to the Policy Manager folder on the eTrust SSO CD.
2. From the command prompt, enter:

   ```
   setup.exe /s /v"<insert variables here>"
   ```

   For information about what values you can specify, see the Command Line Settings section in this chapter.
3. Once the Policy Manager installation wizard opens, follow the prompts to install the Policy Manager.

Install Using the Silent Installation

To install the Policy Manager component of eTrust SSO using the silent installation, follow these steps:

Note: If you previously installed the Policy Server on this computer, you need to stop the eTrust Access Control services before installing the Policy Manager.

1. Open a command prompt and navigate to the Policy Manager folder on the eTrust SSO CD.
2. From the command prompt, enter:

   ```
   setup.exe /s /v"/qn <insert variables here>"
   ```

   For information about what values you can specify, see the Command Line Settings section in this chapter.

   Note: In order to execute a silent installation you have to accept the license agreement. The setting required for accepting the license agreement and silently installing the Policy Manager can be found at the bottom of the license agreement available when running the installation wizard.

Command Line Settings

The command line settings for installing the Policy Manager are:

Setting	Description
/s	Hides the initialization dialog.
/v	Passes parameters and property settings to the installation. It applies to all the parameters and properties listed in this table except /s. Place any parameters you wish to pass to the installation within quotes ("").
/L	Defines the full path and name of the installation log file. Use the mask *v to log all available information.
/qn	In conjunction with the /s parameter, used to initiate a silent installation. **Note:** You need to use the *license_accept* property to execute a silent installation.
license_accept	*license_accept* is the setting required for accepting the license agreement and silently installing the Policy Manager. The actual setting you need to use can be found at the bottom of the license agreement that is available when running the installation wizard.
ACMODE=[0|1]	Specifies whether the Policy Manager is used to manage eTrust Access Control. Use 1 for yes and 0 for no. Only available for a silent installation.
AZNMODE=[0|1]	Specifies whether the Policy Manger is used to manage eTrust Web Access Control. Use 1 for yes and 0 for no. Only available for a silent installation.
SSOMODE=[0|1]	Specifies whether the Policy Manger is used to manage eTrust Single Sign-On. Use 1 for yes and 0 for no. Only available for a silent installation.
INSTALLDIR=[location]	Specifies the location where the Policy Manager will be installed.

Setting	Description
ENCRYPTION_METHOD=[defenc.dll|desenc.dll | tripledesenc.dll]	Specifies the encryption method for the Policy Manager where defenc.dll is the Default method, desenc.dll is the DES method, and tripledesenc.dll is the 3DES method.

Note: To set the default for the products you want the Policy Manager to manage in non-silent installations, modify the PMMode.ini file in the source media directory.

The following example sets the installation directory, and installation log file defaults for the Policy Manager installation and then opens the graphical installation wizard.

```
setup.exe /s /v"INSTALLDIR=C:\PM /L*v %SystemRoot%\PMInstall.log"
```

Perform Post-Installation Verification

To verify that the installation of the Policy Manager has been successful, review the following steps:

1. Log on to the Policy Manager. From the Start button on the task bar, choose Programs, Computer Associates, eTrust, Access Control, Policy Manager.
2. Click the Users, Agents, and Resources icons on the program bar. Expand the folders in the tree to verify that the basic functionality is accessible through the Policy Manager.

Chapter

7

Implementing Authentication

The process by which the end users identify themselves to eTrust Single Sign-On (eTrust SSO) is called primary authentication. You can implement different types of security software and hardware to allows users to perform primary authentication.

eTrust SSO comes with native SSO authentication, LDAP authentication, and provides you with authentication agents to let you use a number of third-party authentication methods as well.

In order to provide maximum operational flexibility, a separate authentication agent serves as a bridge for communication, handling the interactions between the SSO Client and the authentication server.

eTrust SSO includes ready-made agents for various authentication systems.

This chapter describes how to implement each of the authentication agents that are supplied with eTrust SSO:

- Certificate
- Entrust
- LDAP
- Novell NetWare
- RSA SecurID
- SafeWord
- Windows

You can also use the eTrust SSO Open Authentication Toolkit to create an authentication agent for other authentication systems used in your organization. This lets you use your existing authentication methods to authenticate users to eTrust SSO.

One of the three components of each authentication agent is a ticket granting agent (TGA). The TGA is a Windows service or a UNIX daemon. This component communicates with the authentication server and also communicates with the SSO Client library component through TCP/IP.

How Primary Authentication Works

This section gives you an overview of how the primary authentication process works. The following events describe the primary authentication process:

1. The user starts the SSO Client on their workstation.
2. The SSO Client checks the AuthMethods keyname in the Serversets section of the SsoClnt.ini file.

   All authentication methods listed in this section are available to the user. The first in the list will be displayed as the default.
3. The authentication dialog displays, prompting the user to:
   - Select the appropriate server set.
   - Provide credentials, such as a user name and password, biometric information, or a smart card.
4. The SSO Client sends the user's credentials to the authentication agent that is running on the server that corresponds to the chosen authentication method as specified in the configuration file.
5. The authentication agent verifies that the credentials are valid, either using its own built-in mechanism or (the more common scenario) by sending them to an authentication server with a verification request.
6. If the credentials are deemed to be invalid, the authentication agent sends an error message to the SSO Client, informing it that the primary authentication has failed.

   If the verification is successful, the authentication agent creates an SSO ticket, encrypts it using a configured encryption key, and sends it to the SSO Client. The SSO ticket is a string that includes user identification, authentication method, and time stamp. The ticket is valid for a defined number of hours.
7. The SSO Client performs the following two actions with the SSO ticket:
   - Caches the SSO ticket. Later, it uses the same ticket in the application logon process.
   - Sends the SSO ticket to the Policy Server.
8. The Policy Server verifies the SSO ticket.
9. If the ticket is not valid, authentication fails and the user receives an error message.

   If the ticket is valid, the Policy Server retrieves from the user data store the list of the applications that the user is authorized to use, and sends the list to the SSO Client.

   The SSO Client displays the list of applications. The user can now start work.

Before You Implement Authentication

This section is designed to guide you through what you need to know before you implement authentication. In addition to the information in this section, always make sure you review your implementation plan and take note of any specific requirements.

Decide which Authentication Method to Use

You should decide about which authentication method to use in conjunction with your IT security manager.

- If you already have an authentication method deployed in your organization you may wish to continue to use that.
- If you wish to use Biometric authentication you may already have third-party software and wish to continue to use that software.
- If you do not wish to use your existing authentication methods, or have none deployed, you may wish to use an authentication method that comes with eTrust SSO, or create a custom authentication agent to use with eTrust SSO.

Decide Where to Install the Authentication Agent

Here is a list of the authentication methods and suggestions of where to install the corresponding authentication agents if you want to implement that method.

LDAP Authentication

You must install the LDAP authentication agent on a computer that has TCP/IP connection to the computer where an LDAP-based directory product is deployed. eTrust Directory, which is an LDAP directory that you can use, comes with eTrust SSO. It is one of the eTrust IAM Common Components.

SSO Authentication

You do not need to install an authentication agent because the Policy Server verifies the user credentials and creates a ticket.

Note: SSO Authentication does not support hierarchical name spaces.

Windows authentication agents

You should install the Windows authentication agent on a domain controller.

Novell Netware

You should install the Novell Netware authentication agent on a Novell server computer.

Entrust, Certificate, RSA SecurID, Safeword authentication agents

If you want to implement any of these authentication methods, you must install the authentication agent on a computer with a TCP/IP connection to the SSO Client computer, and with an appropriate connection to the computer where the relevant Authentication Server is deployed.

Design Your Server Sets on the SSO Client

To use any of the authentication methods for primary authentication, you must define server sets by correctly configuring the SsoClnt.ini configuration file. For more information about server sets and how to create them, see the chapter "Implementing the SSO Client". For more information about configuring the SSO Client, see the appendix "Configuring the SSO Client: SsoClnt.ini" of the *Administrator Guide*.

Assign Port Numbers to the Authentication Agent

By default every authentication agent is given a default port number. You only need to manually configure the port number of an authentication agent if you:

- Want to install multiple instances of authentication on one authentication agent server.
- Already have a service using the default port number for an authentication agent.

You can only configure the port numbers for the following authentication agents:

- Certificate
- Entrust
- LDAP
- RSA SecurID
- SafeWord

Novell NetWare and Windows authentication agents do not use TCP/IP ports. The Novell authentication agent uses the Novell APIs, and the Windows authentication agent uses named pipes.

Configuring the Port Number Manually

To manually configure a port number on the SSO Client to communicate with the authentication agent computer, follow these steps:

1. Open the SsoClnt.ini file in a text editor.
2. Find where the authentication agent is listed in the [ServerSets#] Section.
3. Where the server is listed, add “:<*port number*>” to the end. For example:

   ```
   [ServerSet0]
   AuthMethods=LDAP
   AuthLDAP=server1:12345
   ```

4. Make sure that the authentication agent host computer has the same port specified to “listen” for information from the SSO Client.

Default Authentication Agents' Port Numbers

Here is a list of the default ports used for the authentication agents:

- Certificate Authentication Agent – Port: 13987
- Entrust Authentication Agent – Port: 13987
- LDAP Authentication Agent – Port: 17979
- RSA/SecurID Authentication Agent – Port: 13969

Synchronize Operating Systems

All operating system clocks must produce a reliable and correct timestamp for the time-zone where each computer hosting any SSO components is located. For example, a computer located in New York hosting a Policy Server will have its operating system clock set to US Eastern Daylight Time (EDT), and a computer located in San Francisco hosting a LDAP Auth Agent will have its operating system clock set to US Pacific Daylight Time (PDT).

Pre-Installation Checklist

Use this checklist to ensure you have performed all pre-installation review tasks:

❑ Ensure that all system requirements are met before you begin installing the authentication agent. For a complete list of system requirements, see the product Readme file.

❑ Ensure that all the necessary prerequisite components have been installed and are functioning properly. Specifically, be sure that the eTrust IAM Common Components have been installed. Test each component to be sure that it works.

❑ Ensure that you know the name of the computer or computers that you are installing the authentication agent on.

❑ Ensure that the computer you are installing the agent on has TCP/IP communications with the SSO Client computers and the Policy Server computers.

❑ Ensure all operating system clocks produce a reliable and correct timestamp for the time-zone where each computer hosting any SSO components is located. See the Synchronize Operating Systems section in this chapter.

❑ For Certificate authentication, decide which revocation methods you want to use.

❑ For Certificate authentication, decide which trusted certificate you want to use.

Implementing the Certificate Authentication Agent

eTrust SSO supports primary authentication using certificates. This section explains how to install the Certificate authentication agent.

Before You Begin

The Before You Begin Section is designed to guide you through what you need to know before you install the Certificate authentication agent. In addition to the information in this section, always make sure you review your implementation plan and take note of any specific requirements.

Specify Trusted Certificates

The Certificate authentication agent uses a list of trusted certificates to determine if it should allow a user certificate to be verified. Unless the issuing certificate of the user certificate is included in this configuration option, the user certificate can not be verified by the Certificate authentication agent.

When you install the Certificate authentication agent you will be asked to specify a trusted certificate. You can use a ‘Browse’ button to navigate to the directory that contains the DER-encoded certificate.

You must specify at least one trusted certificate to install the Certificate authentication agent, but you may also specify multiple trusted certificates. These certificates must all be located in the same Directory.

Understand Revocation Settings

This section explains what certificate revocation is and tells you about the different revocation settings for the certificate authentication agent.

Revocation refers to the fact that the system can block certain certificates. This is based upon the system knowing which certificates cannot be trusted. There are several ways that the system can identify untrustworthy certificates.

CRL

CRL stands for Certificate Revocation List. This is a list of certificates that have been revoked by the Certification Authority. The CRL is a blacklist that contains the certificates which are no longer valid.

Fixed OCSP

Fixed OCSP lets you specify a fixed address for an OCSP responder that can check the user certificates and verify whether they are valid or have been revoked.

You will also need to have the full address (DNS/IP address and the Port) of the responder to use this option.

AIA OCSP

AIA OCSP lets the Certificate authentication agent retrieve the OSCP responder address from the user certificate. This means that you don't have to specify a fixed OCSP address. To use this option the users' certificates must contain an OCSP responder address in the 'Authority Information Access (AIA)' attribute.

CRL DP

The CRLDP stands for CRL Distribution Points. This option lets the Certificate authentication agent retrieve a CRL via either HTTP or LDAP by using an address listed in the 'CRL Distribution Points' attribute of the certificate.

You will also need to have the issuing/signer certificate of the CRLs that will be used by the Certificate authentication agent.

You are required to specify at least one issuing/signer certificate, and you can specify multiple issuing/signer certificates. These certificates must reside in the same directory.

Combinations

The Certificate authentication agent lets you use a combination of two of the available Revocation Status Checking Methods. All combinations consist of CRL together with another method. The available combinations are:

- CRL and Fixed OCSP
- CRL and AIA OCSP
- CRL and CRLDP

The benefit of using a combination of Revocation Status Checking Methods is that it will provide a more accurate result. The Certificate authentication agent will always first check that certificate with the CRL. If the certificate is listed as revoked here, the authentication agent will not check the second method. If the certificate is not listed as revoked on the CRL, the authentication agent will go on to check the second method. The configuration for each of the methods is the same as if you selected them individually.

Configure the SSO Client

This section explains what changes you need to make to the SsoClnt.ini file on the SSO Client computer to configure Certificate authentication:

1. Edit the SsoClnt.ini file to include CERT as one of the authentication methods, preferably the first method in the list. For example:

   ```
   [ServerSet0]
   AuthMethods=CERT
   authCERT=Server1:13987
   ```

   The port number is optional. If the port number is not specified, the default port (13987) is used.

2. Specify the values of the other settings associated with Certificate authentication in the [auth.CERT] section of the SsoClnt.ini file. For example:

   ```
   [auth.CERT]
   certStore=PKCS11 FILE
   defaultPkcs11Slot=
   Pkcs11LibraryPath=C:\Program Files\Schlumberger\Smart Cards and
   Terminals\Cyberflex Access Kits\v4\slbck.dll
   Pkcs11PromptText=
   disablePasswordField=0
   Pkcs11TokenAbsenceBehavior=1
   ```

For more information about the SsoClnt.ini file settings, see the “Configuring the SsoClnt.ini File” appendix in the *eTrust SSO Administrator Guide.*

Install the Certificate Authentication Agent

To install the Certificate authentication agent you must install the necessary files and then install and start the Certificate authentication agent service.

This section explains how to install the Certificate authentication agent, and how to start it once it has been installed.

Wizard Installation

Note: Before you install the Certificate authentication agent you should have all your certificates saved in a single directory on the same computer that you intend to install the agent on. This directory should contain at least one trusted certificate. You will be prompted for the certificates during the installation.

To install the Certificate authentication agent, follow these steps:

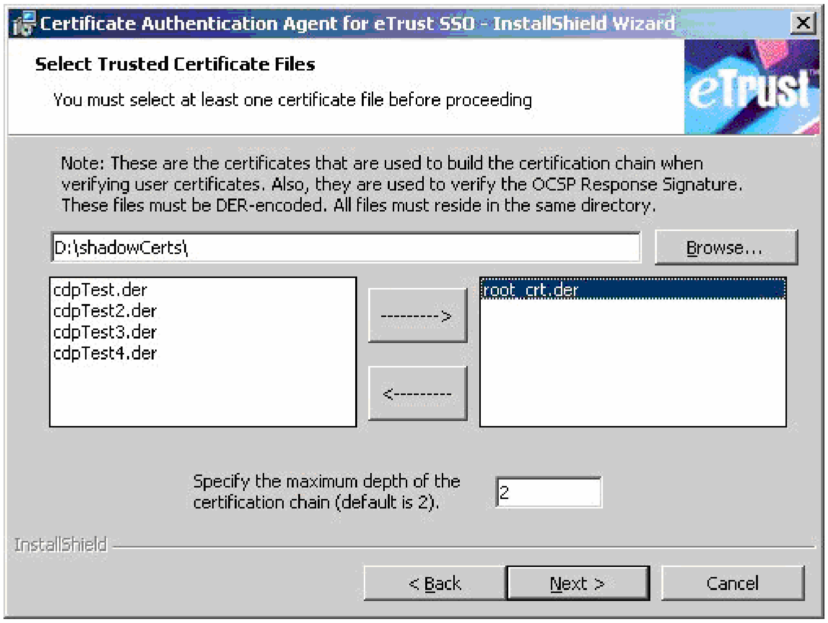
1. From the eTrust Single Sign-On 8.0 Product Explorer wizard expand the eTrust Single Sign-On authentication agents folder, and select Certificate authentication agent.

   The wizard should appear automatically when you insert the eTrust SSO disk. If not, open Windows Explorer and navigate to the CD-ROM directory and double-click the PE_i386.exe file.

   The Install button becomes active.

2. Click Install and accept the license agreement.

   The Select Trusted Certificate Files dialog appears.



Certificate Authentication Agent for eTrust SSO - InstallShield Wizard

Select Trusted Certificate Files

You must select at least one certificate file before proceeding

Note: These are the certificates that are used to build the certification chain when verifying user certificates. Also, they are used to verify the OCSP Response Signature. These files must be DER-encoded. All files must reside in the same directory.

D:\shadowCerts\

cdpTest.der
cdpTest2.der
cdpTest3.der
cdpTest4.der

root_crt.der

Specify the maximum depth of the certification chain (default is 2). 2

3. Navigate to the directory that contains the DER-encoded certificate files of trusted issuing certificates. You must select at least one trusted issuing certificate.

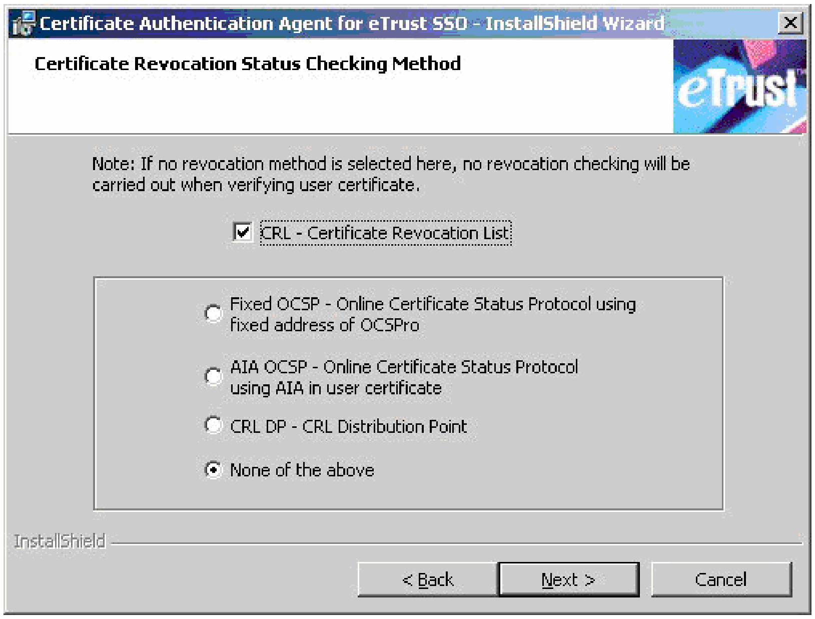
   The Certificate authentication agent uses this list of trusted certificates to determine if it should allow a user certificate to be verified. The user certificate cannot be verified unless the issuing certificate is specified here.

   You can specify multiple trust certificates, but they must all be in the same directory.

   You can also specify the maximum number of certificates that are checked in the chain of certificates in the trusted set. The certification chain is also called verification chain. For more information, see The Configuration Settings for the CERT authentication Agent section of this chapter (the VerifyDepth keyname in the table).

4. Click Next.

   The Certificate Revocation Status Checking Method dialog appears.



Certificate Authentication Agent for eTrust SSO - InstallShield Wizard

Certificate Revocation Status Checking Method

Note: If no revocation method is selected here, no revocation checking will be carried out when verifying user certificate.

☑ CRL - Certificate Revocation List

○ Fixed OCSP - Online Certificate Status Protocol using fixed address of OCSPro

○ AIA OCSP - Online Certificate Status Protocol using AIA in user certificate

○ CRL DP - CRL Distribution Point

● None of the above

You can configure the Certificate authentication agent to perform revocation status checking on the user certificates. These are the six revocation status checking methods that you can use:

- CRL
- Fixed OCSP
- AIA OCSP
- CRLDP
- None
- A combination of CRL, and either Fixed OCSP, AIA OCSP, or CRLDP.

5. Select the appropriate Certificate Revocation Status Checking Method if you want to use a checking method, and click next.
6. Depending on which Certificate revocation status checking method you chose you will be prompted for different information. The following table shows you what information you will need for each option.

If you selected	You will be prompted for this information
CRL	▪ The Certificate Revocation List. ▪ The CA (certificate authority) that issued the CRL (a DER file). ▪ The time interval between each poll for an updated CRL (optional).
Fixed OCSP	▪ The hostname and port number of the OCSP Responder. ▪ The certificate that is used to sign the OCSP request to your responder. This must be a PKCS#12 file. ▪ HTTP Proxy configuration, if necessary, for the Certificate authentication agent to access the OCSP responder.
AIA OCSP	▪ The certificate that is used to sign the OCSP request to your responder. This must be a PKCS#12 file. ▪ HTTP Proxy configuration, if necessary for the Certificate authentication agent to access the OCSP responder.
CRL DP	▪ A certificate that is used to issue the CRL. These files must be DER-encoded. ▪ The time interval between each poll for an updated CRL (optional).

7. In the Additional Information dialog, enter the name of the Authentication Host entry on the Policy Server, and the value of the encryption key associated with it. By default, the Policy Server installation creates a CERT_Authhost entry with a randomly-generated key value. Depending on your desired setup, you have a choice of either using the details of this Authentication Host entry or creating and configuring a new one.

8. Select Next to complete the installation.

Silent Installation

To install the authentication agent using the silent installation, follow these steps:

1. Open a command prompt and navigate to the Authentication Agent folder on the eTrust SSO CD.
2. From the command prompt, enter:

   ```
   setup.exe /s /v"/qn <insert variables here>"
   ```

   For information about what values you can specify, see the Command Line Settings section in this chapter.

   Note: In order to execute a silent installation you have to accept the license agreement. The setting required for accepting the license agreement and silently installing the authentication agent can be found at the bottom of the license agreement available when running the installation wizard.

Command Line Settings

The command line settings for installing an authentication agent are:

Setting	Description
/s	Hides the initialization dialog.
/v	Passes parameters and property settings to the installation. It applies to all the parameters and properties listed in this table except /s. Place any parameters you wish to pass to the installation within quotes ("").
/L	Defines the full path and name of the installation log file. Use the mask * to log all available information. For example: `/L* C:\log.txt`
/qn	In conjunction with the /s parameter, used to initiate a silent installation. **Note:** You need to use the *license_accept* property to execute a silent installation.
license_accept	*license_accept* is the setting required for accepting the license agreement and silently installing the authentication agent. The actual setting you need to use can be found at the bottom of the license agreement that is available when running the installation wizard.
INSTALLDIR=[location]	Specifies the location where the authentication agent will be installed.

Trusted Certificate Files

Setting	Description
TRUSTEDCERTPATH	Specifies the location of .der / .crl files
TRUSTEDCERTNAMES	Specifies a list of .der / .crl files
VERIFYDEPTH	Specifies the maximum depth of the certification chain. Default value is 2

Certificate Revocation List

Setting	Description
CRLFILENAME	Specifies the Certificate Revocation file. It must be signed by the CA and be DER-encoded. This may be a local file, http URL, or ldap URL.
CRLISSUERCERT	Specifies the CA certificate that issued this CRL.
CRLPOLLINTERVAL	Specifies the CRL Polling Interval in seconds. ie. how often to poll for updates of the CRL. If this is 0, there will be no polling for new CRL updates.

Certificate Revocation Status Checking Method

Option 1 - If you use a CRL Distribution Point:

Setting	Description
CRLDPISSUERCERTPATH	Specifies the location of the DER-encoded CRL certificate files.
CRLDPISSUERCERTS	Specifies the list of the DER-encoded CRL certificate files.
PROXYVALUE	Specifies the proxy address to access an OCSP Responder or retrieve CRL over HTTP. "IE5://" specifies to use the Internet Explorer settings on the system.
CRLDPTIMEOUT	Specifies the timeout for retrieval of CRL or CRLDP revocation. Minimum is 30 seconds.

Setting	Description
CRLPOLLINTERVAL	Specifies the CRL Polling Interval in seconds. ie. how often to poll for updates of the CRL. If this is 0, there will be no polling for new CRL updates.

Option 2 - If you use an Online Certification Status Protocol using ACA in user certificates:

Setting	Description
OCSPSIGNCERT	Specifies the Certificate with which to sign OCSP Requests. Must be a PKCS#12 file.
OCSPSIGNCERTPASS	Specifies the password of the above file.
PROXYVALUE	Specifies the proxy address to access an OCSP Responder or retrieve CRL over HTTP. "IE5://" specifies to use the Internet Explorer settings on the system.

Option 3 - If you use Online Certificate Status Protocol using fixed address of OCSPro:

Setting	Description
OCSPDATA	http://hostname-of-ocsp-responder:port-number-of-responder. Default port is 3080.
OCSPSIGNCERT	Specifies the Certificate with which to sign OCSP Requests. Must be a PKCS#12 file.
OCSPSIGNCERTPASS	Specifies the password of the above file.
PROXYVALUE	Specifies the proxy address to access an OCSP Responder or retrieve CRL over HTTP. "IE5://" specifies to use the Internet Explorer settings on the system.

Post Installation Configurations

The following sections explain what you need to do after you have installed the Certificate authentication agent. You only need to configure the SSO client to complete a standard installation. Other configuration options may be necessary depending on your particular requirements.

Create an Authentication Host Entry on the Policy Server

You only need to do this if you decide to use a different authentication host to the one you specified during installation. You will first need to define a new authentication host on the Policy Server. For information on defining an authentication host, see the “Managing Resources” chapter in the *eTrust SSO Administrator Guide*.

Once you have an authentication host defined on the Policy Server, you need to change the AuthHostName registry key value corresponds to the new authentication host entry. You then need to update the TicketKey registry key value to the ticket encryption key value specified for the authentication host entry on the Policy Server. For more information on registry key settings for the Certificate authentication host, see Configuration Settings for the Certificate Authentication Agent later in this chapter.

Set Name Mapping

When a Certificate authentication agent has verified that a user certificate is valid, it creates an SSO ticket for that user. The SSO ticket is sent back and stored on the SSO Client. The SSO ticket is sent to the Policy Server whenever a user requests access to an application, and tells the Policy Server that the user has valid authentication.

To identify which user the SSO ticket belongs to, the SSO ticket contains a field that identifies the user name. The value in the user name field identifies the user and must match the Common Name (CN) attribute for that user in the Policy Server user data store.

Name Mapping Settings

When the eTrust SSO r8 Certificate authentication agent is installed, a default name mapping DLL is provided. This is where you define which attribute to use for the *user name*. These values are set during the authentication agent installation.

The name mapping DLL defines the certificate name mapping behavior and defines what is used in the user name field of the SSO ticket. The name mapping DLL values are found in the following Windows Registry Setting:

```
KEY_LOCAL_MACHINE\SYSTEM\CurentControlSert\Services\[servicename]\Param
eters\name_mapping\
```

By default, the user name inserted into the SSO Ticket is retrieved from the CN field in the certificate file. This is set by the data value for the MappingMethod, as shown in the following table and can be changed to any of the certificate attributes listed in the following table. For example, EMAIL.

Name	Type	Data
MappingMethod	REG_SZ	CN
NameMappingDLLPath	REG_SZ	C:\Program Files\CA\eTrust SSO\Certificate Agent\name_mapping.dll

Name Mapping Attributes

This table lists all the attributes that can be used in the MappingMethod data field. You can designate any of the certificate attributes listed in the following table to populate the *user name* field in the SSO ticket. It is worth noting, however, that values such as C (country) or O (organization) are not user-specific and are therefore generally unsuitable for this kind of identification.

Attribute Code	Attribute	Location in Certificate
CN	Common Name	Subject DN
DN	Distinguished Name	Subject DN
OU	Organizational Unit	Subject DN*
C	Country	Subject DN
O	Organization	Subject DN
L	Location	Subject DN
EMAIL	Email address	Subject Alternative Name
IP	IP Address	Subject Alternative Name
DNS	DNS	Subject Alternative Name
URI	URI	Subject Alternative Name

*

Note: The default DLL will only extract the first instance of an attribute. For example, if a certificate contained two OU fields, only the first encountered would be extracted.

Custom Name Mapping

You can also customize your own *user name* identifier by creating a custom name mapping DLL.

To use a user attribute in the certificate file that is not listed in the default name mapping attributes table, you must create a custom DLL with the following exported functions.

```
int name_mapping_get_mapped_name(const unsigned char* cert, const
unsigned int len, unsigned int* buffLen, char* nameBuff);
int name_mapping_init(const char* serviceName);
void name_mapping_term(void);
```

See the name mapping DLL header file, installed as part of the Certificate authentication agent, for definition of the function signature and parameters.

To use the custom name mapping DLL, specify the path to the custom DLL in the "NameMappingDLLPath" registry entry. The Certificate authentication agent will look up the name of the name mapping DLL using this entry and load the DLL.

The Certificate Auth Agent will use the nameBuff it gets back from the call to name_mapping_get_mapped_name as the username when it creates the SSO Ticket.

Use Certificate Authentication with Active Directory

This section explains how to let the Certificate authentication agent retrieve a CRL from an Active Directory using a CRLDP from the client certificate.

It covers:

- Defining the CRLDP address that will be published in the user certificates
- Enabling anonymous access to the CRL store in Active Directory
- Configuring the Certificate authentication agent to use the CRLDP address from the user certificate.

Step 1: Installing the MS Windows Support Tools on the Active Directory Computer

From the Windows 2003 Server CD install the SUPTOOLS.MSI found in the directory \SUPPORT\TOOLS\

Step 2: Creating an ADSI Edit Console

1. Select Start, Run, and enter mmc.

   The Microsoft Management Console application starts.
2. Select File, Add/Remove Snap-in
3. Click the Add button.

   A list of available snap-ins displays.
4. Select ADSI Edit from the list and click Add.

   ADSI Edit is added to the list of snap-ins.
5. Click Close and then OK.
6. Right-click on the ADSI Edit attribute under the Console Root entry and select Connect to.
7. Make sure the Select a well known Naming Context option is enabled.
8. Select Domain from the drop down list and click OK.
9. Repeat steps 6-8, this time selecting Configuration from the context menu.
10. Click OK.

Step 3: Enabling Anonymous Access to the Active Directory

1. From within the ADSI Edit console, expand the Configuration node and navigate to the following
DN: CN=Directory Service,CN=Windows NT,CN=Services
2. Right-click on the CN=Directory Service node and select Properties from the menu.
3. With the Attribute Editor tab selected, scroll through the list until you find the dsHeuristics attribute.
4. Double-click on the dsHeuristics attribute to open the editor. If the attribute is empty, set it with the value: 0000002. If the attribute has an existing value, make sure the seventh digit is set to 2.
5. Click OK and then OK again.

Step 4: Enabling Anonymous Access to the CRL Store of the Active Directory

Now that the ability to make anonymous connections to the Directory is enabled, you need to specify which attributes/entries that exist in the AD can actually be accessed via an anonymous connection.

1. From within the ADSI Edit console, expand the Domain node. This should display an node which contains the same name as the domain that is running on the computer (for example, DC=name,DC=com). Right-click on this node and select properties from the menu.
2. Select the Security tab and click Add. Enter anonymous in the object name field and select Check Names. This should resolve the name to ANONYMOUS LOGON. Click OK twice.
3. Select and Expand the Configuration node. Right-click on the first entry (CN=Configuration,DC=name,DC=com) and select Properties. Add the ANONYMOUS LOGON in the Security tab. This can be done using the same steps as before.
4. Expand the CN=Configuration,DC=name,DC=com node. The CRL store is located four levels under the Configuration node. You will need to add the "ANONYMOUS LOGON" user in the security tab to the following attributes:
   - CN=Services
   - CN=Public Keys Services
   - CN=CDP
   - CN=*DomainName*
   - CN=*rootCertName*

   Each attribute can be found by expanding the node listed above it. Also the last attribute is located inside the DomainName attribute.

5. You can test that the Anonymous Access has been configured correctly by using Jxplorer. Open Jxplorer and enter the following information:

   ```
   BaseDN: CN=rootCertName,CN=computerName,CN=CDP,CN=Public Key
   Services,CN=Services,CN=Configuration,DC=domainprefic,DC=com
   Host: AD computer name or IP Address
   Port: 389
   Security Level: Anonymous
   ```

6. Click OK.

   You should be able to connect to the CRL Store of the Active Directory. The first attribute is the list should be certificateRevocationList

Step 5: Configuring the CRL Distribution Point for the Microsoft CA

Along with configuring the Active Directory to accept anonymous connections, you need to specify the correct LDAP URL that will be used as the CRLDP.

1. Open the Certification Authority manager, right-click on the top level of the structure (it will have the same name as the CN of your root certificate) and select Properties.

2. Select the Extensions tab, and make sure that CRL Distribution Point (CDP) is selected from the drop down list.

   Depending on if you have already edited this extension, the default entries listed should be:

   ```
   C:\WINDOWS\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix><Delta
   CRLAllowed>.crl
   ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortName>,CN=
   CDP,CN=Public Key
   Services,CN=Services,<ConfigurationContainer><CDPObjectClass>
   http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAl
   lowed>.crl
   file://\\<ServerDNSName>\CertEnroll\<CaName><CRLNameSuffix><DeltaCRL
   Allowed>.crl
   ```

3. Make sure that only the following attributes are enabled for the extensions:

   - C:\Windows…
     - Publish CRLs to this location
     - Publish Delta CRLs to this location
   - ldap:///...
     - Publish CRLs to this location
     - Publish Delta CRLs to this location
   - http://...
     - No attributes
   - File://\\..
     - No attributes

Note: These are the default extensions. The only important that you really need if the default LDAP URL, which allows the Microsoft CA to publish the CRL to the Active Directory. The reason the other extensions arent included in published certificates is that the Certificate authentication agent will only use the first address listed in the certificate.

You now need to add a new extension which will be used as the CRLDP by the Certificate authentication agent.

1. Click the Add button, and paste the following into the Location field:

   ```
   ldap://hostname/ipaddress:389/CN=<CATruncatedName><CRLNameSuffix>,CN
   =<ServerShortName>,CN=CDP,CN=Public Key
   Services,CN=Services,<ConfigurationContainer>
   ```

   Alternatively, you can also use the following LDAP URL:

   ```
   ldap://hostname/ipaddress:389/CN=<CATruncatedName><CRLNameSuffix>,CN=
   <ServerShortName>,CN=CDP,CN=Public Key
   Services,CN=Services,<ConfigurationContainer>
   ?certificateRevocationList?base?(objectClass=cRLDistributionPoint)
   ```

2. Click the OK button to add the new LDAP URL. Select the new LDAP CRLDP from the extension list and enable the following attribute for the new extension. Enable to following attributes:

   - Include in all CRLs
   - Include in CRLs
   - Include in the CDP extension

   Note: These should be the only attributes available for the new LDAP URL.

3. Click OK and then Yes when asked to restart the Certificate service.

4. Right-click on the Revoked Certificates node in the Certification Authority tab and select All Tasks \ Publish. The will generate a new CRL.

5. You will now need to reissue the user certificates, so that they include the new CRLDP location. Issue a test certificate and check that the correct LDAP URL is included in the CRLDP extension in the certificate.

Step 6: Configuring the Certificate authentication agent to Use CRLDP to Find Revocation Status of User Certificates

To use the CRLDP address in the user certificates, the Certificate authentication agent must be configured correctly. Open the registry editor and navigate to the following registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sso_tga_cert_Agent
1\Parameters\sso_tga_cert_Agent1
```

To use the CRLDP revocation method the following values need to be configured:

- AuthHostName
- CrlDPIssuerCertPath
- CrlDPIssuerCerts
- CrlDPTimeOut
- CrlPollInterval
- RevocationMeth
- TrustedCertNames
- TrustedCertPath

Configuration Settings for the Certificate Authentication Agent

This section lists the settings you can configure in the Certificate authentication agent. All of these settings may be edited, but you must restart the eTrust SSO – Certificate authentication agent Windows service for the changes to take effect.

The settings for the Certificate authentication agent are found below the following Windows Registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sso_tga_cert_Agent1\Paramete
rs\sso_tga_cert_Agent1
```

The following table lists the configurable settings:

Keyname	Description	Default Value
AuthHostName	The name of the authentication host that is included in the SSO ticket. If you leave this blank, the computer name of the authentication host will be used (this is the legacy behavior from SSO 7.0 and earlier). A default authentication host entry, CERT_Authhost, is created by default during the Policy Server installation. It is associated with ps-ldap user datastore and has a randomly-generated encryption key (see TicketKey configuration option further below) value assigned to it.	CERT_Authhost
ChildLimit	Determines the number of worker threads that get created for dealing with incoming client requests.	3
CrlDPIssuerCertPath	Path to the directory where the CRL issuer certificates for CRLDP revocation checking are stored.	
CrlDPIssuerCerts	Comma separated file name list of the CRL issuer certificates that are in the directory specified by the value of CrlDPIssuerCertPath.	
CrlDPTimeOut	How long to try for when retrieving a CRL (in seconds).	60
CrlFileName	Location of the DER-encoded CRL file. It can be a HTTP web address or a LDAP directory entry both in URL format, or a local file or a file located on a network drive. When specifying a local file or a file on a network drive, both direct path and the URL format can be used.	
CrlIssuerCert	Path and name of the DER-encoded CRL issuer certificate file.	

Keyname	Description	Default Value
CrlPollInterval	The time interval in seconds between each poll for new updates of CRL. ■ If the CRL is up to date: - and CrlPollInterval is 0, then no polling of CRL file will take place until the next update due attribute of the CRL file is reached. - and CrlPollInterval is greater than 0, then polling will take place during that interval. ■ If the CRL is out of date: - and the CrlPollInterval is 0 or greater than 15, then polling will take place at 15 second intervals. - and the CrlPollInterval is between 1-14 inclusive, then polling will take place during that interval.	0
HttpProxy	The proxy name through which the OCSP request is sent and/or the CRL is retrieved over HTTP.	
IdleFreq	Idle frequency, in calls per second.	20
ListenQueSize	Determines the maximum length of the queue of pending connections. If a connection request arrives and the queue is full, the client will receive an error response. You can increase this value if the Ticket Granting Agent (TGA) is unable to process the incoming authentication requests (from SSO Client) fast enough, with communication-related error messages being generated.	5
OcspResponder	The URL of the OCSP responder.	
OcspSignCert	The full path name of the certificate that will be used to sign requests sent to OCSP Responder. This must be in pkcs12 format.	
OcspSignCertPass	Defines the password for OcspSignCert.	
PortNumber	Port number on which the TGA is listening for client requests.	13987
RecvBuffSize	Length of the buffer used when receiving the data (in bytes).	131072 (128 KB)

Keyname	Description	Default Value
RevocationMeth	Defines a revocation method used for certificates validation. When the method is specified it can have the following values: FIXED_OCSP, AIA_OCSP, CRL, FIXED_OCSP+CRL, AIA_OCSP+CRL, CRLDP, CRLDP+CRL	
SendBuffSize	Length of the buffer used when sending the data (in bytes).	131072 (128 KB)
TicketKey	Key used to encrypt the ticket that is created by the TGA (after successful authentication) and sent to the SSO client. The value of this option must correspond to the encryption key value associated with the authentication host entry on the Policy Server that corresponds to the value of AuthHostName configuration option (see earlier in this table).	-
TimeOutConnect	Connection time-out value (in seconds).	60
TimeOutRecv	Receive time-out value (in seconds).	60
TimeOutSend	Send time-out value (in seconds).	30
TrustedCertNames	A list of DER-encoded certificate file names that are in the directory defined by TrustedCertPath. The names must be separated by comma.	
TrustedCertPath	The directory where trusted certificates can be found.	
VerifyDepth	The maximum depth of the verification chain. If this is empty, it will be set to 2. The value of this depth will affect the checking of the certificates in the trusted set. If you want the verification and checking of expiration of all the certificates in the chain, you need to specify a big enough value here and include the self signed root certificate in the trusted set. For example, if you have a certification chain comprised of ROOT, CA and END_ENTITY, you need to set this value to 2 or more to make the verification on CA and END_ENTITY, and the expiration checking on all certificates in the chain to happen.	2

Starting the Certificate Agent Service Manually

When the service is running, the Certificate agent is ready to accept authorization queries from the eTrust SSO Client.

When you restart the Certificate agent computer, the Certificate authentication agent Windows service starts automatically.

To start the service manually, follow these steps:

1. Go to the Control Panel and select Settings, Administrative Tools, Services.
2. Find the 'eTrust SSO - Certificate authentication agent – Agent 1' in the list and right-click and select Start.

Implementing the Entrust Authentication Agent

eTrust SSO supports primary authentication with Entrust, which is a public key infrastructure developed by Entrust Technologies Limited. eTrust SSO can use Entrust's digital signing and digital signature verification capabilities to confirm the end user's identity.

You can create user aliases for the users who use the Entrust authentication method. This lets you manage those users by their short names instead of their X.500 names. For more information about creating user aliases, see the *eTrust SSO Command Reference Guide*.

Before You Begin

The Before You Begin Section is designed to guide you through what you need to know before you install the Entrust authentication agent. In addition to the information in this section, always make sure you review your implementation plan and take note of any specific requirements.

Understand the Components Used in the Entrust Authentication Process

The setup process involves the following components that take part in eTrust SSO primary authentication with Entrust:

Entrust server
The computer that the Entrust Directory Server resides on.

Authentication agent server
The computer on which the Entrust authentication agent is installed

SSO Client
Installed on the end-user workstation.

Policy Server
Accessed by the SSO Administrator using the Policy Manager or via selang.

Components Installed on the SSO Client

When it is configured for Entrust primary authentication, the SSO Client contains the following components in addition to the standard files:

- The eTrust SSO Open Authentication Engine (OAE) for Entrust.
- The eTrust OAE GUI for Entrust, which displays a dialog box for user authentication.
- The Entrust INI file (this is a standard Entrust file and should be copied from the Entrust server).
- The Entrust EPF files (these user profile files are standard Entrust files and should be copied from the Entrust server)

Components Installed on the Entrust Authentication Agent Server

A properly configured authentication agent server contains:

- The executable for the Entrust authentication agent for eTrust SSO (this is the ticket granting agent, or TGA)
- The Entrust INI file (this is a standard Entrust file and should be copied from the Entrust server)
- The Entrust EPF files (these user profile files are standard Entrust files and should be copied from the Entrust server)

Entrust can function in either of two modes: Entrust Lite or Entrust Full. eTrust SSO supports both modes, by using the EntrustFile APIs.

Prepare the Entrust Server Computer

1. Log on to the Entrust server computer as an administrator.

2. Insert the Entrust CD into the CD ROM drive.

3. Select and install Entrust/PKI Documentation.

4. If the computer runs Windows XP, install Update MDAC (Microsoft Data Access).

5. After familiarizing yourself with the documentation to make sure your computer satisfies minimum system requirements, install the Informix component.

6. During the Informix installation, if you encounter a Possible Problem Using Current Account pop-up window, informing you that the current user account was created with upper-case characters, click the Yes button.

7. When prompted in a Select Drive For Database window to select the drive that will host the ifmxdata directory, choose a drive letter from the pull-down menu. Entrust components should be located on the same drive as eTrust Directory files.

6. Install the latest JRE (Java Runtime Environment) if it is not already installed.

7. Install a directory of your choice, if one is not configured already. You can use eTrust Directory, which is installed on the Policy Server computer.

Configure eTrust Directory to work with Entrust

The following instructions assume that you have installed eTrust Directory, and that you are working with the sample directory, Democorp.

1. Open the directory configuration file \schema\x500.dxc file. This is usually located at:

   ```
   C:\Program Files\CA\eTrustDirectory\dxserver\config\schema
   ```

2. Check that the DXC file contains definitions for the pmiUser object class and the attributeCertificateAttribute attribute.
   If this class and attribute are not defined, use the Entrust documentation and website to update your directory schema.

3. In the same directory, find the default.dxg file and add the following line if it is not already in the file:

   ```
   source “entrust.dxc”;
   ```

4. Open the command prompt and run the following command to check that Democorp is running:

   ```
   dxserver status
   ```

5. Run the following command to reload the configuration settings:

   ```
   dxserver init democorp
   ```

6. Click Start, Programs, eTrust Directory, JXplorer to open JXplorer.
7. In JXplorer, connect to the sample directory DEMOCORP, and create a new entry at the top level:
   a. Set the RDN to ou=Authority.
   b. Include the following classes: organizationalUnit and entrustCA.
   c. Enter a password in the userPassword field.
8. In the newly created Authority level, create another new entry:
   a. Set the RDN to cn=Administrator.
   b. Include the following classes: inetOrgPerson and entrustUser.
   c. Set the sn to Administrator.
   d. Enter a password in the userPassword field.
9. Insert the Entrust CD into the CDROM drive, and install the Entrust Authority component. This option is initially disabled, because Informix needs to be present on the system before the Entrust Authority database can be created. Entrust Authority must be installed on a Windows 2000 server.
10. Use the default locations for the Entrust/Authority data files and backup files (for example, use c:\authdata and c:\entbackup).

    These directories will be referred to as ENT_AUTH_DATA_DIR and ENT_AUTH_BACKUP_DIR for the rest of these instructions.

11. In the Directory Node and Port dialog, use the default value for Directory Node Name, but enter 19389 as a value for Directory Listen Port. That is the port number used to connect to Democorp, and the Certification Authority was created under o=DEMOCORP.

12. You'll be prompted to enter the Certification Authority distinguished name, the CA Directory Access password, the Directory Administrator distinguished name and the Directory Access password: the DN and password values should correspond to those of the Authority and Administrator entries created in the Configure eTrust Directory to Work with Entrust section.

13. To enter the Directory Administrator's distinguished name, open JXplorer and right-click on the newly created Administrator under the authority tree. Click Copy Node and paste this into the configuration utility.

    If any errors are reported in the log produced by *Entrust Directory Verification Tool*, make sure they are analyzed and addressed before proceeding with the installation.

14. Use the default values specified in Advanced Directory Attributes' window, and throughout the rest of the utility execution.

15. In the Setup Complete window, check the box to run the Entrust/Configuration utility, and click the Finish button.

16. In the Configuration Complete' window, tick the box to run Entrust/Master Control, before clicking on the *OK* button.

17. In the Entrust/Authority Master Control' dialog, click *Login* button, and enter passwords for three Master Users and the First Officer. Make sure you remember the password values or note them down, because you will be required to use them throughout Entrust authentication tests.

18. After Entrust/Authority installation is completed (Entrust Master Control and Entrust RA components are available in Start->Programs->Entrust PKI), edit the entrust.ini file in the [ENT_AUTH_DATA_DIR]\manager (e.g. c:\authdata\manager\) directory and comment out the entire [FIPS Mode] section. Failure to do so will result in inability to start Entrust authentication agent (tgaents.exe) later on.

19. Create one Entrust user in the Entrust database for each eTrust SSO user that will authenticate to eTrust SSO using Entrust.

Create an Entrust User and Profile

1. Ensure Entrust/Authority service is running, by either checking Services list (Start->Settings->Control Panel->Administrative Tools->Services) or running Entrust/Master Control.

2. Open Entrust/RA (from Start->Programs->Entrust PKI)

3. Enter the First Officer password you created in the Configure eTrust Directory to Work with Entrust section.

4. Right-click on Users, and select the New User option.

5. Fill in the First Name and Last Name fields, and check the Create Profile box and click OK.

6. Enter a profile name and password, and verify the user creation request with First Officer's password.

Configure the SSO Client

This section explains what changes you need to make to the SsoClnt.ini file on the SSO Client computer to configure Entrust authentication:

1. Edit the SsoClnt.ini file to include ENTS as one of the authentication methods, preferably the first method in the list. For example:

   ```
   [ServerSet0]
   AuthMethods=ENTS
   authCERT=Server1:13987
   ```

   The port number is optional. If the port number is not specified, the default port (13987) is used.

2. Specify the values of the other settings associated with Entrust authentication in the [auth.ENTS] section of the SsoClnt.ini file.

   For more information about the SsoClnt.ini file settings, see the "Configuring the SsoClnt.ini File" appendix in the *eTrust SSO Administrator Guide.*

3. Obtain the following files from your Entrust software provider and copy them into the SSO Client installation directory:

   - entapi32.dll
   - enterr.dll
   - etfile32.dll

Install the Entrust Authentication Agent

This section explains how to install the Entrust authentication agent, and how to start it once it has been installed.

Wizard Installation

To install the Entrust authentication agent, follow these steps:

1. From the eTrust Single Sign-On 8.0 Product Explorer wizard expand the eTrust Single Sign-On authentication agents folder, and select Entrust authentication agent.

   The wizard should appear automatically when you insert the eTrust SSO disk. If not, open Windows Explorer and navigate to the CD-ROM directory and double-click the PE_i386.exe file.

   The Install button becomes active.

2. Click Install and accept the license agreement.

   The Destination Folder dialog appears.

3. Change the installation folder or click Next to accept the default.

   The Entrust Configuration Files dialog appears.

4. Specify the location of the entrust.ini file, or a copy of this file on the Entrust authentication agent server computer. This should be located in the following directory:

   ```
   [ENT_AUTH_DATA_DIR]\manager\
   ```

5. Specify a path to the Entrust Profile file, or a copy of this file on the Entrust authentication agent server computer. The file should be one of the .epf files in the following directory:

   ```
   [ENT_AUTH_DATA_DIR]\manager\epf directory
   ```

   This must be a valid user, since it acts like a personality in SSO but there is no importance to who this user is.

6. Enter and confirm a password to use with Entrust, then click Next.

7. In the Additional Information dialog, enter the name of the Authentication Host entry on the Policy Server, and the value of the encryption key associated with it. By default, the Policy Server installation creates a ENTS_Authhost entry with a randomly-generated key value. Depending on your desired setup, you have a choice of either using the details of this Authentication Host entry or creating and configuring a new one.

8. Click Next and then Install to complete the installation.

9. Obtain the following files from your Entrust software provider and copy them into the Entrust authentication agent installation directory:

- entapi32.dll
- enterr.dll
- etfile32.dll

Silent Installation

To install the authentication agent using the silent installation, follow these steps:

1. Open a command prompt and navigate to the Authentication Agent folder on the eTrust SSO CD.
2. From the command prompt, enter:

   ```
   setup.exe /s /v"/qn <insert variables here>"
   ```

   For information about what values you can specify, see the Command Line Settings section in this chapter.

   Note: In order to execute a silent installation you have to accept the license agreement. The setting required for accepting the license agreement and silently installing the authentication agent can be found at the bottom of the license agreement available when running the installation wizard.

Command Line Settings

The command line settings for installing an authentication agent are:

Setting	Description
/s	Hides the initialization dialog.
/v	Passes parameters and property settings to the installation. It applies to all the parameters and properties listed in this table except /s. Place any parameters you wish to pass to the installation within quotes ("").
/L	Defines the full path and name of the installation log file. Use the mask * to log all available information. For example: `/L* C:\log.txt`

Setting	Description
/qn	In conjunction with the /s parameter, used to initiate a silent installation. **Note:** You need to use the *license_accept* property to execute a silent installation.
license_accept	*license_accept* is the setting required for accepting the license agreement and silently installing the authentication agent. The actual setting you need to use can be found at the bottom of the license agreement that is available when running the installation wizard.
INSTALLDIR=[location]	Specifies the location where the authentication agent will be installed.
ENTSINIFILE	Specifies the location of the Entrust.ini file
ENTSPROFILE	Specifies the location of the profile file
ENTSPWD	Specifies the Entrust password.
AUTHHOSTNAME	Specifies the authentication host in the Policy Server for this agent type.
ENTSKEY	Specifies the encryption key for the authentication host.

Post Installation Configurations

This section explains what you need to do after you have installed the Entrust authentication agent.

Configuration Settings for the Entrust Authentication Agent

This section lists the settings you can configure in the Entrust authentication agent. All of these settings may be edited, but you must restart the eTrust SSO – Entrust authentication agent Windows service for the changes to take effect.

The settings for the Certificate authentication agent are found below the following Windows Registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sso_tga_ents_Agent1\Paramete
rs\sso_tga_ents_Agent1
```

The following table lists the configurable settings:

Keyname	Description	Default Value
AuthHostName	The name of the authentication host that is included in the SSO ticket. If you leave this blank, the computer name of the authentication host will be used (this is the legacy behavior from SSO 7.0 and earlier). A default authentication host entry, ENTS_Authhost, is created by default during the Policy Server installation. It is associated with ps-ldap user datastore and has a randomly-generated encryption key (see TicketKey configuration option further below) value assigned to it.	ENTS_Authhost
ChildLimit	Determines the number of worker threads that get created for dealing with incoming client requests.	3
EntrustIniFile	The absolute path to the Entrust INI file	
EntrustPassword	Password to the EntrustProfile	
EntrustProfile	The absolute path to the Entrust EPF file	
IdleFreq	Idle frequency, in calls/second.	20
ListenQueSize	The value of this configuration option determines the maximum length of the queue of pending connections. If a connection request arrives and the queue is full, the client will receive an error response. This value can be increased if the Ticket Granting Agent (TGA) is unable to process the incoming authentication requests (from SSO Client) fast enough, with communication-related error messages being generated.	5

Keyname	Description	Default Value
PortNumber	Port number on which the TGA is listening for client requests.	13987
RecvBuffSize	Length of the buffer used when receiving the data (in bytes).	131072 (128 KB)
SendBuffSize	Length of the buffer used when sending the data (in bytes).	131072 (128 KB)
TicketKey	Key used to encrypt the ticket that is created by the TGA (after successful authentication) and sent to the SSO client. The value of this option must correspond to the encryption key value associated with the Auth Host entry on the Policy Server that corresponds to the value of AuthHostName configuration option (see earlier in this table).	-
TimeOutConnect	Connection time-out value (in seconds).	60
TimeOutRecv	Receive time-out value (in seconds).	60
TimeOutSend	Send time-out value (in seconds).	30
UserNamePrefix	The text before the user name that will not be put in the SSO ticket during authentication. For example, set the UserNamePrefix to **cn=** to remove the first three characters from the following DN: `cn=Juanita Perez, ou=CompanyName` This option can be useful if the type of the user datastore on the Policy Server does not correspond with the user datastore used during authentication. For example, authenticating using credentials of a user from eTrust Directory and then verifying the ticket against a user in Access Control-type data store.	
UserNameSuffix	The text after the user name that will not be put in the SSO ticket during authentication. For example, set the UserNameSuffix to **, ou=CompanyName** to remove the last sixteen characters from the following DN: `cn=Juanita Perez, ou=CompanyName` See comment for UserNamePrefix option above for more detail.	-

Starting the Entrust Agent Service Manually

When the service is running, the Entrust agent is ready to accept authorization queries from the eTrust SSO Client.

When you restart the Entrust agent server computer, the Entrust authentication agent Windows service starts automatically.

To start the service manually, follow these steps:

1. Go to the Control Panel and select Settings, Administrative Tools, Services.
2. Find the ‘eTrust SSO – Entrust authentication agent – Agent 1’ in the list and right-click and select Start.

Implementing the LDAP Authentication Agent

eTrust SSO supports primary authentication to user stores which are LDAP compliant. For example, Microsoft Active Directory, and Novell eDirectory. This section explains how to install the LDAP authentication agent.

Before You Begin

The Before You Begin Section is designed to guide you through what you need to know before you install the LDAP authentication agent. In addition to the information in this section, always make sure you review your implementation plan and take note of any specific requirements.

Create Users in an LDAP User Data Store

Create (if necessary) an LDAP-based user data store on the Policy Server, and ensure that the desired users are defined in the directory associated with it. The examples in this chapter are using ps-ldap data store that is created by default during Policy Server installation.

1. Install the Policy Server and the Policy Manager, as described in this guide.
2. Open the Policy Manager.
3. Create two new users in the ps-ldap data store.

   Admin
   You will use this user to configure the LDAP authentication agent.

   LDAPuser
   You will use this user account to test the LDAP authentication method.
4. For both users, assign the LDAP authentication method, and set a password for the LDAP authentication method.
5. Click Resources, Single Sign-On Resources, Data Stores, User Data Stores, right-click the ps-ldap user data store and select Properties.
6. Note the following properties of the ps-ldap data store:
   - Base Path
   - Port Number

In this example we will use these properties to configure the LDAP authentication agent for binding to the Policy Server

Install the LDAP Authentication Agent

To install the LDAP authentication agent you must install the necessary files and then install and start the LDAP authentication agent service.

This section explains how to install the LDAP authentication agent, and how to start it once it has been installed.

Wizard Installation

To install the LDAP authentication agent, follow these steps:

1. From the eTrust Single Sign-On 8.0 Product Explorer wizard expand the eTrust Single Sign-On authentication agents folder, and select LDAP authentication agent.

   The wizard should appear automatically when you insert the eTrust SSO disk. If not, open Windows Explorer and navigate to the CD-ROM directory and double-click the PE_i386.exe file.

   The Install button becomes active.

2. Click Install and accept the license agreement.

   The Destination Folder dialog appears.

3. Change the installation folder or click Next to accept the default.

   The Authentication dialog appears.

4. Enter the following information:

   – The name of the computer where you have the user directory.

     If you want to use eTrust Directory, this is the name of the Policy Server computer where eTrust Directory is installed by default.

   – The port number of the computer where you have the user directory.

     For eTrust Directory, this is 13389.

   – The format string, used to construct the DN of the user in the LDAP data store.
     For eTrust Directory for example, use the common name (cn) as the attribute for identifying a user. Enter:

     ```
     cn=%s, <base_path>
     ```

     where <*base_path*> is the base path you noted when you created users in the LDAP user data store.

5. On the Credentials for Initial Bind dialog, enter the following information:
   - The DN of the Admin user you created previously.
   - The password of the Admin user.
6. On the Additional Information dialog, enter the name of the Authentication Host entry on the Policy Server, and the value of the encryption key associated with it. By default, the Policy Server installation creates a LDAP_Authhost entry with a randomly-generated key value. Depending on your desired setup, you have a choice of either using the details of this Authentication Host entry or creating and configuring a new one.
7. Click Next and then Install to complete the installation.

Silent Installation

To install the authentication agent using the silent installation, follow these steps:

1. Open a command prompt and navigate to the Authentication Agent folder on the eTrust SSO CD.
2. From the command prompt, enter:

   ```
   setup.exe /s /v"/qn <insert variables here>"
   ```

   For information about what values you can specify, see the Command Line Settings section in this chapter.

   Note: In order to execute a silent installation you have to accept the license agreement. The setting required for accepting the license agreement and silently installing the authentication agent can be found at the bottom of the license agreement available when running the installation wizard.

Command Line Settings

The command line settings for installing an authentication agent are:

Setting	Description
/s	Hides the initialization dialog.
/v	Passes parameters and property settings to the installation. It applies to all the parameters and properties listed in this table except /s. Place any parameters you wish to pass to the installation within quotes ("").
/L	Defines the full path and name of the installation log file. Use the mask * to log all available information. For example: `/L* C:\log.txt`
/qn	In conjunction with the /s parameter, used to initiate a silent installation. **Note:** You need to use the *license_accept* property to execute a silent installation.
license_accept	*license_accept* is the setting required for accepting the license agreement and silently installing the authentication agent. The actual setting you need to use can be found at the bottom of the license agreement that is available when running the installation wizard.
INSTALLDIR=[location]	Specifies the location where the authentication agent will be installed.
LDAPHOST	Specifies the directory computer name.
LDAPPORT	Specifies the TCP/IP address of the directory
STATICNAME	Specifies the DN of the user repository.
PRIMARIES_NAME	Logon name for the initial bind.
PRIMARIES_PASSWORD	Logon password for the initial bind.
AUTHHOSTNAME	Specifies the authentication host in the Policy Server for this agent type.
ENCRYPTIONKEYVALUE	Specifies the encryption key for that authentication host.

Post Installation Configurations

The following sections explain what you need to do after you have installed the LDAP authentication agent.

Configuration Settings for the LDAP Authentication Agent

This section lists the settings you can configure in the LDAP authentication agent. All of these settings may be edited, but you must restart the eTrust SSO – LDAP authentication agent Windows service for the changes to take effect.

The settings for the LDAP authentication agent are found below the following Windows Registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sso_tga_ldap_Agent1\Paramete
rs\sso_tga_ldap_Agent1
```

The following table lists the configurable settings:

Keyname	Description	Default Value
AuthHostName	The name of the authentication host that is included in the SSO ticket. If you leave this blank, the computer name of the authentication host will be used (this is the legacy behavior from SSO 7.0 and earlier). A default authentication host entry, LDAP_Authhost, is created by default during the Policy Server installation. It is associated with ps-ldap user datastore and has a randomly-generated encryption key (see TicketKey configuration option further below) value assigned to it.	LDAP_Authhost
AuthMethod	Method used for LDAP authentication. Possible value are 'Compare' (see description of IdAttribute option further below, for details) and 'Bind' (default). When 'Bind' method is used, LDAP authentication agent verifies the validity of the provided credentials using bind attempt. Bind can be used regardless of LDAP server platform but it can take much more time than Compare. In certain cases Bind will be a method of choice, simply because of the directory restrictions. For example, in Active Directory the 'userpassword' attribute is read-only, and is not suitable for use with 'Compare' LDAP authentication method.	Bind
ChildLimit	Determines the number of worker threads that get created for dealing with incoming client requests.	3

Keyname	Description	Default Value
ConnectionLifetime	The maximum time in seconds that the connection made by the LDAP authentication agent to the LDAP authentication server is maintained. If the information needed by the agent is obtained before this period elapses, the agent terminates the connection.	3600
IdAttribute	If AuthMethod is 'Compare', compare the value of this attribute of the user, with the value entered in the password field in the LDAP authentication dialog.	
IdleFreq	Idle frequency, in calls/second.	20
ListenQueSize	The value of this configuration option determines the maximum length of the queue of pending connections. If a connection request arrives and the queue is full, the client will receive an error response. This value can be increased if the Ticket Granting Agent (TGA) is unable to process the incoming authentication requests (from SSO Client) fast enough, with communication-related error messages being generated.	5
MaxConnections	The maximum number of connections that will be allowed to be opened to the group (pool) of LDAP authentication servers defined in tga_ldapPolicy.ini.	10
OfflineTimeout	The time (in seconds) for which the LDAP authentication server stays marked as offline after the LDAP authentication agent fails to communicate with it.	120
PolicyFilePath	Path to the tga_ldapPolicy.ini file	C:Program Files\CA\eTrust SSO\LDAP Agent\tga_ldapPolicy.ini
PortNumber	Port number on which the TGA is listening for client requests.	17979
StandbyConnections	The minimum number of connections to the group (pool) of LDAP authentication servers (defined in tga_ldapPolicy.ini) The number of connections maintained in the pool is kept within the range of StandbyConnections and MaxConnections. A minimum number of standby connections is maintained, and increased to the maximum number as required. When reducing the number of connections (due to not having been used recently) the standby is used as the minimum.	5

Keyname	Description	Default Value
TicketKey	Key used to encrypt the ticket that is created by the TGA (after successful authentication) and sent to the SSO client. The value of this option must correspond to the encryption key value associated with the Auth Host entry on the Policy Server that corresponds to the value of AuthHostName configuration option (see earlier in this table).	
TimeOutConnect	Connection time-out value (in seconds).	60
TimeOutRecv	Receive time-out value (in seconds).	60
TimeOutSend	Send time-out value (in seconds).	30
UserNamePrefix	The text before the user name that will not be put in the SSO ticket during authentication. For example, set the UserNamePrefix to **cn=** to remove the first three characters from the following DN: `cn=Juanita Perez, ou=CompanyName` This option can be useful if the type of the user datastore on the Policy Server does not correspond with the user datastore used during authentication. For example, authenticating using credentials of a user from eTrust Directory and then verifying the ticket against a user in Access Control-type data store.	
UserNameSuffix	The text after the user name that will not be put in the SSO ticket during authentication. For example, set the UserNameSuffix to **, ou=CompanyName** to remove the last sixteen characters from the following DN: `cn=Juanita Perez, ou=CompanyName` See comment for UserNamePrefix option above for more detail. UserNamePrefix and UserNameSuffix configuration parameters can both be omitted, in which case user’s entire distinguished name (DN) will be stored in the ticket generated by the LDAP authentication agent.	

tga_ldapPolicy.ini file Settings

The following settings can be configured in tga_ldapPolicy.ini file that gets installed to the same directory as the LDAP authentication agent Windows service executable.

NameMapping

One or more name mappings must be defined, contained in sections named [NameMapping<index>], with the first index value being 0 and consequent ones being in increments of 1. If you have sections [NameMapping0] and [NameMapping7], the latter won't be read in or used.

The configuration tokens that make up the NameMapping section are:

Name	Description
NameMapping	The method for mapping a User Name entered in the LDAP authentication dialog to LDAP user distinguished name (DN). Select one of two possible values: 1. Substitution 2. Search
StaticName	A format specifier string used to construct the distinguished name (DN) of the user, given the value entered by the user in the authentication dialog. The format string should generally be of the form: <attribute name>=%s,<the remainder of the user distinguished name value>. **Note:** Only if NameMapping=Substitution.
BaseDN	The Base DN for the LDAP search. **Note:** Only if NameMapping=Search
Filter	A filter for the LDAP search, that usually takes the form of the format specifier string <attribute name>=%s. Filter needs to be designed in such a way so that it could be used to uniquely identify a user below a base DN (see BaseDN parameter above). **Note:** Only if NameMapping=Search
Scope	The scope for the LDAP search if the NameMapping type 'Search' is used. Select one of three possible values: 1. Subtree 2. OneLevel 3. Object **Note:** Only if NameMapping=Search

While selecting the method for *name mapping*, consider that *search,* although is more flexible than *substitution,* can also be much more time consuming.

Primaries and Secondaries

LDAP authentication agent will be able to distribute processing between LDAP servers. The Administrator will be able to define two groups of LDAP servers: *Primary* and *Secondary*. LDAP authentication agent will always try to bind to the servers from the *Primary* group first and only if all of them are not available (or not responding), it will bind to the servers from the *Secondary* group.

Within each group of servers, LDAP server definitions consist of two parts:

- `LDAPHost<index>=<hostname>[<port number>][/bias_value]`

  with the first index value being 0 and consequent ones in increments of 1.

  Port number and bias value are optional, with the default values being 389 and 100 respectively. Bias value can be used to configure load-balancing between the servers within the group (i.e. LDAP server with a bias value of 50 is half-as likely to be chosen when decision is made to which server to connect).

- `[<group name>.LDAPHost<index>]`

  a section containing the details required for the initial administrative bind, when a connection to the server is established for the first time.

  For example, if you have LDAPHost3=somecomputer:13389/150 in the [Primaries] section, you'll need to introduce a [Primaries.LDAPHost3] section, consisting of the following tokens:

Name	Description
AuthenticationLevel	Defines the authentication type used for binding to the LDAP server. Select one of three possible values: 1. Anonymous 2. Simple 3. SSL
LoginName	Defines the fully qualified distinguished name (DN) of a user with administrative privileges, defined on the LDAP server, for non-Anonymous authentication. **Note:** Only if AuthenticationLevel=Simple
Password	Defines the password for the user whose DN was specified via LoginName configuration (see above), for non-Anonymous authentication. **Note:** Only if AuthenticationLevel=Simple

Name	Description
Keystore	Defines a full path of the store containing Agent certificate for SSL communication. **Note:** Only if AuthenticationLevel=SSL

Note: At least one LDAP server must be defined in the *Primaries* group, in order for the LDAP authentication agent to initialize successfully.

If any of the parameters required for non-*Anonymous* authentication are missing, LDAP authentication agent will try to use anonymous authentication while binding to LDAP Server. If any of the parameters required for SSL communication are missing, the LDAP authentication agent will try to communicate with the LDAP Server using clear text communication.

Implementing the NetWare Authentication Agent

eTrust SSO supports primary authentication to Novell Netware.

Before You Begin

The Before You Begin Section is designed to guide you through what you need to know before you install the Netware authentication agent. In addition to the information in this section, always make sure you review your implementation plan and take note of any specific requirements.

Install the NetWare Client

1. Make sure that the Novell NetWare client for Windows is already installed on the client workstation.

   This is because you will need to copy Novell agent files onto the NetWare server.

2. In the NetWare client, select Properties, Advanced Settings, then set the Station Time to off.

   This stops the time synchronization between the client computer and the NetWare server.

Configure the SSO Client

This section explains what changes you need to make to the SsoClnt.ini file on the SSO Client computer to configure Novell authentication:

1. Edit the SsoClnt.ini file to include NOVELL as one of the authentication methods, preferably the first method in the list. For example:

   ```
   [ServerSet0]
   AuthMethods=NOVELL
   ```

2. Edit the SsoClnt.ini to include the name of the NetWare authentication host in the auth agent keyname. For example:

   ```
   [Serverset0]
   AuthNOVELL=server1
   ```

For more information about the SsoClnt.ini file settings, see the “Configuring the SsoClnt.ini File” appendix in the *eTrust SSO Administrator Guide.*

Install the NetWare Authentication Agent

This section explains how to install the NetWare authentication agent, and how to start it once it has been installed.

Wizard Installation

You need to install the NetWare authentication agent on a Novell server on the network. To install the Netware authentication agent, follow these steps:

1. Open Windows Explorer and navigate to the CD-ROM drive and locate the /Agents/AuthNW folder.
2. Locate the following three files:
   - **ssoauth.nlm**—The NetWare authentication agent module.
   - **ssoauth.dat**—Contains the NetWare authentication agent key.
   - **ssoauth.ini**—The NetWare authentication agent configuration file.
3. Copy these files into the SYSTEM directory of the NetWare server.

   If this is not possible, copy the file into any other directory on the NetWare server, and specify the path to this file when you load the module, and ensure that the configuration file ssoauth.ini contains the correct paths to the agent files.

Note: To complete the installation and allow the NetWare authentication agent to work with eTrust SSO, you need to configure the installation files. See the Post Installation Configurations section below.

Post Installation Configurations

This section explains what you need to do after you have installed the NetWare authentication agent.

Create an Authentication Host Entry on the Policy Server

You only need to do this if you decide to use a different authentication host to the default created as part with the Policy Server installation (NOVELL_Authhost). For information on defining an authentication host, see the "Managing Resources" chapter in the *eTrust SSO Administrator Guide*.

Configure the NetWare authentication agent

To configure the NetWare authentication agent, follow these steps:

1. Log on to the Novell Client to access the NetWare file system from Windows. Refer to www.novell.com for information about using the Novell Client.
2. In Windows Explorer, right-click on the copied files, select Properties, and clear the read-only attribute. The files should now be found in the SYSTEM directory of the NetWare server.
3. Open the ssoauth.dat in a text editor and change the default key used for encryption to correspond to the Policy Server authentication host entry you want to use. By default, the Policy Server installation creates a NOVELL_Authhost entry with a randomly-generated key value.
4. Add the agent (ssoauth.nlm) to the list in autoexec.ncf to start the agent automatically when the system is rebooted.
5. Start the NetWare authentication agent manually:

   ```
   NW_server : load ssoauth
   ```

6. In the Netware authentication agent screen, select the Configuration option in the Available Options section.

4. Set the following parameters in the configuration dialog:

Setting	Values
Use external NCP IN	Yes No (this is the default)
NCP ID	0
Provide Windows support	Yes (this is the default) No
Key Location	SYS:SYSTEM/SSOAUTH.DAT
Trace file name	SYS:SYSTEM/SSOTRACE.DAT
Trace file size	4K
Trace auto-backup	Yes
Trace file backup name	SYS:SYSTEM/SSOBCK.LOG
Use NDS user name	Yes No
User name case	**As defined in NetWare**—The NetWare agent recognizes the case that the administrator defines for the user in the database (default). **Lower case only**—The NetWare agent recognizes only lower-case letters in user names. **Upper case only**—The NetWare agent recognizes only upper-case letters in user names.

Allow Users to Access the Authentication Host

You need to update the eTrust SSO user records so that users can use the NetWare authentication method.

View the NetWare Authentication Agent Trace Log

The file ssotrace.log is the NetWare authentication agent's trace and activity log.

The SSO NetWare agent writes to this file, but if the agent doesn’t find an ssotrace.log file, it opens a new one in the designated directory.

To view trace log of the SSO NetWare agent, select Activity Log and choose current log or backup log. The activity log window shows a list of agent-related activities.

Implementing the RSA Authentication Agent

eTrust SSO supports primary authentication with RSA SecurID, a product developed by RSA.

Before You Begin

The Before You Begin Section is designed to guide you through what you need to know before you install the RSA authentication agent. In addition to the information in this section, always make sure you review your implementation plan and take note of any specific requirements.

Register the Authentication Host as an Agent Host

Your ACE Server administrator must register the RSA authentication agent server as an Agent Host.

1. There must be a TCP/IP connection between the ACE server and RSA authentication host server.
2. Copy the sdconf.rec file given to you by your ACE Server administrator into your Windows system folder.

For more information, contact your ACE Server administrator

Note: The user in the Policy Server must have the same logon name as on the RSA ACE Server.

Configure the SSO Client

This section explains what changes you need to make to the SsoClnt.ini file on the SSO Client computer to configure RSA authentication:

1. Edit the SsoClnt.ini file to include RSA as one of the authentication methods, preferably the first method in the list. For example:

   ```
   [ServerSet0]
   AuthMethods=RSA
   ```

2. Edit the SsoClnt.ini to include the name of the RSA authentication host in the auth agent keyname. For example:

   ```
   [Serverset0]
   AuthNOVELL=server1
   ```

For more information about the SsoClnt.ini file settings, see the “Configuring the SsoClnt.ini File” appendix in the *eTrust SSO Administrator Guide.*

Install the RSA SecurID Authentication Agent on Windows

To install the RSA authentication agent you must install the necessary files and then install and start the RSA SecurID authentication agent service.

This section explains how to install the RSA authentication agent, and how to start it once it has been installed.

Wizard Installation

To install the Certificate authentication agent, follow these steps:

1. From the eTrust Single Sign-On 8.0 Product Explorer wizard expand the eTrust Single Sign-On authentication agents folder, and select RSA authentication agent.

   The wizard should appear automatically when you insert the eTrust SSO disk. If not, open Windows Explorer and navigate to the CD-ROM directory and double-click the PE_i386.exe file.

   The Install button becomes active.

2. Click Install and accept the license agreement.

   The Destination Folder dialog appears.

3. Change the installation folder or click Next to accept the default.

   The Additional Information dialog appears.

4. Enter the name of the Authentication Host entry on the Policy Server, and the value of the encryption key associated with it. By default, the Policy Server installation creates a RSA_Authhost entry with a randomly-generated key value. Depending on your desired setup, you have a choice of either using the details of this Authentication Host entry or creating and configuring a new one.

Silent Installation

To install the authentication agent using the silent installation, follow these steps:

1. Open a command prompt and navigate to the Authentication Agent folder on the eTrust SSO CD.

2. From the command prompt, enter:

```
setup.exe /s /v"/qn <insert variables here>"
```

For information about what values you can specify, see the Command Line Settings section in this chapter.

Note: In order to execute a silent installation you have to accept the license agreement. The setting required for accepting the license agreement and silently installing the authentication agent can be found at the bottom of the license agreement available when running the installation wizard.

Command Line Settings

The command line settings for installing an authentication agent is:

Setting	Description
/s	Hides the initialization dialog.
/v	Passes parameters and property settings to the installation. It applies to all the parameters and properties listed in this table except /s. Place any parameters you wish to pass to the installation within quotes ("").
/L	Defines the full path and name of the installation log file. Use the mask * to log all available information. For example: `/L* C:\log.txt`
/qn	In conjunction with the /s parameter, used to initiate a silent installation. **Note:** You need to use the *license_accept* property to execute a silent installation.
license_accept	*license_accept* is the setting required for accepting the license agreement and silently installing the authentication agent. The actual setting you need to use can be found at the bottom of the license agreement that is available when running the installation wizard.

Setting	Description
INSTALLDIR=[location]	Specifies the location where the authentication agent will be installed.
AUTHHOSTNAME	Specifies the authentication host in the Policy Server for this agent type.
SDIKEY	Specifies the encryption key for that authentication host.

Install the RSA SecurID Authentication Agent on UNIX

To install the RSA SecurID Authentication Agent on UNIX follow these steps:

1. From the command prompt and navigate to the RSA agent folder on the eTrust SSO CD (SSO/Agents/RSA/UNIX).
2. From the command prompt, enter:

```
./install_rsa <insert variables here>
```

This will install the agent in interactive mode. For information about what values you can specify or to perform a silent installation, see the Command Line Settings section in this chapter.

Command Line Settings

Note: In order to execute a silent installation you have to accept the license agreement. The setting required for accepting the license agreement and silently installing the authentication agent can be found at the bottom of the license agreement available when running the installation wizard.

The command line settings for installing an authentication agent is:

Setting	Description
-s	Specifies that the installation is in silent mode.
license_accept	*license_accept* is the setting required for accepting the license agreement and installing the authentication agent. The actual setting you need to use can be found at the bottom of the license agreement that is available when running the installation wizard.
-d <target_dir>	Specifies the installation directory.
-a <auth_host_name>	Specifies the Authentication host to be used for ticket processing.
-t <ticket key value>	Specifies the key to be used for encryption during ticket creation.
-h/-help	Provides help.

Post-installation Configurations

This section explains what you need to do after you have installed the RSA authentication agent.

Re-install the RSA SecurID Authentication Agent

If you uninstall the RSA SecurID authentication agent and then re-install it, alter the configuration on the RSA ACE server:

1. Open the **Edit Agent Host** dialog.
2. De-select the **Sent Secret Node** check box.

Configuration Settings for the RSA Authentication Agent

This section lists the settings you can configure in the RSA authentication agent. All of these settings may be edited, but you must restart the eTrust SSO – RSA SecurID authentication agent Windows service for the changes to take effect.

The settings for the Windows authentication agent are found below the following Windows Registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sso_tga_rsa_Agent1\Parameter
s\sso_tga_rsa_Agent1
```

The following table lists the configurable settings:

Keyname	Description	Default Value
AuthHostName	The name of the authentication host that is included in the SSO ticket. If you leave this blank, the computer name of the authentication host will be used (this is the legacy behavior from SSO 7.0 and earlier). A default authentication host entry, RSA_Authhost, is created by default during the Policy Server installation. It is associated with ps-ldap user datastore and has a randomly-generated encryption key (see TicketKey configuration option further below) value assigned to it.	RSA_Authhost
ChildLimit	Determines the number of worker threads that get created for dealing with incoming client requests.	3
IdleFreq	Idle frequency, in calls/second.	20
ListenQueSize	The value of this configuration option determines the maximum length of the queue of pending connections. If a connection request arrives and the queue is full, the client will receive an error response. This value can be increased if the Ticket Granting Agent (TGA) is unable to process the incoming authentication requests (from SSO Client) fast enough, with communication-related error messages being generated.	5
PortNumber	Port number on which the TGA is listening for client requests.	13969
RecvBuffSize	Length of the buffer used when receiving the data (in bytes).	131072 (128 KB)
SendBuffSize	Length of the buffer used when sending the data (in bytes).	131072 (128 KB)
StandbyConnections	The minimum number of connections to the authentication servers. When reducing the number of connections (due to not having been used recently) the standby is used as the minimum.	5
TicketKey	Key used to encrypt the ticket that is created by the TGA (after successful authentication) and sent to the SSO client. The value of this option must correspond to the encryption key value associated with the Auth Host entry on the Policy Server that corresponds to the value of AuthHostName configuration option (see earlier in this table).	
TimeOutConnect	Connection time-out value (in seconds).	60
TimeOutRecv	Receive time-out value (in seconds).	60
TimeOutSend	Send time-out value (in seconds).	30

Starting the RSA Agent Service Manually on Windows

When the service is running, the RSA SecurID agent is ready to accept authorization queries from the eTrust SSO client.

When you restart the RSA agent server computer, the RSA authentication agent Windows service starts automatically.

To start the service manually, follow these steps:

1. Go to the Control Panel and select Settings, Administrative Tools, Services.
2. Find the 'eTrust SSO – RSA authentication agent – Agent 1' in the list and right-click and select Start.

Starting the RSA Agent Manually on UNIX

To start the service manually, enter

```
startserver -c <ConfigFile> [-p <PortNumber>] –altpwd
```

where:

- c <Conf igFile>
A path to the configuration file that you have either created or modified previously. This parameter is not mandatory. If the parameter is not specified. the SafeWord authentication agent will look for swec.cfg in the same directory as the agent executable.

-p <PortNumber>
Overrides the default port. The value defaults to 13970.

-altpwd
cd to "/usr/tmp"

Note: There are two different port numbers that relate to this integration:

- The -p parameter relates to communication between the SSO Client and the RSA authentication agent, and therefore the value that is supplied should match the appropriate value in the `ssoclnt`.ini file.
- The port number in swec.cfg identifies the communication line between the RSA authentication server and the RSA authentication agent.

Implementing the SafeWord Authentication Agent

eTrust Single Sign-On supports primary authentication with SafeWord, a product developed by Secure Computing Corporation. The SSO SafeWord interface seen by end users is similar to the Secure Computing Corporation interface. The terminology used in the SSO SafeWord interface is also very similar to the Secure Computing Corporation terminology.

The SafeWord authentication agent only runs on UNIX platforms.

Before You Begin

The Before You Begin Section is designed to guide you through what you need to know before you install the SafeWord authentication agent. In addition to the information in this section, always make sure you review your implementation plan and take note of any specific requirements.

Configure the SSO Client

This section explains what changes you need to make to the SsoClnt.ini file on the SSO Client computer to configure SafeWord authentication:

1. Edit the SsoClnt.ini file to include SafeWord as one of the authentication methods, preferably the first method in the list. For example:

   ```
   [ServerSet0]
   AuthMethods=SWEC
   ```

2. Edit the SsoClnt.ini to include the name of the SafeWord authentication host in the auth agent keyname. For example:

   ```
   [Serverset0]
   AuthSWEC=server1
   ```

For more information about the SsoClnt.ini file settings, see the “Configuring the SsoClnt.ini File” appendix in the *eTrust SSO Administrator Guide.*

Install the SafeWord Authentication Agent

To install the Safeword Authentication Agent follow these steps:

1. From the command prompt navigate to the SWEC agent folder on the eTrust SSO CD (SSO/Agents/SWEC/UNIX).

2. From the command prompt, enter:

```
./install_seotp <insert variables here>
```

This will install the agent in interactive mode. For information about what values you can specify or to perform a silent installation, see the Command Line Settings section in this chapter.

Note: In order to execute a silent installation you have to accept the license agreement. The setting required for accepting the license agreement and silently installing the authentication agent can be found at the bottom of the license agreement available when running the installation wizard.

Command Line Settings

Note: In order to execute a silent installation you have to accept the license agreement. The setting required for accepting the license agreement and silently installing the authentication agent can be found at the bottom of the license agreement available when running the installation wizard.

The command line settings for installing an authentication agent is:

Setting	Description
license_accept	*license_accept* is the setting required for accepting the license agreement and installing the authentication agent. The actual setting you need to use can be found at the bottom of the license agreement that is available when running the installation wizard.
-a <auth hostname>	Specifies the Authentication host to be used for ticket processing.
-d <target_dir>	Specifies the installation directory.
-h/-help	Provides help.
-port <port number>	Specifies the SafeWord server port number.
-s	Specifies that the installation is in silent mode. See, *license_accept*.
-server <hostname>	Specifies the SafeWord server host name.
-t <ticket key value>	Specifies the key to be used for encryption during ticket creation.

Post-Installation Configurations

This section explains what you need to do after you have installed the SafeWord authentication agent.

Review the swec.cfg Configuration File

Review the contents of the swec.cfg configuration file that is installed to the same directory as the Safeword authentication agent executable. The important entries are as follows:

```
02  SafeWord Authen. Server Name:       <hostname> 0 0 <port-number>
09  User ID Source (USER/SYSTEM):       USER
10  Server’ s System Name:      STANDARD
```

where <hostname> is the Safeword Server host name, and <port-number> is the port number on which the Safeword Server listens to incoming authentication requests (by default it is 5030).

Start the SafeWord Agent Manually

To start the service manually, enter

```
startserver -c <ConfigFile> [-p <PortNumber>] –altpwd
```

where:

- c <Conf igFile>
A path to the configuration file that you have either created or modified previously. This parameter is not mandatory. If the parameter is not specified. the SafeWord authentication agent will look for swec.cfg in the same directory as the agent executable.

-p <PortNumber>
Overrides the default port. The value defaults to 13970.

-altpwd
cd to “/usr/tmp”

Note: There are two different port numbers that relate to this integration:

- The -p parameter relates to communication between the SSO Client and the SSO SW Agent, and therefore the value that is supplied should match the appropriate value in the `ssoclnt`.ini file (see below).
- The port number in swec.cfg identifies the communication line between the SafeWord Authentication Server and the SafeWord authentication agent.

Implementing the Windows Authentication Agent

eTrust SSO supports user authentication to Windows.

Before You Begin

The Before You Begin Section is designed to guide you through what you need to know before you install the Windows authentication agent. In addition to the information in this section, always make sure you review your implementation plan and take note of any specific requirements.

Set Up a Domain Controller

Before you start installing the Windows authentication agent, make sure to set up your domain controller and create a user. You then need to put the computers you want to run the client, the server and the Windows authentication agent from onto the network. Optionally, these can be the same computer.

Create an Authentication Host Entry on the Policy Server

You only need to do this if you decide to use a different authentication host to the default created as part with the Policy Server installation (WIN_Authhost). For information on defining an authentication host, see the “Managing Resources” chapter in the *eTrust SSO Administrator Guide*.

Create Users

Create SSO users with the same name as a user on the domain controller and allow them to access the authentication host you are using for the Windows authentication. For example, a user named fred would be fred.picard.net and have access to WIN_Authhost.

Make sure to allow this user to log on using the Windows auth method.

Create a User Alias

Enter the following command into a selang session to change the authentication host and user values for the ones you have used:

```
er authhost <auth_host_name> useralias(“<user>=<alias>”)
```

Configure the SSO Client

This section explains what changes you need to make to the SsoClnt.ini file on the SSO Client computer to configure Windows authentication:

1. Edit the SsoClnt.ini file to include NT as one of the authentication methods, preferably the first method in the list. For example:

   ```
   [ServerSet0]
   AuthMethods=NT
   ```

2. Edit the SsoClnt.ini to include the name of the Windows authentication host in the auth agent keyname. For example:

   ```
   [Serverset0]
   AuthNT=server1
   ```

For more information about the SsoClnt.ini file settings, see the “Configuring the SsoClnt.ini File” appendix in the *eTrust SSO Administrator Guide.*

Install the Entrust Authentication Agent

This section explains how to install the Windows authentication agent.

Wizard Installation

To install the Windows authentication agent, follow these steps:

1. Log onto a computer on the network as a domain controller user
2. From the eTrust Single Sign-On 8.0 Product Explorer wizard expand the eTrust Single Sign-On authentication agents folder, and select Windows authentication agent.

   The wizard should appear automatically when you insert the eTrust SSO disk. If not, open Windows Explorer and navigate to the CD-ROM directory and double-click the PE_i386.exe file.

   The Install button becomes active.
3. Click Install and accept the license agreement.

   The Destination Folder dialog appears.
4. Change the installation folder or click Next to accept the default.

   The Additional Information dialog appears.
5. Enter the name of the Authentication Host entry on the Policy Server, and the value of the encryption key associated with it. By default, the Policy Server installation creates a WIN_Authhost entry with a randomly-generated key value. Depending on your desired setup, you have a choice of either using the details of this Authentication Host entry or creating and configuring a new one.

Silent Installation

To install the authentication agent using the silent installation, follow these steps:

1. Open a command prompt and navigate to the Authentication Agent folder on the eTrust SSO CD.
2. From the command prompt, enter:

   ```
   setup.exe /s /v"/qn <insert variables here>"
   ```

   For information about what values you can specify, see the Command Line Settings section in this chapter.

   Note: In order to execute a silent installation you have to accept the license agreement. The setting required for accepting the license agreement and silently installing the authentication agent can be found at the bottom of the license agreement available when running the installation wizard.

Command Line Settings

The generic command line settings for installing an authentication agent is:

Setting	Description
/s	Hides the initialization dialog.
/v	Passes parameters and property settings to the installation. It applies to all the parameters and properties listed in this table except /s. Place any parameters you wish to pass to the installation within quotes ("").
/L	Defines the full path and name of the installation log file. Use the mask * to log all available information. For example: `/L* C:\log.txt`
/qn	In conjunction with the /s parameter, used to initiate a silent installation. **Note:** You need to use the *license_accept* property to execute a silent installation.
license_accept	*license_accept* is the setting required for accepting the license agreement and silently installing the authentication agent. The actual setting you need to use can be found at the bottom of the license agreement that is available when running the installation wizard.
INSTALLDIR=[location]	Specifies the location where the authentication agent will be installed.
AUTHHOSTNAME	Specifies the authentication host in the Policy Server for this agent type.
ENCRYPTKEY	Specifies encryption key for the authentication host.

Post-installation Configurations

This section explains what you need to do after you have installed the Windows authentication agent.

Configuration Settings for the Windows Authentication Agent

This section lists the settings you can configure in the Windows authentication agent. All of these settings may be edited, but you must restart the eTrust SSO – Windows authentication agent Windows service for the changes to take effect.

The settings for the Windows authentication agent are found below the following Windows Registry key:

```
HKLM\SOFTWARE\Computer Associates\eTrustSSO\NT authentication agent
```

The following table lists the configurable settings:

Keyname	Description	Default Value
AuthHostName	The name of the authentication host that is included in the SSO ticket. If you leave this blank, the computer name of the authentication host will be used (this is the legacy behavior from SSO 7.0 and earlier). A default authentication host entry, WIN_Authhost, is created by default during the Policy Server installation. It is associated with ps-ldap user datastore and has a randomly-generated encryption key (see TicketKey configuration option further below) value assigned to it.	WIN_Authhost
encryption_key	Key used to encrypt the ticket that is created by the TGA (after successful authentication) and sent to the SSO client. The value of this option must correspond to the encryption key value associated with the Auth Host entry on the Policy Server that corresponds to the value of AuthHostName configuration option (see earlier in this table).	
LogCFG	Full path to the logging configuration file for Windows authentication agent.	<installation directory>\NtAgentLog.cfg

Starting the Windows Agent Service Manually

When the service is running, the Windows agent is ready to accept authorization queries from the eTrust SSO client.

When you restart the Windows agent server computer, the Windows authentication agent Windows service starts automatically.

To start the service manually, follow these steps:

1. Go to the Control Panel and select Settings, Administrative Tools, Services.
2. Find the 'eTrust SSO – Windows authentication agent' in the list and right-click and select Start.

Creating a Custom Authentication Agent

eTrust SSO offers a number of out-of-the-box methods for primary authentication, for example, SSO, Windows, and RSA SecureID as discussed in this chapter. However, you may want to develop your own specific authentication mechanism, for example, a biometric provider might want to integrate their solution into eTrust SSO.

eTrust SSO provides the functionality to accomplish this by giving you the tools to develop code that integrates with a defined SSO code interface. This interface is defined and the information is supplemented using a simple sample integration MS VC++ project that can be requested from your CA representative. This sample demonstrates the steps you must follow can take to develop your own authentication agent that integrates with eTrust SSO.

Program Architecture

All eTrust SSO authentication agents have a similar architecture. Each authentication agent has three components:

- A graphical user interface (GUI) – resides on SSO Client
- An open authentication engine (OAE) – resides on SSO Client
- A ticket-granting agent (TGA) – resides on an SSO Authentication Host

The GUI Component

The GUI DLL provides the eTrust SSO Client with an Authentication dialog, which is defined by the interface function authenticate_Dlg.

The OAE Component

The open authentication engine is also known as the interface library.

This library provides the SSO Client with an interface for requesting authentication defined by the oae_GetTicket function.

The OAE also provides a call-back function for the GUI component defined by the AuthCb_Verify function. This function is triggered when the OK button is pressed on the Login dialog. The OAE then sends a TCP/IP request to the TGA component. In this way this part of the authentication agent is responsible for communication between the GUI and the TGA.

The TGA Component

This agent can be either a Windows service or UNIX daemon. The TGA communicates directly with the authentication server. It also communicates with client-side library components through TCP/IP.

The Windows and UNIX versions have the same architecture. The differences are caused by the differences between the tools that each operating system uses to create functions such as sub-processes, threads and inter-process communication.

The encrypted TCP/IP communication between authentication agent components is implemented using core tcpxdr and tcpcomm components. Logging is done using log4cpp.

Chapter

8

Implementing the SSO Client

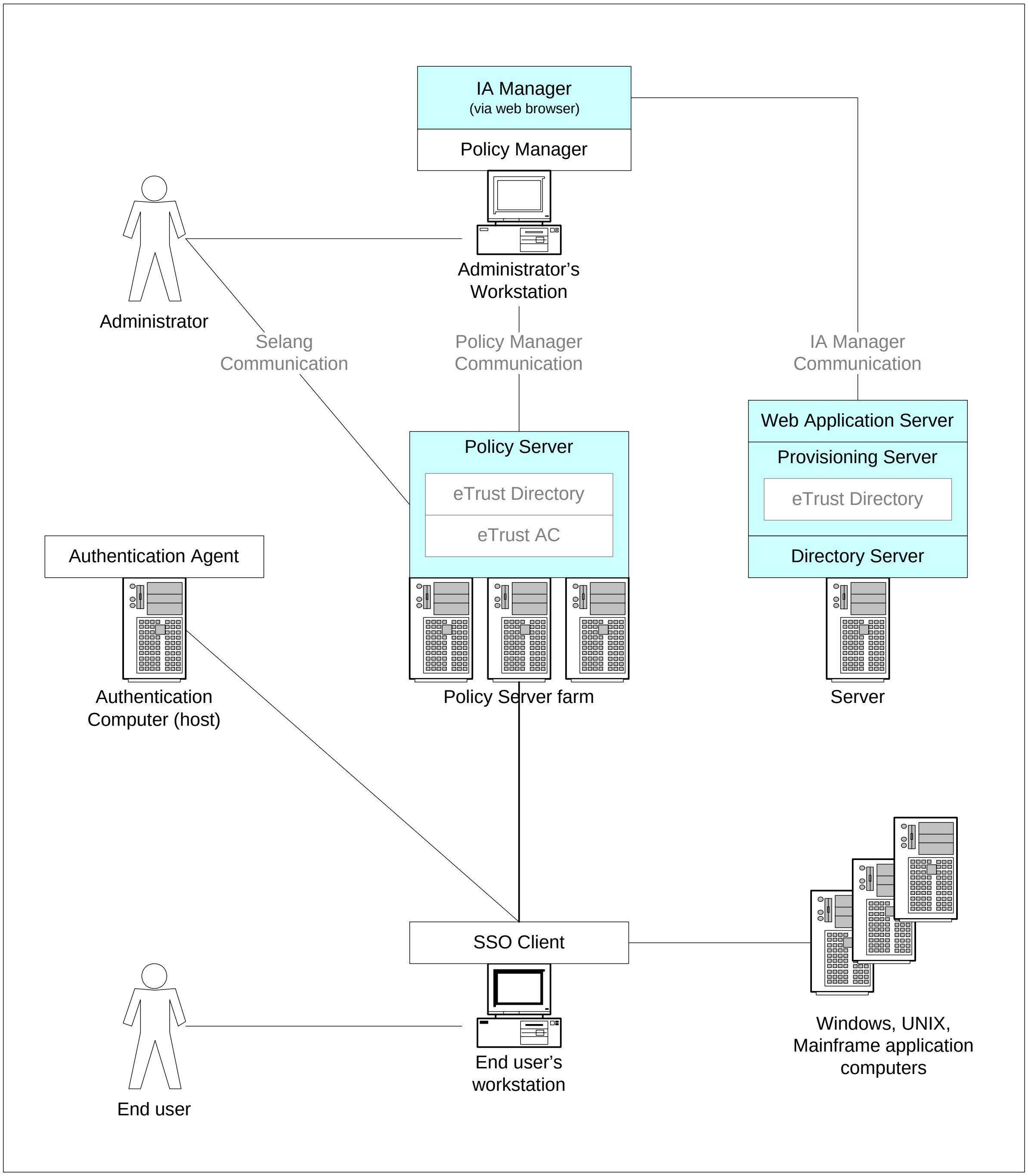
This chapter explains how to install the SSO Client.

The SSO Client is an application that allows users in your enterprise to work with eTrust Single Sign-On (eTrust SSO). This is the only eTrust SSO component that the end user sees and works with.

The SSO Client runs on every workstation that uses eTrust SSO services.

Architecture

The following diagram shows where the SSO Client fits into the architecture of a typical eTrust SSO deployment.



Before You Begin

The Before You Begin Section is designed to guide you through what you need to know before you install the SSO Client. In addition to the information in this section, always make sure you review your implementation plan and take note of any specific requirements.

Before you install the SSO Client, you should install the Policy Server and an authentication agent (if you are not using SSO authentication). You must know the names of the computers that these components have been installed on before you begin this process.

Decide Where to Install the SSO Client

The SSO Client:

- Must be installed on every end-user's computer
- Can optionally be installed on the Administrators' computers
- Must be installed on the Citrix MetaFrame Server computer *if* you are deploying the Citrix Application Migration with eTrust SSO

Note: You can distribute the SSO Client using Unicentre Software Delivery 4.0.

Decide on a Method of Installation

This section helps you decide how to install the SSO Client.

Wizard Installation Versus Silent Installation

There are two ways to install the SSO Client:

- Wizard installation (Windows GUI)
  This is recommended if you are installing the SSO Client on less than 10 computers.
- Silent installation (command line prompt)
  This is recommended if you are installing the SSO Client on more than 10 computers.

You should decide which installation method to use based on how many computers you want to install the SSO Client on. The numbers indicated above are just a guide. Each implementation has different requirements.

Note: You must use the wizard installation at least once before you can perform a silent installation. This lets you accept the license agreement and create the SsoClnt.ini file that is required for the silent installation.

For more information about the SsoClnt.ini file, see the "Configuring the SSO Client (SsoClnt.ini)" appendix in the *eTrust SSO Administrator Guide* or the SsoClnt_Readme.htm that is installed with the SsoClnt.ini file.

Typical Versus Custom Installation

Part way through this installation you will be asked to choose whether you want to do a custom installation or a typical installation. You only need to select custom installation when you want to:

- Change the default authentication agents installed (by default all authentication agents are installed).
- Install the SSO GINA functionality (Windows NT/XP/2000/2003 only).
- Workstation Mode options (Windows NT/XP/2000/2003 only). This covers shared workstation mode and you will only get this option if you choose to install the SSO GINA.
- Configure the SSO Client Toolbar as the default, instead of SSO Client Tools. This affects how users access their eTrust SSO application list.
- Install the SSO Client on a Citrix Metaframe server or an ICA Client computer (this is only relevant if you are deploying the Citrix Application Migration with eTrust SSO).

For more information about Workstation Mode setting and GINA functionality, see, the “Configuring the SSO Client (SsoClnt.ini)” appendix in the *eTrust SSO Administrator Guide* or the SsoClnt_Readme.htm that is installed with the SsoClnt.ini file.

Design Your Server Sets

A server set is a group of related servers and server information. The SSO Client uses these server sets to decide which Policy Server(s) or authentication server(s) it should refer to.

Sever sets extend the fault tolerance and failover of the SSO Client functionality where it interacts with the Policy Server(s) and the authentication server(s).

Sever sets also help users identify which servers to log onto because you can give server sets meaningful names which appear in the drop-down list on the SSO Client logon screen. For example you could name two server sets, “Logon at Home” and “Logon at Work”.

How to Create a Server Set

You must create at least one server set for the SSO Client to refer to. The first server set is always called **ServerSet#0**.

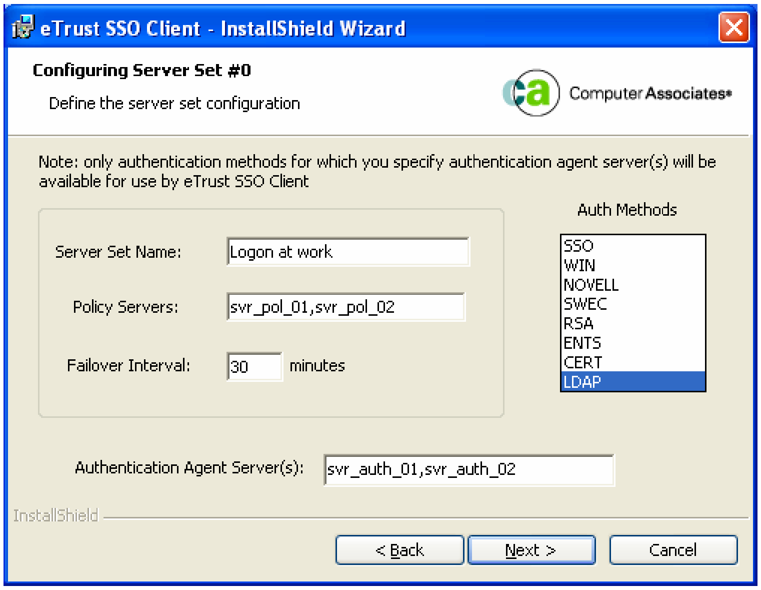
To create a server set you can either:

- Follow the SSO Client wizard installation (either Typical or Custom)
- Edit the SsoClnt.ini file using a text editor

  Note: You must install the SSO Client using the installation wizard at least once to create an SsoClnt.ini file.

How to Configure Server Sets

Part way through the SSO Client Installation Wizard, you will see this screen that helps you configure your server sets.



eTrust SSO Client - InstallShield Wizard

Configuring Server Set #0

Define the server set configuration

Note: only authentication methods for which you specify authentication agent server(s) will be available for use by eTrust SSO Client

Server Set Name: Logon at work

Policy Servers: svr_pol_01,svr_pol_02

Failover Interval: 30 minutes

Auth Methods: SSO, WIN, NOVELL, SWEC, RSA, ENTS, CERT, LDAP (selected: LDAP)

Authentication Agent Server(s): svr_auth_01,svr_auth_02

Server Set Name: Enter the name of the sever set. Make this a user-friendly name because users see this in their SSO Client logon drop-down list.

Policy Servers: Enter the name(s) of the Policy Server computer(s). You can enter multiple computer names separated by commas or spaces. If the SSO Client cannot connect to the first computer in the list, it will try the second, and so on.

Failover Interval: Enter the time that you want to elapse before the SSO Client will retry a failed Policy Server. For example, if the SSO Client cannot connect to **svr_pol_01** it will try **svr_pol_02** and will not try to connect to **svr_pol_01** again for 30 minutes.

Authentication Hosts: Enter the name(s) of the computer(s) that host the authentication software. You can enter multiple computer names separated by commas or spaces. If the SSO Client cannot connect to the first computer in the list, it will try the second, and so on.

Note: You must specify an authentication host for every authentication method that you want users to be able to use.

Authentication Methods: Highlight an authentication method and specify the name of the Authentication Host for the corresponding authentication software.

Once the first SSO Client has been installed you can copy and modify the SsoClnt.ini file which contains the Server Set configuration. For more information about the SsoClnt.ini file, see the “Configuring the SSO Client (SsoClnt.ini)” appendix in the *eTrust SSO Administrator Guide*.

Pre-Installation Checklist

Before you begin, use this checklist to make sure you have all the information and software that you need to install the SSO Client.

□ Ensure you are running Windows 98SE or later.

□ Ensure that the computer you are installing the SSO Client on has a network connection with TCP/IP to communicate with the Policy Server.

□ Ensure that you have decided which authentication method(s) to use and have installed the authentication software, if necessary.

SSO authentication is native to eTrust SSO and does not need to be installed separately.

□ Ensure you have the server set information ready. For each server set you will need the names of the:

- Server set(s) (this is the name that the user will see in the authentication dialog)
- Authentication host computer(s)
- Policy Server computer(s)

□ For silent installation of the SSO Client, ensure that you have saved changes to the SsoClnt.ini file and put it in the installation directory.

For more information about the SsoClnt.ini file, see the "Configuring the SSO Client (SsoClnt.ini)" appendix in the *eTrust SSO Administrator Guide* or the SsoClnt_Readme.htm that is installed with the SsoClnt.ini file.

□ If you want to supply your own Readme.html file to your users, place this in the installation folder with the SsoClnt.ini file.

□ If you want to use the SSO GINA, ensure that you set administrator privileges for the computer you install the SSO Client on.

□ If you want to use the SSO GINA, and you don't want to use the default SSO GINA pages, you should supply your own SSO GINA images.

For more information about the SsoClnt.ini file, see:

- "Configuring the SSO Client (SsoClnt.ini)" appendix in the *eTrust SSO Administrator Guide*
- "Working with the SSO Client" chapter in the *eTrust SSO Administrator Guide*

□ Write and configure the Tcl scripts to logon to applications. You can install the SSO Client without these scripts, but the single sign-on functionality relies on these scripts.

Install Using the Graphical Wizard on Windows

This section explains how to install the SSO Client using the installation wizard.

Install Using the Wizard

This procedure describes how to install the SSO Client using the Product Explorer Wizard.

Tip: When you enter more than one computer name in a list you can separate the names with commas and/or spaces.

To install the SSO Client component of eTrust SSO using the wizard, follow these steps:

1. Insert the product installation CD into your CD-ROM drive.

   If you have Autorun enabled, the Product Explorer automatically displays. Otherwise, navigate to the CD-ROM drive and double-click the PE_i386.EXE file.

2. From the Product Explorer main menu, select Single Sign-On Client 8.0, and click Install.

3. Follow the prompts and when you are done, click Install to start the SSO Client installation.

   Part way through the installation you will be asked to configure server set information. For more information about how to configure server sets, see the Design Your Server Set section in this chapter.

Tip: When the dialog InstallShield Wizard Complete appears, you have successfully installed the SSO Client. Be sure to review the Readme file, and then click Finish to complete the process.

How to Modify SSO Client on Windows

If you need to modify SSO Client components, you can either use the:

- Graphical wizard from the SSO CD, as you did for the SSO Client installation
- Add or Remove Programs from the Windows Start menu

The wizard detects that the SSO Client is installed and shows the interface for modification and maintenance of SSO Client components.

You can also modify the SSO Client by editing the SsoClnt.ini file.

For more information about the SsoClnt.ini file, see the “Configuring the SSO Client (SsoClnt.ini)” appendix in the *eTrust SSO Administrator Guide* or the SsoClnt_Readme.htm that is installed with the SsoClnt.ini file.

Note: We recommend that you shut down the SSO Client before you make any changes. If you do not shut down the SSO Client, you must restart it for changes to take effect.

Install Using the Silent Installation on Windows

This section explains how to install the SSO Client using a silent installation.

You must configure the SsoClnt.ini file prior to installing the SSO Client using the silent installation method. You get the SsoClnt.ini file by installing the SSO Client using the installation wizard.

If you accept the default locations that are set during the default installation of the SSO Client using the wizard, the SsoClnt.ini file is located in %Program Files%\CA\eTrust SSO\Client folder (where %Program Files% is the value of the Program Files environment variable on the local machine)

Install Using the Silent Installation

This method is good when you want to install the SSO Client quickly on many computers, but you also want to be able to configure multiple settings in the SsoClnt.ini file.

1. Install the SSO Client using the wizard.
2. Modify the SsoClnt.ini file to suit your installation needs.

   Unless you have specified a different location the SsoClnt.ini file is located in %Program Files%\CA\eTrust SSO\Client folder (where %Program Files% is the value of the program files environment variable on the local machine)

   For more information about how to configure your SsoClnt.ini file, see Appendix A in the *eTrust SSO Administrator Guide* or the SsoClnt_Readme.htm file.
3. Copy the installation files to a network drive and put the customized SsoClnt.ini file in the same folder. You can also put a customized version of the Readme.htm in this folder.
4. Open the command prompt and navigate to the location of the installation files.
5. From the command prompt, type:

   ```
   setup.exe /s /v"/qn <insert variables here>"
   ```

   You can specify certain information in the silent command line. For information about what values you can specify in the silent install, see the Command Line Settings section of this chapter.

   The SSO Client will install silently using the supplied SsoClnt.ini file for all the configuration information.

Command Line Settings for Silent Installations

You can set several values when you install the SSO Client using a silent installation.

Setting	Description
ALLUSERS=2	This setting lets Windows add the SSO Client to the Add/Remove Programs list. You should always include this in your silent installation command and it should always be set to "2"
INSTALLDIR = [enter location]	Installation directory on the user's computer
INSTALLLEVEL=130	Install all authentication methods *plus* the SSO GINA. You cannot install the GINA silently without also installing all the authentication methods. We recommend that you only use INSTALLLEVEL 110 or 130, not both.
STARTUPFOLDER=[1|0]	Specify whether the eTrust SSO application list will display in the user's Windows Start menu. 0 = Don't create in Start menu 1 = Do create in Start menu* *See SESSMGMTENABLED below.
SESSMGMTENABLED=[1|0]	Enables Session Management GINA pass - through option in the Windows Start menu. If you: ▪ are installing the GINA, *and* ▪ are creating Shortcut in the Start menu, *and* ▪ have selected GinaPassThrough = yes (in the SsoClnt.ini file) then we strongly recommend that you set SESSMGMTENABLED=0 (0 = no, 1 = yes)

REBOOT=[F|R]	Reboot the computer after installation?
	F = Force a reboot
	R = Suppress a reboot

Setting	Description
ADDLOCAL=[Gina|GinaPassThrough|StationLock|StationLock9x|Tcl]	This command lets you define the GINA (logon screen) and which GINA functionally you would like to install. You can specify multiple ADDLOCAL values, separated by commas. **Note:** You must list Gina for any Gina functionality.

Here is an example of a silent install command that includes variables:

```
Setup.exe /s /v"/qn INSTALLLEVEL=110 STARTUPFOLDER=1 REBOOT=R"
```

For more information about the SSO GINA see the e*Trust SSO Administrator Guide* “Configuration the Client” chapter.

Configure the SSO Client

This section tells you the theory behind configuring the SSO Client for silent installations, advanced or custom functionality, and large-scale deployments.

How to Configure the SSO Client

The behavior of the SSO Client is determined by the SsoClnt.ini file.

The SsoClnt.ini file is broken into sections. Each section has one or more settings that you can change to alter the behavior of the SSO Client. Settings are also known as tokens or keynames. Each section is denoted by words or letters enclosed in square brackets, for example the first section of the SsoCltn.ini file is [ServerSet0].

To set the behavior of the SSO Client you file you often have to make changes to several different sections of the SsoClnt.ini file in conjunction with each other.

For more information about the SsoClnt.ini file, see the "Configuring the SSO Client (SsoClnt.ini)" appendix in the *eTrust SSO Administrator Guide* or the SsoClnt_Readme.htm that is installed with the SsoClnt.ini file.

How to Regularly Update the SSO Client

You can define a centralized SsoClnt.ini file to be used by many SSO Client workstations. Using a centralized SsoClnt.ini file lets you regularly update all the SSO Clients quickly and easily.

The SSO Client obtains its initialization parameters from one of the following places:

- The SsoClnt.ini file, which is located in the same directory as the SSO Client executable:

  This is stored on the location workstation but you can configure this file to periodically check and download a new SsoClnt.ini files from a central server using the GlobalIniFile setting.

- Local operating parameters

- For Window clients, from the local Windows registry
- For UNIX clients, from the SsoClnt.ini file in the home directory

To configure a centralized SsoClnt.ini you must set the UseGlobalIniFile keyname to Yes in the SsoClnt.ini. This triggers a centralized SsoClnt.ini file to automatically be "copied" down to the local workstation from the network when the SSO Client starts up, if the local SsoClnt.ini file is deemed to have expired.

For more information about the SsoClnt.ini file, see the "Configuring the SSO Client (SsoClnt.ini)" appendix in the *eTrust SSO Administrator Guide* or the SsoClnt_Readme.htm that is installed with the SsoClnt.ini file.

The SSO Client in Large Scale Deployment

If you are installing the SSO Client on multiple different workstations, you should customize the SsoClnt.ini to suit your needs before you install the SSO Client. For this reason we recommend that you install, configure, and test the SSO Client on one or two machines before you distribute it to the rest of your enterprise.

To silently install the SSO Client on a large scale, copy the Client installation files to a network drive together with the customized SsoClnt.ini file.

SSO Client Security Considerations

For security reasons, you may want to clear the username field in the Windows Logon tab, so that by default, the last user who logged on is not listed.

Also, you may want to hide the Shutdown button on the Windows Only tab.

To hide the name of the last user to log on, set the following registry key to 1:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\dontdisp
laylastusername
```

To disable the Shutdown button, set the following registry key to 0:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\shutdown
withoutlogon
```

Troubleshooting the Installation

If you are signing on for the first time after eTrust SSO was installed, you can test the SSO Client using the LDAP administrator name and the SSO authentication method. The default LDAP administrator name is ldap-admin. This is defined during the IAM Common Components installation when you configure the Policy server.

You can set up logging to track down any issues with the installation. We recommend that you don't leave logging on all the time because the log files will take up a lot of space. Just turn logging on when you need it for a specific reason. For more information about logging, see the *eTrust SSO Administrator Guide*, "Auditing, Logging, and Tracing" chapter.

Chapter

9

Adding Applications to SSO

This chapter describes how to add applications to the eTrust Single Sign-On (eTrust SSO) system so that you can allocate them to users.

eTrust SSO automates the process of end-users logging on to the applications. Before end-users can start using eTrust SSO, a set of logon scripts have to be written. You need a logon script for every application that users need to access from eTrust SSO.

The logon script is a sequence of instructions that automate the logon process. The primary task of the logon script is to simulate users actions when they log into an application and insert their user credentials (user name and password, for example) when required. Additionally, a logon script may contain procedures for other tasks associated with the logon process, such as changing a password and letting the Policy Server know the outcome of the logon attempt.

For more information about adding applications to SSO, see the “Authenticating Users to Applications” chapter to the *eTrust SSO Administrator Guide.*

How Logon Scripts Work

Whenever an authorized user selects an SSO-supported application, the SSO interpreter receives the logon script and the logon data from the Policy Server and executes the script.

A logon script needs to conform exactly to the specific logon requirements of an application, mimicking the data entry and actions of an end-user of that application in your system. Therefore, the person writing eTrust SSO logon scripts needs to work together with an applications administrator who has a detailed knowledge of the logon process for each application.

These logon scripts are written in an extended version of Tcl, a scripting language that gives you the use of variables, conditions, loops, procedures, and other common programming constructs with a minimum of complexity. Prior experience with Tcl is not required, but the scriptwriter should be familiar with the applications involved and, in particular, the logon processes. For a full description of the SSO scripting language and writing logon scripts, see the *eTrust SSO Scripting Reference Guide*.

The SSO Interpreter is an eTrust SSO component that executes the Tcl scripts. Once the SSO Interpreter has carried out all the procedures in the logon script, the application continues to run with no further input from eTrust SSO.

To enable application-specific logon scripts to serve various users, eTrust SSO maintains separate logon variables for each authorized user for each application. The logon scripts refer to these logon variables for individual logon name and password and other data that may be necessary.

Before You Begin

Before you start writing a logon script you need to do some preparation. Here is an outline of the things you need to do before you start writing a logon script.

Decide What You Want the Script To Do

It is important to work out exactly what you want the script to do. A simple example might be that you want to launch an application, enter the user credentials and press the OK button.

You can also create scripts that perform quite complicated logons and logons, or scripts that automate part of the process and require user input before they process any further.

Document The Process That You Want to Automate

You must run through the process manually and document every step. This is what the script will automate.

For example:

1. Launch the application
2. Wait for the logon box
3. Enter the username
4. Tab to the next field
5. Enter the password
6. Press the OK button.

Make sure that you understand all the possible variables that might occur, for example, whether users are periodically prompted to change their password. The script that you write must be able to handle these exceptions.

Identify Where the Data is Stored

Before you start you must know where the following information is stored:

- Application or file executable
- Logon Script
- User data store

Developing Logon Scripts

The security or system administrator in charge of eTrust SSO is usually responsible for preparing the logon scripts. Generally, programmers write logon scripts under the administrator's supervision.

Following is an example of the main portion of a logon script for a telnet client that comes with Windows NT:

```
# run the NT telnet client
sso run -path telnet.exe

# connect to the remote host
sso menu -item “Connect/Remote System”
sso setfield -label “Host Name” -value $_HOST
sso click -label Connect

# verify that the telnet window appears
sso window -title Telnet

# wait for the user ID; respond
sso waittext -text “logon:”
sso type -text “$_LOGINNAME{enter}”

# wait for the password prompt; respond
sso waittext -text “password:”
sso type -text “$_PASSWORD{enter}”

# wait for the system prompt
sso waittext -text “>“

...
```

The logon variables that appear in this logon script are $_HOST, $_LOGINNAME, and $_PASSWORD. The SSO Interpreter on the user's workstation replaces these variables with the values received from the Policy Server.

Symbol	Meaning
$	Tcl variables
$_	SSO logon variables
#	Comment

For a full explanation of logon scripts, see the eTrust SSO *Tcl Scripting Reference Guide*.

Logon Variables

The logon variables include the logon script and the logon data sent to the SSO Client. These variables are fetched from the data stores. Some variables pertain to the current application, some are specific to the current user in relation to the current application, and some may hold installation-wide data.

The logon variables are stored in the LDAP or eTrust Access Control data store in the user's record as properties of the LOGONINFO section. Some of the logon variables are used for authentication (*logon credentials*) and others provide operational and auditing information (such as time of last logon).

For an illustration of how the logon variables are used, lets look at the following scenario.

1. Assume a user named Terri selects CICS_TEST from the application list.

   The application record of CICS_TEST in the eTrust Access Control data store contains:

   - DIALOG_FILE property with the value CICS.TCL
   - LOGON_TYPE property with the value AppTicket
   - HOST property with the value MVS_TEST

   In Terri's user record, in the LOGONINFO section relating to CICS_TEST, the property LOGONNAME contains the value UTST021.

2. The Policy Server generates an AppTicket and stores the result in the Tcl variable _PASSWORD.
3. The Policy Server places the logon name UTST021 in the Tcl variable _LOGONNAME.
4. The server sends the CICS.TCL logon script and the two logon variables _PASSWORD, _LOGONNAME, and _HOST to the SSO Client.
5. The SSO Client executes the supplied script, entering the username (_LOGONNAME) and ticket (__PASSWORD) as required.

Learn Mode (First Logon Situation)

In order to reduce the amount of configuration needed, eTrust SSO has a *learn mode* that functions during the first logon to an application and lets the end user provide the logon credentials for the application.

If the user credentials needed for an application are not found in the user record and the application logon uses password authentication, the Policy Server and SSO Client assume that this is the first time the user is logging into the application via eTrust SSO. eTrust SSO then enters learn mode (also called the *first logon situation*), as follows:

1. The Policy Server notifies the SSO Client that no credentials are available.
2. The SSO Client displays a Learn Mode dialog box that prompts the user for user credentials (logon name and password for the application requested).
3. After the user supplies the user credentials, the client sends the credentials to the server and the client repeats the logon process with the new logon credentials.

Note: Learn mode only functions for users who are authorized to use an application and who have carried out primary authentication. Subsequent logon attempts to the same application by that user will automatically use the credentials they previously entered in learn mode.

Logon Script Maintenance

You should remember that eTrust SSO logon scripts use and interact with many variables and elements of the computing environment. Changes in the environment will affect the operation of logon scripts. For example:

- Changes in hard disk organization that change the location of applications may cause SSO-run commands to fail because the pathname argument will no longer be correct.
- Upgrading an application may result in many changes: new executable name or new logon windows with different titles and field labels. eTrust SSO extensions that refer to these elements will no longer function as expected.
- Upgrades and changes to operating systems will have similar effects.

Because of this, it is important that the administrator supporting eTrust SSO coordinate personnel responsible for version control and be in the loop on system environmental changes and application upgrades.

Where the Logon Scripts are Stored

The logon scripts are stored as ASCII files on the Policy Server host.

The exact location of the logon scripts is determined by different methods according to the Policy Server host operating system - Windows or UNIX.

Policy Server Host OS	Whether the Script Location is set
Windows	Windows Registry: HKEY_Local_Machine →Software→Computer Associates→eTrust→Shared→Policy Server→8.0→ ssod→<ScriptPath> Default ScriptPath is: %Program Files%\CA\eTrust Policy Server\scripts
UNIX	PolicyServer.ini file. ScriptPath key value (or token).

Application Authentication

All application logons supported by eTrust SSO follow the same overall process. The specific sub-section of application logon that handles the way the user is authenticated to the application is called *application authentication*. eTrust SSO offers two different methods of application authentication:

- Password authentication which can be used for applications on any platform (Windows, UNIX or Mainframe)
- Ticket authentication which is only used for Mainframe applications. Ticket authentication can be broken down into two subsections:

  - PassTickets

  - AppTickets

The application authentication method used for an SSO-supported application is specified in the LOGON_TYPE property of the application's record in the eTrust Access Control data store. If a value for the LOGON_TYPE property is not specified, the default method used is native SSO password.

Setting Up Password Authentication (All Platforms)

The following steps describe how to set up password authentication for an application:

1. Define the application in the eTrust Access Control data store with logon type pwd.
2. Link the application to a password policy using the Policy Manager (if required).
3. Authorize users and user groups to the application using the Policy Manager.
4. Write the logon script using Tcl and place it in the scripts directory defined in the policyserver.ini file (for UNIX) or the ScriptPath in the Registry settings (Windows) on the Policy Server host.
5. Have a user log into the application. The first time the user logs in, check that Learn Mode is activated.
6. During the second and succeeding logons, the user is not prompted for a password.
7. Change the user's password to check that the logon script and Policy Server process the new password correctly.

   For more information, see Changing the Primary Authentication Password and Defining the Lifetime of Passwords in the chapter "Administering eTrust SSO Users and Resources" and Logon script Maintenance in the chapter "Managing eTrust SSO Services."

Web-Based Applications

There are three ways to implement eTrust SSO for web applications:

- Client logon
- Cookie logon – requires the Web Agent
- Browser logon – requires the Web Agent

There are multiple web logon methods because different methods are suited to different web applications and different architectures. You can install all of these methods within the same eTrust SSO system.

There are multiple web logon methods because different methods are suited to different web applications and different architectures.

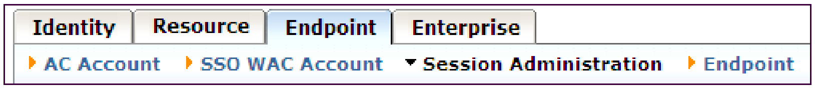
The term ‘web applications’ in this chapter includes restricted web pages.

For more information about the different ways to log on to web resources using eTrust SSO, contact your eTrust representative.

Chapter

10 Implementing Session Management

eTrust Single Sign-On (eTrust SSO) has the ability to control the number of sessions a user can have open concurrently. You can configure automatic session management by setting rules in the Policy Server, or you can you can work with sessions manually, using Session Administration in the IA Manager.



When you install eTrust SSO, the SSO Client is already capable of managing user sessions as long as you have also installed the SSO GINA. The installation and use of the SSO GINA is mandatory for Session Management to work correctly in the SSO Client.

To turn Session Management on, you need to enable session management in the Policy Server, create a session profile and apply it to a user or a group using the Policy Manager.

You can access the Session Administration tool in the IA Manager. This is used to monitor and terminate specific user sessions.

Note: When Session Management is turned on in the Policy Server, all users will have a default policy applied. You can view a user's default by going to the Policy Manager, clicking on a user, selecting their session profile list then clicking the **Effective Profile** button.

Automatic Session Management

This section tells you how to set up automatic session management to limit the numbers of eTrust SSO sessions a user can have open simultaneously.

Overview

This section give you an overview of the steps involved with setting up automatic session management. To set up automatic session management that lets you limit the number of sessions a users can have open simultaneously you must perform these steps:

- Configure the Policy Server
- Change the SSO Client port number
- Create and apply session profile

Pre-Installation Considerations

Here are the things you need before you start installing Session Management.

- You must have the basic eTrust SSO components installed and working. This includes the following components:
    - SSO Client
    - IAM Common Components
    - Policy Manager
    - Authentication Agent (if necessary)
    - Authentication software installed (if necessary)
- You must synchronize the clocks between the Policy Server (or multiple Policy Servers if you have a server farm) and the authentication host machine.

Configure the Policy Server

This section tells you how to configure the Policy Server on both Windows and UNIX platforms to enable automatic sessions management.

For Windows and UNIX installation you must use the Windows Registry on the Policy Server to configure session management. The relevant registry values were set up when you installed the Policy Server.

1. Open the Policy Manager and go to Resources, Configuration Resources, Policy Server Settings.
2. Double-click on Session Management

   The View or Set GPSCONFIGPROPERTY Properties - Settings
3. Double-click SessMgmtEnable.

   Select either:

   Enabled

   Session management is enabled, but is not required
   This allows SSO Clients from eTrust SSO 6.5 to work **without** Session Management, and SSO Clients from eTrust SSO 7.0 and 8.0 to work **with** Session Management

   Required

   Session management is required. If an eTrust SSO 6.5 Client (or earlier) is started, it attempts to connect to the Policy Server and then closes immediately.

   Note: If you set Session Management to Required then you must enter the IA Manager IP address as a Sessionless Terminal.
4. Restart the Policy Server.
5. Change any of the other settings that you require. For more information see the Session Management Settings section in this chapter.

Change the SSO Client Port Number

To use the Direct Notification method, the SSO Client must be listening for notification messages from the Policy Server on a particular port.

You may need to change the range of port numbers if you know that an application on your network routinely uses a port in this range. The default range is 20001-20201.

You can change this port in the Session Management section of the SsoClnt.ini file on each client computer.

1. Open the SsoClnt.ini file.
2. Find the Session Management section.
3. Change the range of port numbers listed for ClientPortRange keyname.

Creating and Applying Session Profiles with Policy Manager

For more information about creating and applying session profiles, see the Managing User Sessions chapter in the *eTrust SSO Administrator Guide*.

Working with MetaFrame Application Migration

If you have Citrix MetaFrame installed, you can use eTrust SSO to allow users to migrate their open applications from one workstation to another. For more information, see the MetaFrame Application Migration section in the *eTrust SSO Administrator Guide*.

To partially automate the migration of MetaFrame applications with eTrust SSO, use the following session management settings:

- Enable session management (set SessMgmtEnable to Enabled or Required)
- Apply a policy to each user that sets the maximum number of eTrust SSO sessions to 1.

You will need a Tcl script that closes all applications launched from eTrust SSO.

Configure the Session Administrator

Update the Locations of the Log Files

There are two kinds of log file for the Session Administrator:

- The Session Administrator's communications with the Policy Server
- The Session Administrator's inner workings

Also, you can read the logs of the Tomcat server. These logs are written to the **CATALINA_HOME\logs** directory.

Note the use of the double back-slashes in the following instructions.

To Change the Location of the Communication Log File

1. Find the following file:

   ```
   C:\Program Files\CA\eTrust Identity and Access Manager\WEB-
   INF\logs\log4c_config.cfg:
   ```

2. In the log4c_config.cfg file, find the following line:

   ```
   log4cplus.appender.session_admin.File=C:\\Program Files\\CA\\eTrust
   Identity and Access Manager\\WEB-INF\\logs\\SessionMgtGUI_C.log
   ```

3. Change the path. For example, you could change it to:

   ```
   c:\\mydir\\logfiles\\mylogfile.txt
   ```

To Change the Location of the Session Administrator Log File

1. Open the following file:

   ```
   C:\\Program Files\\CA\\eTrust Identity and Access Manager\\WEB-
   INF\\logs\\log4j_SesMgt.lcf
   ```

2. Find the following line:

   ```
   log4j.appender.R.File=C:\\Program Files\\CA\\eTrust Identity and Access
   Manager\\WEB-INF\\logs\\SessionMgtGUI_J.log
   ```

3. Change the line to refer to a different file location. For example:

   ```
   log4j.appender.R.File=c:\\mylogdir\\mylogfile.txt
   ```

Session Management Settings

There are two ways to configure session management. Also, you can configure a backup method in case the main method fails.

- **Method 1: Direct Notification (Default)**—To terminate a session, the Policy Server sends a message directly to the SSO Client. This is the faster method of session termination.
- **Method 2: Terminate Message in Heartbeat Response**—The SSO Client sends a regular heartbeat to the Policy Server, and the Policy Server responds. To terminate a session, the Policy Server includes a message in one of its heartbeat responses. This is slower, but it can be used in systems that contain internal firewalls or gateway computers that affect IP addressing.
- **Backup Method: No Heartbeat Heard**—The SSO Client terminates a user session if the Policy Server does not reply to a certain number of heartbeats. This is useful as a backup in case the main method fails

Chapter

11 Implementing Password Agents

This chapter explains how to install the following components:

- Password Synchronization Agent for Windows
- Password Synchronization Agent for Mainframe
- One Time Password Agent for UNIX

Password Synchronization Agents

This section describes how to install the Password Synchronization Agents (PSA). For more information about the PSA, see the "Managing Passwords" chapter of the *Administrator Guide*.

Before You Begin

The Before You Begin Section is designed to guide you through what you need to know before you install the Policy Manager. In addition to the information in this section, always make sure you review your implementation plan and take note of any specific requirements.

Decide on a Method of Installation

This section explains each type of installation to help you choose which method you should use.

The Password Synchronization Agents (PSA) both Windows and Mainframe, can be installed by one of two methods:

Graphical installation wizard – Windows

The installation wizard leads you through the various steps required for installing the PSA. Use this method to familiarize yourself with the installation options.

Silent installation - Windows

Using the command line, you can silently install the PSA. You can also use this method to push the installation to remote computers.

Pre-Installation Checklist

Use this checklist to make sure you have performed all pre-installation review tasks:

- ❑ Ensure that all system requirements are met before you begin installing the Policy Manager. For a complete list of system requirements, see the product Readme file.

- ❑ Ensure that all the necessary prerequisite components have been installed and are functioning properly. Specifically, be sure that the following components have been installed and tested:

  - eTrust IAM Common Components
  - Policy Manager

- ❑ Ensure that you know the name of the computer or computers that you are installing the PSA on.

- ❑ Ensure that all system requirements are met before you begin installing the Policy Manager. For a complete list of system requirements, see the product Readme file.

- ❑ Ensure that all the necessary prerequisite components have been installed and are functioning properly. Specifically, be sure that the eTrust IAM Common Components have been installed. Test each component to be sure that it works.

- ❑ Ensure that the computer you are installing the PSA on has TCP/IP communications with the Policy Servers computers.

- ❑ Ensure that you have the following information:

  - Name of the Policy Server computers
  - Name of the Policy Server administrator
  - AUTHHOST entry
  - Name of the Primary Domain Controller
  - Name of the User Data Store on the Policy Server

Windows Password Synchronization Agent

This section explains how to install the Windows Password Synchronization Agent

Graphical Wizard Installation

To install the Policy Manager component of eTrust SSO using the graphical wizard, follow these steps:

1. Insert the product installation CD into your CD-ROM drive.

   If you have Autorun enabled, the Product Explorer automatically displays. Otherwise, navigate to the CD-ROM drive and double-click the PE_i386.EXE file.

2. From the Product Explorer main menu, select eTrust Single Sign-On Password Synchronization Agents, Windows Password Synchronization Agent, and click Install.

3. Follow the wizard prompts and when you are done, click Install to start the PSA installation.

Silent Installation

To install the Password Synchronization Agent (PSA) using the silent installation, follow these steps:

1. Open a command prompt and navigate to the Password Synchronization Agent folder on the eTrust SSO CD.

2. From the command prompt, enter:

   ```
   setup.exe /s /v"/qn <options>"
   ```

   For information about what values you can specify, see the Command Line Settings section in this chapter.

   Note: In order to execute a silent installation you have to accept the license agreement. The setting required for accepting the license agreement and silently installing the authentication agent can be found at the bottom of the license agreement available when running the installation wizard.

Command Line Settings

The command line settings for installing the PSA are:

Setting	Description
/s	Hides the initialization dialog.
/v	Passes parameters and property settings to the installation. It applies to all the parameters and properties listed in this table except /s. Place any parameters you wish to pass to the installation within quotes ("").
/L	Defines the full path and name of the installation log file. Use the mask * to log all available information. For example: `/L* C:\log.txt`
/qn	In conjunction with the /s parameter, used to initiate a silent installation. **Note:** You need to use the *license_accept* property to execute a silent installation.
license_accept	*license_accept* is the setting required for accepting the license agreement and silently installing the authentication agent. The actual setting you need to use can be found at the bottom of the license agreement that is available when running the installation wizard.
SERVERNAME	Specifies the name of the Policy Server. Use the computer name or IP address.
PSAADMINAUTHHOST	The authentication host used by the PSA for SSO authentication.
ADMINUSER	Specify the Administrator defined on the Policy Server that is used to set up the trust relationship. For example, ps-admin.
ADMINPWD	Specify the administrator password on the Policy Server. For example, the password for ps-admin.

Setting	Description
PDC	Specify the synchronization application. By default this is your Primary Domain Controller (PDC). If you specify the name of the domain, use the NETBIOS domain name, not the FULL DNS name. For example: NETBIOS domain name = AC-AU01 FULL DNS name = acmecorp.com
USERDATASTORE	Specify the name of the user data store defined on the Policy Server. This is where the users whose passwords will be synchronized are stored.
SEARCHFILTER	Search filter that is used to locate a specific user in the data store. Do not use the search filter if you do not have a hierarchical structure.
INSTALLDIR=[location]	Specifies the location where the Policy Manager will be installed.

Mainframe Password Synchronization Agent

This section explains how to install the Mainframe Password Synchronization Agent

Graphical Wizard Installation

To install the Policy Manager component of eTrust SSO using the graphical wizard, follow these steps:

1. Insert the product installation CD into your CD-ROM drive.

   If you have Autorun enabled, the Product Explorer automatically displays. Otherwise, navigate to the CD-ROM drive and double-click the PE_i386.EXE file.

2. From the Product Explorer main menu, select eTrust Single Sign-On Password Synchronization Agents, Mainframe Password Synchronization Agent, and click Install.

3. Follow the wizard prompts and when you are done, click Install to start the PSA installation.

Silent Installation

To silently install the Mainframe Password Synchronization Agent (PSA), follow these steps:

1. Open a command prompt and navigate to the Password Synchronization Agent folder on the eTrust SSO CD.

   ```
   SSO\syncagents\mainframe
   ```

2. From the command prompt, enter:

   ```
   setup –options-record C:\responsefile.txt
   ```

   This command will start the wizard and record everything you enter while you install the PSA.

3. Type the silent installation command and invoke the response file you have recorded.

   ```
   setup –options C:\responsefile.txt –silent
   ```

   If you want to create a log of this installation, you can use the optional parameter `–log @ALL`, for example:

   ```
   setup –options C:\responsefile.txt –silent –log @ALL
   ```

One Time Password Agent

This section explains how to install the One Time Password (OTP) for UNIX.

After you have installed the OTP agent you can configure it. For information about configuring the OTP, see the “Managing Passwords” chapter in the *Administrator Guide.*

UNIX OTP

To install the One Time Password Agent (OTP), follow these steps:

1. From the command prompt navigate to the UNIX OTP agent folder on the eTrust SSO CD.

   ```
   SSO/Agents/OTP/UNIX
   ```

2. From the command prompt, enter:

   ```
   ./install_seotp <options>
   ```

   This will install the agent in interactive mode. For information about what values you can specify or to perform a silent installation, see the Command Line Settings section in this chapter.

   Note: In order to execute a silent installation you have to accept the license agreement. The setting required for accepting the license agreement and silently installing the authentication agent can be found at the bottom of the license agreement available when running the installation wizard.

UNIX OTP Command Line Settings

Setting	Description
-d <*target directory*>	Specifies the installation directory.
-h/-help	Provides help.
license_accept	*license_accept* is the setting required for accepting the license agreement and installing the authentication agent. The actual setting you need to use can be found at the bottom of the license agreement that is available when running the installation wizard.
-noserver	Specifies that this is not a NIS or a DNS server.
-s	Specifies that the installation is in silent mode.
-server	Specifies that this is a NIS server.

Chapter

12

Implementing Citrix Application Migration

This chapter explains how to set up Citrix MetaFrame application migration. Citrix MetaFrame application migration within eTrust SSO refers to the functionality that lets users transfer an application session launched through eTrust SSO from one workstation to another. Throughout this chapter we will refer to this functionality as 'application migration.'

This functionality is only available when you deploy eTrust SSO within a Citrix MetaFrame client-server environment. Citrix products are sold independently of eTrust SSO.

Client Experience of Application Migration

Using 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.

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. The doctor can simply log on to workstation B, launch the application manager from his list of SSO applications, put Patient History into 'suspend mode' and reopen Patient History on the new workstation. The application automatically opens exactly where the doctor was last working.

Overview of Application Migration Installation

This section is a summary of the steps that you need to set up application migration using eTrust SSO. The rest of this chapter explains each step in detail. We recommend that you work through this chapter in the order it is written until you understand the process fully:

1. Check that you have all the pre-requisite software, access and logons and fill in the Pre-installation Checklist
2. Install the SSO Client on the Citrix MetaFrame Server
3. Install the SSO Client on the ICA Client workstation
4. Write Script A: This is the script you must write to launch the published application connection on the ICA Client computer
5. Write Script B: This is the script you must write to launch the SSO-enabled application on the MetaFrame Server computer
6. Define Script A on the Policy Server
7. Define Script B on the Policy Server
8. Create an SSO-enabled published application on the MetaFrame Server computer (this uses script B)
9. Create an ICA connection on the ICA Client computer to the published application on the MetaFrame Server (this uses script A)
10. Define the logon credentials for the user for both scripts

Example Applications

To help you understand this process, we have used Application Manager and Calculator as examples that are described after every step in the process. At the end of this chapter you should be able to migrate these two applications.

- You will probably already have Calculator installed on your computer as part of a standard Windows setup.
- You will install Application Manager automatically when you install the SSO Client installation on the Citrix MetaFrame Server later in this chapter. For more information about Application Manager see the MetaFrame Application Manager section later in this chapter.

Pre-installation Considerations

This section outlines all the software, connections and access rights you need to set before you start implementing application migration.

Prerequisite Software

You must have the following software installed and operational before you can set up application migration:

- Citrix MetaFrame server installed on at least one server machine (Windows Server XP or 1.8)
- ICA Client installed on at least two workstations (Windows 2000 or XP)
- Policy Server installed on a server machine
- Policy Manager installed on a workstation (or server) and connected to the Policy Server
- Authentication method (for example, native SSO authentication)

Prerequisite Access and Logons

You must have access and logon information set up as follows.

- Administrator logon details for the Policy Server
- Administrator logon details for the Citrix Server
- SSO user logon details to SSO
- SSO user logon details for the Citrix MetaFrame Server

There is space to write these details on the Pre-Installation Checklist.

Note: Every SSO user must have a unique logon to the Citrix MetaFrame Server.

Pre-Installation Checklist

This is a checklist for all the information that you will need in order to implement application migration. Throughout this chapter you will be prompted to write information on this page, so you may want to print it out and write on it.

Be careful to protect password security. You may not want to write passwords on this piece of paper.

□ Policy Server machine name ____________________

□ Policy Server administrator username ____________________

□ Policy Server administrator password ____________________

□ Citrix MetaFrame machine name ____________________

□ Citrix MetaFrame administrator username ____________________

□ Citrix MetaFrame administrator password ____________________

□ Citrix MetaFrame test user username ____________________

□ Citrix MetaFrame test user password ____________________

□ SSO test user data store ____________________

□ SSO test user username ____________________

□ SSO test user password ____________________

The following refers to logon Scripts A and B. You must write a Script A **and** a Script B for **every** application that you want users to be able to migrate. We have provided you with example scripts that are listed here and are explained in this chapter.

□ Example application name `Application Manager`

□ Example Script A name `appman_script_a.tcl`

□ Example Script B name `appman_script_b.tcl`

□ Example application name `Calculator`

□ Example Script A name `calc_script_a.tcl`

□ Example Script B name `calc_script_b.tcl`

Install Application Migration

Install the SSO Client on an ICA Client Computer

This procedure tells you how to install the SSO Client on a Citrix ICA Client machine.

1. From the eTrust Single Sign-On Product Explorer wizard choose **Single Sign-On Client**.

   The wizard should appear automatically when you insert the eTrust SSO disk. If not, open Windows Explorer and navigate to the CD-ROM directory and double-click the PE_i386.exe file.

2. Follow the prompts to install, but make sure you:

   - Choose **Custom** installation and choose the options that are appropriate for your environment
   - Choose **I'm installing eTrust SSO on an ICA Client Workstation** when prompted
   - Choose authentication method that users must use

   The SSO Client will now be installed on the ICA Client machine.

Install the SSO Client on the Citrix MetaFrame Server

This procedure tells you how to install the eTrust SSO Client on the Citrix MetaFrame server.

1. Go to Windows Start, Control Panel, Add or Remove Programs, Add New Programs.

2. Browse the eTrust SSO installation CD to the SSO Client folder and select setup.exe, then click Finish.

   This will start the SSO Client installation wizard.

3. Follow the prompts to install, and accept default values but make sure you:

   - Choose **Custom** installation
   - Choose **I'm installing eTrust SSO on a Citrix MetaFrame Server**.
   - Do not choose the SSO Client to run in Toolbar Mode.

   The SSO Client will now be installed on the Citrix MetaFrame Server machine.

   Note: You might want to consider making sure that the ssoagent.exe process is closed when the ssointrp.exe process ends in the Citrix session, when Script B is completed. To do this you should go to the [SSO Interpreter] section of the SsoClnt.ini file and set CloseAgentOnExit=yes.

Write Script A

This procedure tells you how to write a Script A. Every application that you want SSO users to be able to migrate must have its own Script A. A Script A runs on the ICA Client machine and launches the Citrix published application connection.

1. Open a text editor and write Script A in Tcl.

   You will need this name later when you are making your ICA Client connection.

2. Save the Script A in the Scripts directory on the Policy Server.

   Be default, the Scripts directory is found at:
   `C:\Program Files\CA\eTrust Policy Server\Scripts\`

Examples of Script A

This section shows you two examples of Script As, one for Application Manager and one for Calculator.

Here are some things you should know about the following example Script As in this section:

- These are example scripts only and you will need to customize these scripts to suit your environment. For example, you may need to increase or decrease the SSO sleep time.
- The underlined text in these examples represents the published application name that is defined on the Citrix MetaFrame server (you do not need to underline any text in your script). These names **must** match each other in this script.
- The login name and password referred to in this script are the credentials that the user uses to log on to the Citrix MetaFrame Server. These credentials must be unique for each SSO user.
- These scripts assume that the ICA Client is installed in the following location on the workstation: C:\Program Files\Citrix\ICA Client\pn.exe
- These example script names are written on the example Pre-Installation Checklist at the start of this chapter.

Application Manager Example Script A

Here is an example Script A for Application Manager to run in a Remote Desktop Citrix environment. This script will not work in a Seamless Windows Citrix Environment.

Application name:	Application Manager
Script A name:	appman_script_a.tcl

```
sso run -path {C:\\Program Files\\Citrix\\ICA Client\\pn.exe /APP:"Application_Manager"}
sso lockinput
sso window -titleglob "Application Manager - Citrix ICA Client"
sso sleep -time 4
sso type -text "$_LOGINNAME"
sso type -text "{tab}"
sso type -text "$_PASSWORD"
sso type -text "{enter}"
sso unlockinput
```

For examples of more complex and robust scripts, see the Example Scripts section at the back of this chapter.

Calculator Example Script A

Here is an example Script A for Calculator to run in a Remote Desktop Citrix environment. This script will not work in a Seamless Windows Citrix Environment.

Application name:	Calculator
Script A name:	calc_script_a.tcl

```
sso run -path {C:\\Program Files\\Citrix\\ICA Client\\pn.exe /APP:"Calculator"}
sso lockinput
sso window -titleglob "Calculator - Citrix ICA Client"
sso sleep -time 4
sso type -text "$_LOGINNAME"
sso type -text "{tab}"
sso type -text "$_PASSWORD"
sso type -text "{enter}"
sso unlockinput
```

For examples of more complex and robust scripts, see the Example Scripts section at the back of this chapter.

Write Script B

This procedure tells you how to write a Script B. Every application that you want SSO users to be able to migrate must have its own Script B. A Script B runs on the Citrix MetaFrame Server and launches the SSO-enabled application. This script represents standard SSO functionality, but it is defined as a hidden application on the Policy Server.

1. Open a text editor and write Script B in Tcl.
2. Save the Script B in the Scripts directory on the Policy Server. For example:

   ```
   C:\Program Files\CA\eTrust Policy Server\Scripts\appman_script_b.tcl
   ```

Examples of Script B

This section shows you two example Script Bs, one for Application Manager and one for Calculator.

Here are some things you should know about the following example Script Bs in this section:

- These are example scripts only and you will need to customize these scripts to suit your environment.
- You should write this script as if it was launching an application on a local workstation (normal eTrust SSO functionality).
- This is a simple example script that does not require a username and password. Most SSO-enabled applications would require a username and password.
- The scripts assume that Application Manager and Calculator are located at the defined locations. The M: drive may be a different drive letter on your Citrix MetaFrame server.
- These example script names are written on the example Pre-Installation Checklist at the start of this chapter.

Application Manager Example Script B

Here is an example Script B for Application Manager. This script will work in either a Seamless Windows Citrix environment or a Remote Desktop Citrix environment.

Application name:	Application Manager
Script B name:	appman_script_b.tcl

```
sso run -path {M:\\Program Files\\CA\\eTrust SSO\\Client\\mf_appl_migration.exe}
```

Calculator Example Script B

Here is an example Script B for Calculator. This script will work in either a Seamless Windows Citrix environment or a Remote Desktop Citrix environment.

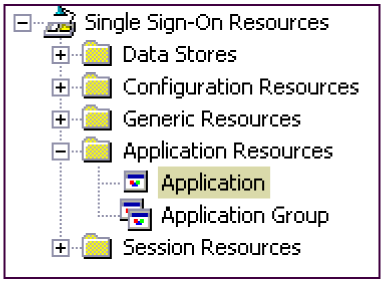
Application name:	Calculator
Script B name:	calc_script_b.tcl

```
sso run -path {M:\\WINNT\\system32\\calc.exe}
```

Define Script A on the Policy Server

This procedure tells you how to define a Script A on the Policy Server. The Script A launches the Citrix published application connection on the ICA client machine.

1. Launch the Policy Manager
2. In the Program Bar navigate to Single Sign-On Resources, Application Resources, Application.



3. Right-click in the Application Window and choose New.
   The Create New APPL Resource – General dialog appears.
4. Fill in the details of the application.

   For example:

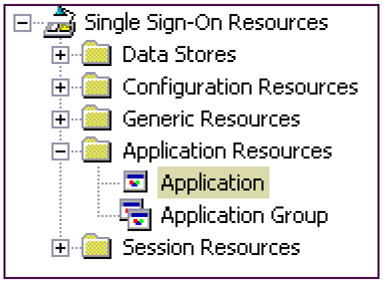
Name:	Application Manager Script A
Caption:	Application Manager
Type:	Desktop Application

   Note: The caption is what the user sees in their eTrust SSO Application List.
5. Click the Scripting button.
   The Scripting dialog appears.
6. Enter the Script A name in the Script File field, and then click OK.
   For example, appman_script_a.tcl.
7. Select the Authorize icon.
   The Create New APPL Recourse – Authorize dialog appears.
8. Right-click and choose Add.
   The Add Access Control List Accessor dialog appears.
9. Choose the users who will have access to this application, and then click OK.
   These should be the same users that you allocate to have access to Script B.

Define Script B on the Policy Server

This procedure tells you how to define a Script B on the Policy Server. The Script B must be defined as a hidden application. This script will launch the SSO-enabled application on the Citrix Server.

1. Launch the Policy Manager
2. In the Program Bar navigate to Single Sign-On Resources, Application Resources, Applications.



3. Right-click in the Application Window and choose New.
   The Create New APPL Resource – General dialog appears.
4. Fill in the details of the application.

   For example:

Name:	Application Manager Script B
Caption:	Application Manager (Hidden)
Type:	Desktop Application

5. Click the Scripting button.
   The Scripting dialog appears.
6. Enter the Script B name in the Script File field and click OK.
   For example: appman_script_b.tcl.
7. Click the Attributes icon.
   The View or Set APPL Properties – Attributes dialog appears.
8. Choose the Hidden checkbox.
9. Select the Authorize icon.
   The Create New APPL Recourse – Authorize dialog appears.
10. Right-click and choose Add
    The Add Access Control List Accessor dialog appears.
11. Choose the user(s) who will have access to this application and click OK when you are finished. This user(s) should be the same users that you allocated access to Script A.

Create an SSO-Enabled Published Application

This section tells you how to configure an application hosted on the Citrix Server so that it can be accessed from a user's eTrust SSO list on the ICA Client machine.

These instructions apply to Citrix XP. You can also configure Application Migration with Citrix 1.8.

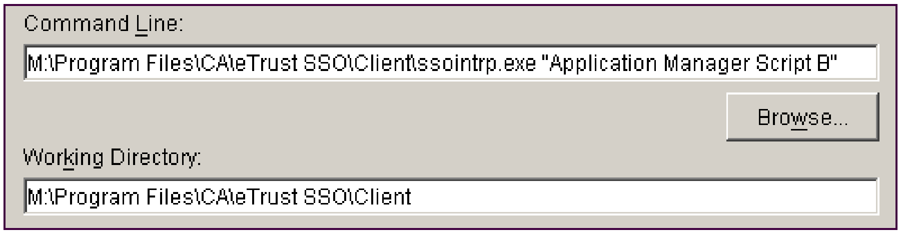
1. Open the Citrix Management Console on the Citrix MetaFrame Server machine.
2. Choose the Publish Application icon.

   This launches the Application Publishing Wizard.
3. Enter the display name and descriptions for the application and press Next. For example:
   - Display Name: Application Manager
     This is the name referred to in Script B. This name is not visible to end users.
   - Application Description: Application Manager
     The display name is not visible to end users.

   The Specify What to Publish dialog appears.
4. In the Specify What to Publish dialog, chose the following:
   - Application (option button)
   - Command Line: Browse for ssointrp.exe then type the exact name of the application that has script B assigned to it (you defined this using the Policy Manager)
   - Working Directory: This is the folder in which the ssointrp.exe is stored. This will be populated automatically if you browse for ssointrp.exe.

   For example:

   ```
   C:\Program Files\CA\eTrust SSO\Client\ssointrp.exe “Application Manager Script B"
   ```



Command Line: M:\Program Files\CA\eTrust SSO\Client\ssointrp.exe "Application Manager Script B"

Working Directory: M:\Program Files\CA\eTrust SSO\Client

   When you click Next the Program Neighborhood Settings dialog appears.

5. Continue through the Publish Application screens until you get to the Specify Servers dialog appears (you can accept the default information for all intervening screens).
6. Add all servers that should be able to run the published application.

When you click Next the Specify Users dialog appears.

7. Add all users or user groups that need access to this application.

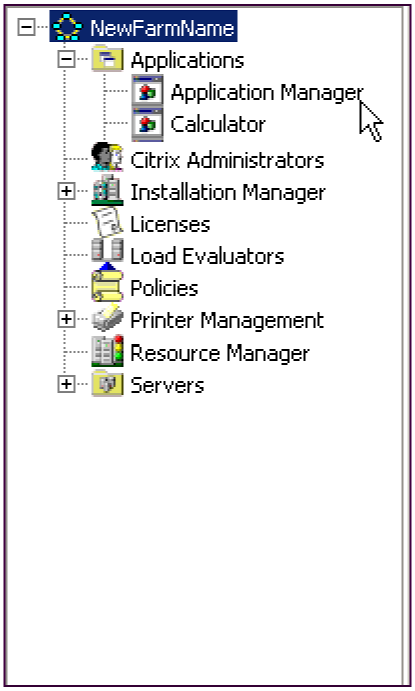
   Note: *Do not* choose Allow Anonymous Connections, because application migration only supports explicit applications.

   When you click Next the Specify File Type Associations dialog appears.

8. Specify any associations that you require (none by default).

   When you click Finish you return to the Citrix Management Console.

9. Check that the application that you just published is visible in the Applications folder. You should see the Display Name that you entered in step 3.



Create an ICA Connection To The Published Application

This procedure tells you how to make the ICA Client connection to the MetaFrame server application.

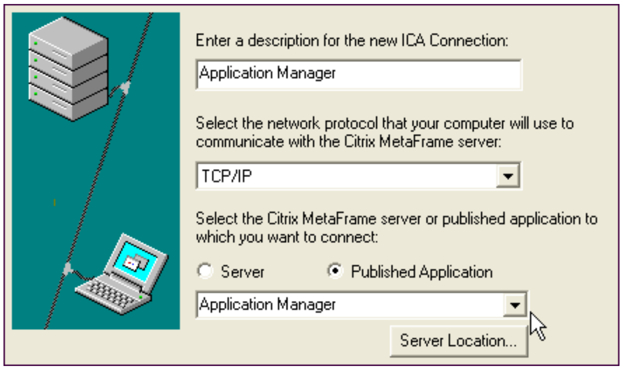
1. On the ICA Client machine, open the Citrix Program Neighborhood from the Start menu.
2. Choose Application Set Manager
3. Choose Custom ICA Connections
4. Choose Add ICA Connection

   The Add New ICA Connection wizard appears
5. Choose the type of connection (this will usually be the LAN option) and click Next.
6. Enter the appropriate information, and make sure that you choose the Published Application option, then click Next.

   For example:

   - Description: Application Manager

     This description should exactly match the name of the published application defined in Script A. This is the Application Name on your Pre-Installation Checklist.
   - Protocol drop-down: TCP/IP
   - Option: Published Application
   - Application drop-down: Application Manager
     (This drop-down menu shows the Display Names entered when you published the application on the Citrix MetaFrame Server).



Enter a description for the new ICA Connection:

Application Manager

Select the network protocol that your computer will use to communicate with the Citrix MetaFrame server:

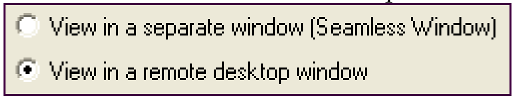
TCP/IP

Select the Citrix MetaFrame server or published application to which you want to connect:

○ Server ● Published Application

Application Manager

7. Choose View in a remote desktop window and click Next.



○ View in a separate window (Seamless Window)

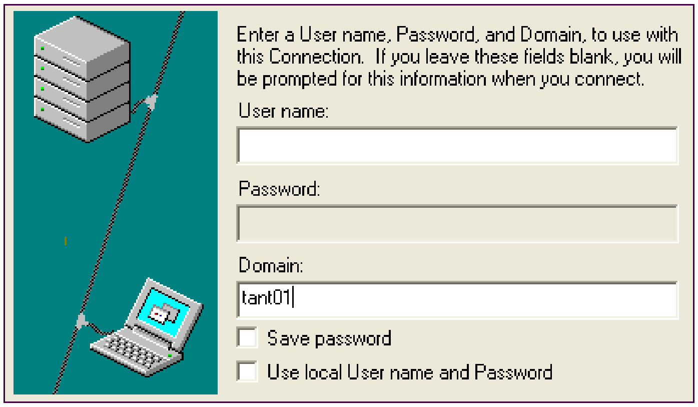
● View in a remote desktop window

***Important!** You must choose this option for MetaFrame Application Manager to work because there must be a separate Citrix session for **every** application. If you do not want to use the Application Manager and want your end users to run all of their applications in one Citrix session, you may chose to run the published applications in a Seamless Window.*

8. Choose the encryption level and click Next.

9. You must uncheck Use local User name and Password and fill in the fields as show:

User name:	[Leave blank]
Password:	[Leave blank]
Domain:	[Specify the domain for the connection]



Enter a User name, Password, and Domain, to use with this Connection. If you leave these fields blank, you will be prompted for this information when you connect.

User name:

Password:

Domain: tant01

□ Save password

□ Use local User name and Password

This ensures the logon dialog is displayed when the ICA Client connection is launched. Script A will be used to automatically log the SSO user on to the Citrix Server using the relevant Citrix logon credentials defined on the Policy Server in the following section.

10. Finish the setup, you can accept the defaults.

More Information About the Logon Window

The application logon dialog is only displayed when a new Citrix Session is established. The logon script A will insert the user's authentication credentials.

In a Remote Desktop Windows environment a new Citrix Session is established for every application that is launched on the Citrix MetaFrame Server.

In a Seamless Windows environment a new Citrix Session is only established for the first application that is launched - all other applications are considered to be part of this first Citrix Session.

Define the Application Credentials for Each User

This procedure tells you how to define the logon credentials for the SSO user to log on to the:

- Citrix MetaFrame server (Script A)
- SSO-enabled published application (Script B)

1. Launch the Policy Manager and navigate to Single Sign-On Users, and find the test user.
2. Right-click on the test user and choose Properties.

   The View or Set User Properties – General dialog appears.

5. Choose Application List icon

   The View or Set User Properties – Application List dialog appears.

6. Choose the Script A application and click the Update Login Information button.

   The Update Login Information dialog appears.

7. Enter the appropriate username (login name) and password for this user on the domain that will let the user access the published application for access to the Citrix MetaFrame server then click OK.

   Remember that this is the script that launches the published application link on the ICA client machine, so these credentials are what the user would normally enter to logon to the Citrix MetaFrame server to access the application.

   Note: Every SSO user must have their own unique logon details to the Citrix MetaFrame Server so that SSO can recognize individual sessions.

8. Choose the Script B application and click the Update Login Information button.

   The Update Login Information dialog appears.

9. Enter the appropriate username (login name) and password for this user for the published application that runs on the MetaFrame Citrix server then click OK

   Note: In our example Script B for the Application Manager, we do not make reference to a username and password, because the Application Manager does not have a logon screen. You would normally need to specify a username and password for the application that runs Script B. This Update Login Information dialog is where you enter the username and password that would be inserted into Script B.

Test Application Migration

This procedure tells you how to test application migration. This is the procedure that end-users would follow.

1. Using the test user, logon and authenticate to SSO on the ICA client machine. This means that you will have a current SSO ticket.

2. Choose the application from the list of SSO-enabled applications.

   For example, Calculator, if you have defined it.

   The scripts should now launch the application.

3. Enter some numbers into Calculator. Remember these numbers so that you can test that you are opening the same session on the new machine.

4. Using the test user, logon and authenticate to SSO on a second ICA client machine.

5. Launch Application Manager from the list of SSO-enabled applications.

   The Application Manager launches and you will see Calculator under the list of published applications.

7. Click the Disconnect button to put the application into suspend mode. You should notice the Calculator application session close on the first ICA Client machine.

8. Launch Calculator from the list of SSO-enabled applications.

   You should see the same session of Calculator with the numbers that you entered in step three.

Troubleshooting

Here are some trouble shooting tips to help you if you cannot get Application Migration working.

- Ensure the logon credentials that you used to access the Citrix MetaFrame Server are valid and that the user has the relevant Citrix privileges to run the published application.
- Make sure that you have a current valid SSO ticket by logging on the SSO user again.
- Check that the MetaFrame Manager has the Remote Procedure Call (RPC) Windows Service on the Citrix MetaFrame Server is running (this is only necessary for the Application Manager program).
- Check that every Citrix MetaFrame server that hosts published applications is listed in the SsoMetafrrame.ini file. These servers should be listed as shown:

  ```
  [Simple_Config]
  MetaframeServers=<names of servers, space separated>
  ```

  This is only necessary for the Application Manager program.
- Check the Tcl logon scripts
- Check the application script names in the Policy Manager
- Check that the Description you entered when you made the ICA connection to the Published application matches the names that you entered in script A.

If you are still having problems running the Application Manager, you can inspect the MetaFrameLog.cfg in the SSO Client directory on the Citrix Server.

MetaFrame Application Manager

The MetaFrame Application Manager (Application Manager) is a software tool that lets users administer their own sessions. Whether you give users access to this tool is a choice you need to make based on how much control you want to give to your end users.

The design of the Application Manager is based on a Citrix utility that is normally only available to administrators. The Application Manager lets users view all the instances of each SSO-enabled software package that they are currently logged onto.

Although the Application Manager will work in both a Remote Desktop and Seamless Window environment, its full functionality is only realized in a Remote Desktop Window environment. This is because the Application Manager relies on a Citrix session hosting a single SSO application, not a Citrix session hosting multiple SSO applications (which is what happens in a Seamless Window environment).

Application States

The Application Manager lets users put application sessions into one of three states:

Application State	Result
Connected	This means that the application is currently running on a workstation.
Disconnected	This means that the application is 'suspended' but not closed and can be migrated to another workstation. Do not confuse this with "terminated".
Terminated	This means that the application has been closed and is not available to be migrated to another workstation.

Application Manager Installation

The Application Manager runs on the Citrix Server. You will automatically install the Application Manager when you install the SSO Client on the Citrix Server. You then have the option of adding this as an SSO-enabled application to each user's SSO application list.

Application Migration Configuration

This section tells you about ways you can configure Application Migration and a little bit more about how it works with the SSO Client.

Suspend ICA Client Connections During SSO Logoff

When the SSO Client is installed on the ICA Client workstations, a Tcl script called Citrix_SSO_Logoff.tcl is installed in the SSO Client directory. This script automatically converts all open ICA Client connections to the “disconnected” state on the Citrix MetaFrame server when the user logs off SSO on that workstation.

If the same user then logs on to SSO on another ICA Client workstation and starts one of the disconnected applications, the previous instance of that application will be returned to the user.

Shared Workstations and Session Management

Application Migration functionality is often used in conjunction with session management in a shared workstation environment. If you give every user a session profile that limits them to one SSO session and automatically closes their previous instance of eTrust SSO then applications will “follow” users from workstation to workstation using the Citrix_SSO_Logoff.tcl logoff script discussed in the previous section.

For more information about shared workstation mode see the “Working with the SSO Client” chapter of the *eTrust SSO Administrator Guide.*

For more information about managing user sessions see the “Managing User Sessions” chapter of the *eTrust SSO Administrator Guide*.

Script A Samples

Here are some Script A examples for Application Manager and Calculator. These are similar to the examples shown in the Write Script A section earlier in this chapter, but are more robust and complex.

These are example scripts only and you may need to change these scripts to suit your environment.

Calculator in Seamless Window Mode

Here is an example of a robust Script A written for Calculator that will run in a Seamless Windows Citrix environment.

Application name:	Calculator
Script A name:	calc_script_a.tcl

```
# Is the application already running? If yes, set focus to ERRORMODE resume
set wintitle [sso window -titleglob "Calculator - \\\\Remote"]

# If not launch the ICA Client connection to run the published application
if {! [string match "$wintitle" "Calculator - \\Remote"]}
{
       set _ERRORMODE stop

       sso lockinput
       sso run -path {C:\\Program Files\Citrix\\ICA Client\\pn.exe /APP:Calculator}

       # Does the user already have a Citrix Session established?
       set _ERRORMODE resume
       set loginwintitle [sso window -titleglob "Log On to Windows - \\\\Remote"]

       # If not (i.e. prompted for Citrix login credentials), login to Citrix
       # to establish Citrix session
       if {[string match "$loginwintitle" "Log On to Windows - \\Remote"]}
       {
                set _ERRORMODE stop
                sso sleep -time 4
                sso type -text "$_LOGINNAME"
                sso type -text "{tab}"
                sso type -text "$_PASSWORD"
                sso type -text "{enter}"
       }
    sso unlockinput
}
set _ERRORMODE stop
```

Here is an example Script A for Calculator to run in a Remote Desktop Citrix environment.

Application name: Calculator
Script A name: calc_script_a.tcl

```
# Is the application already running? If yes, set focus to ERRORMODE resume
set wintitle [sso window -titleglob "Calculator - Citrix ICA Client"]
set _ERRORMODE stop

# If not launch the ICA Client connection to run the published application and
login to Citrix
if {! [string match "$wintitle" "Calculator - Citrix ICA Client"]}
{
       sso lockinput
       sso run -path {C:\\Program Files\Citrix\\ICA Client\\pn.exe /APP:Calculator}
       sso window -titleglob "Calculator - Citrix ICA Client"
       sso sleep -time 4
       sso type -text "$_LOGINNAME"
       sso type -text "{tab}"
       sso type -text "$_PASSWORD"
       sso type -text "{enter}"
       sso unlockinput

}
```

Chapter

13 Implementing a Server Farm

This chapter explains how to set up a server farm for eTrust SSO for Windows.

A server farm is a system of multiple networked Policy Server computers. If you have more than one Policy Server within your company you should connect them together in a server farm. The data on each server can then be replicated to all the other servers in the farm.

The benefits of a server farm that has full replication and hot backup include:

- No need to maintain separate data stores
- Failover, which is the ability of a server to take over if one server goes offline, without affecting services

For further information about failover, see the “Working with Server Farms” chapter of the *eTrust SSO Administrator Guide*.

A computer that has a Policy Server installed on it is called a host computer.

Before You Begin

The Before You Begin section is designed to guide you through what you need to know before you install a server farm of Policy Servers.

Overview

The purpose of a server farm is to enable each server to send data to, and receive data from, every other server in the farm to allow backup and failover.

If you are installing a new server farm, and you have no existing Policy Servers, you can install all the servers from the IAM Common Components and specify each of the other servers in the server farm to automatically set up a server farm. After all the Policy Servers have been installed in this way, they will automatically communicate with each other and replicate data.

If you are adding servers to a server farm, you should follow the steps outlined in this chapter.

Pre-Installation Checklist

Please list the information outlined below to help you with the installation.

- □ List the name(s) of all Policy Server(s) that you want to include in the server farm.
- □ List the names of the eTrust Directory and eTrust AC data stores.
- □ Check that all servers are connected to the network and available to each other.
- □ If you intend to install the Policy Server and the Policy Manager on the same computer, make sure you refer to the Policy Manager and Policy Server on One Computer section of the "Implementing the Policy Manager" chapter in this guide.
- □ Ensure that your operating system produces a reliable and correct timestamp for the local time-zone. If it does not, the product may not work. For example, the operating system clock of a Policy Server host in New York is set to US Eastern Daylight Time (EDT), whilst the operating system clock of an LDAP Authentication Agent host in San Francisco is set to US Pacific Daylight Time (PDT).

Implementing a Server Farm

If you are installing eTrust SSO for the first time, you can implement a server farm of Policy Servers using the IAM Common Components installation.

While you are installating the IAM Common Components you must select "Custom" installation and when you get to the "Policy Server: Assign Computer(s)" screen you should specify multiple computers. These computers will then be configured as a server farm and each Policy Server can send and receive data from every other Policy Server in the farm.

For more information about installing the IAM Common Components see the "Implementing the IAM Common Components" chapter of this guide.

Upgrading a Server Farm

If you are upgrading your SSO server farm from either Policy Server 7.0 or SSO Server 6.5, you should follow these steps to upgrade successfully:

In this procedure, we will refer to the following computer names:

- Computer A = server farm member
- Computer B = server farm member

1. Run the IAM Common Components upgrade on all servers in the server farm.
2. Choose one of the Policy Servers in the server farm to be the master server.

   In this example, we will call Computer A the master server.
3. Perform an online backup using:

   ```
   dbmgr –backup <backup directory>
   ```
4. Shut down the eTrust AC services on Computer B, using the command:

   ```
   % secons -s
   ```
5. Transfer the data from step 3 to the following directory on Computer B.

   ```
   <eTrust AC>/data/seosdb
   ```
6. Restart eTrust AC on Computer B, using the command:

   ```
   % seosd -start
   ```
7. Restart the Policy Server service using the Window Services Manager.
8. Recreate the local Windows Administrator User on Computer B in the local eTrust AC Database using these steps:

   a. Launch the Policy Manager, connect to the Policy Server on Computer B using the Policy Server administrator user credentials (entered during installation).

      Note: If you cannot connect to Computer B, log into the Policy Server on Computer A using the Policy Manager. In the Resources Tab, select Authentication Host. Double-click on the EAC_Authhost resource. Select the 'Backward Compatibility' Tab and try to add the fully qualified domain name or short hostname of Computer B as a HOSTNAME property.

   b. In the eTrust Access Control tab, double-click on the Users icon.

   c. Enter the name of your local administrator on Computer B. This is normally 'Computer B\Administrator'.

   d. Click on the Advanced button, select the 'Create in eTrust Environment'.

   e. Click the User Attributes Tab and check the 'Administrator' box

9. Authorize the local Windows administrator user on Computer B to use Computer B's Terminal resource

   a. Launch the Policy Manager, connect to the Policy Server on Computer B using the Policy Server administrator user credentials (entered during installation).

   b. Go to the Terminals Resources tab

   c. Select either:

      - SSO Resources tab, Single Sign-On Resources, Configuration Resources, Terminal, or

      - AC resources tab, Access Control Resources, Common, Login Protection, Terminal

   e. Select properties on the terminal representing Computer B

   f. Click on the Authorize Tab , select '+' and add Computer B's local Windows administrator user (as created in Step 9), with 'full control' access.

10. On Computer B, log in to Windows as the local administrator. Check that you can connect to the local eTrust AC database via selang.

Adding a New Server Farm Member

If you are adding a Policy Server to an existing Server Farm, follow these steps:

In this procedure, we will refer to the following computer names:

- Computer A = master server
- Computer B = server farm member
- Computer C = new server farm member

1. Run the IAM Common Components installation on Computer C to install the Policy Server on Computer C. Specify Computer A and Computer B as part of the server farm when you install the Policy Server on Computer C.
2. After the installation completes successfully on Computer C, shut down the following services:
    a. Policy Server using the Windows Services Tab:
    Go to the Services Tab, find eTrust Policy Server, right-click and select 'Stop'
    b. eTrust AC, using:
    ```
    secons -s
    ```
    c. DSAs, using:
    ```
    dxserver stop PS_<Computer C>
    dxserver stop PSTD_<Computer C>
    ```
3. Re-run IAM Common Components installation CD on each of the existing server farm members, specifying Computer A, Computer B and Computer C as the server farm members.
4. Export the ps-ldap directory on Computer A using:
    ```
    % dxdumpdb -p "o=PS" ps > ldap.ldif
    ```
5. Perform an online backup using:
    ```
    dbmgr –backup <backup directory>
    ```
6. Transfer the data from step 5 to the following directory on Computer C
    ```
    <eTrust AC>/data/seosdb
    ```
7. Transfer the ldap.ldif file from Computer A to Computer C.
8. On Computer C, load in the exported LDIF data from Computer A into the ps-ldap directory on Computer C.
    a. Sort ldap.ldif
    ```
    % ldifsort ldap.ldif > newldap.ldif
    ```
    b. Load newldap.ldif into the directory on Computer C

```
% dxloaddb newldap.ldif ps
```

9. On Computer C, restart the following services

   a. DSAs, using:

      ```
      - dxserver start all
      ```

   b. eTrust AC, using:

      ```
      - seosd -start
      ```

   c. Policy Server - using the Windows Services Tab.

      Go to the Services Tab, find eTrust Policy Server, right-click and select 'Start'.

10. Recreate the local Windows Administrator User on Computer C in the local eTrust AC Database using these steps:

    a. Launch the Policy Manager, connect to the Policy Server on Computer C using the Policy Server administrator user credentials (entered during installation).

       Note: If you cannot connect to Computer C, log into the Policy Server on Computer A using the Policy Manager. In the Resources Tab, select Authentication Host. Double-click on the EAC_Authhost resource. Select the 'Backward Compatibility' Tab and try to add the fully qualified domain name or short hostname of Computer C as a HOSTNAME property.

    b. In the eTrust Access Control tab, double-click on the Users icon.

    c. Enter the name of your local administrator on Computer C. This is normally 'Computer C\Administrator'.

    d. Click on the Advanced button, select the 'Create in eTrust Environment'.

    e. Click the User Attributes Tab and check the 'Administrator' box

11. Authorize the local Windows administrator user on Computer C to use Computer C's Terminal resource

    a. Launch the Policy Manager, connect to the Policy Server on Computer C using the Policy Server administrator user credentials (entered during installation).

    b. Go to the Terminals Resources tab

    c. Select either:

       - SSO Resources tab, Single Sign-On Resources, Configuration Resources, Terminal, or
       - AC resources tab, Access Control Resources, Common, Login Protection, Terminal

    e. Select properties on the terminal representing Computer C

f. Click on the Authorize Tab , select '+' and add Computer C's local Windows administrator user (as created in Step 9), with 'full control' access.

12. On Computer C, log in to Windows as the local administrator. Check that you can connect to the local eTrust AC database via selang.

Removing a Server Farm Member

In this procedure, we will refer to the following computer names:

- Computer A = server farm member
- Computer B = server farm member
- Computer C = server to be removed

For each of the server farm members, you need to unsubscribe the unwanted server farm member. Therefore, to remove a Policy Server from a server farm, follow these steps on both Computer A **and** Computer B:

1. Unsubscribe Computer C from both Computers A and B using the following command on each computer:

   ```
   sepmd -u PS_PMDB <Computer C>
   ```

2. Re-run the IAM Common Components installation. Modify the installation to exclude Computer C.

3. Open `<eTrust Directory Install directory>/dxserver/config/knowledge/PS_Server.dxg>`

4. Comment out, or delete lines that contain:

   - `PS_<computer_C>.dxc`
   - `PSTD_<computer_C>.dxc`

5. Reload the DSA configuration:

   - `% dxserver init PS_<hostname>`
   - `% dxserver init PSTD_<hostname>`

   `Where <hostname> is Computer C or Computer B`

6. Log into the Policy server on any computer in the server farm via the Policy Manager and remove Computer C from the TERMINAL and AUTHHOST resources.

   Note: If necessary, uninstall the Policy Server on Computer C by running the IAM Common Components installation CD on that computer.

Chapter

14 Upgrading

This chapter explains how to upgrade from previous versions of eTrust SSO.

This table is a summary of the components used in the current and previous two eTrust SSO releases.

Function	Release 6.5	Release 7.0	Release 8.0
Administration Tools	▪ SSO Assistant ▪ selang	▪ Policy Manager ▪ Session Administrator ▪ selang	▪ Policy Manager ▪ IA Manager ▪ selang
Desktop Client	▪ SSO Client 6.5	▪ SSO Client 7.0	▪ SSO Client 8.0
Server Architecture	▪ SSO Server	▪ Policy Server 2.0	▪ Policy Server 8.0 ▪ Provisioning Server ▪ Web Application Server ▪ Directory Server (optional)
Authentication Agents	▪ Certificate ▪ Entrust ▪ Novell Netware ▪ SDI ▪ Safeword ▪ SSO ▪ Windows (NT)	▪ Certificate ▪ Entrust ▪ LDAP ▪ Novell Netware ▪ RSA SecurID ▪ Safeword ▪ SSO ▪ Windows (NT)	▪ Certificate ▪ Entrust ▪ LDAP ▪ Novell Netware ▪ RSA SecurID ▪ Safeword ▪ SSO ▪ Windows (NT)

Function	Release 6.5	Release 7.0	Release 8.0
Data Stores Windows	▪ eTrust Access Control 4.1 SP1	▪ eTrust Access Control 5.2 ▪ eTrust Directory 4.0 SP1	▪ eTrust Access Control 8.0 ▪ eTrust Directory 8.0 SP 1
Data Stores UNIX	▪ eTrust Access Control 5.0 SP2	▪ eTrust Access Control 5.1 ▪ eTrust Directory 4.0 SP1	▪ eTrust Access Control 8.0 ▪ eTrust Directory 8.0 SP1
Password Synchronization	▪ Windows PWS agent ▪ Mainframe PSW agent	▪ Windows PWS agent ▪ Mainframe PWS agent	▪ Windows PWS agent ▪ Mainframe PWS agent
One Time Passwords	▪ UNIX OTP Agent	▪ UNIX OTP Agent	▪ UNIX OTP Agent

Administration Tools Upgrade

This section explains how to upgrade each of the management tools.

SSO Assistant

The SSO Assistant was delivered with eTrust SSO 6.5. This administration tool is no longer supported. You should remove the SSO Assistant from your system. You should use the IA Manager and the Policy Manager instead.

For further information about uninstalling the SSO Assistant, see the "Uninstalling eTrust SSO" chapter in this guide.

Policy Manager

The Policy Manager was new to eTrust SSO 7.0 and has been updated for eTrust SSO 8.0. The Policy Manager is a Windows applications that should be installed on each Administrator's workstation. The Policy Manager is an important tool for configuring eTrust SSO.

Here is an overview of how to upgrade the Policy Manager:

1. Insert the eTrust SSO 8.0 Installation CD.
2. Select Policy Manager.

   The Policy Manager installation wizard appears.
3. Select Install.
4. Follow the prompts and select "Upgrading" when prompted

   The Installation Wizard detects that you have the old Policy Manager installed and will upgrade to the new version.

For more information about installing the Policy Manager, see the "Implementing the Policy Manager" chapter in this guide.

IA Manager

IA Manager is new to eTrust SSO 8.0. This is a web-based administration interface. The IA Manager is used by all the products in the eTrust IAM suite. This currently supplements the Policy Manager but does not replace it.

To use the IA Manager, administrators connect to the Web Application Server via their browser. The Web Application Server is installed from the eTrust IAM Common Components CD.

Here is an overview of how to install and connect to the IA Manager:

1. Insert the eTrust IAM Common Components Installation CD
2. Follow the prompts to install the eTrust IAM Common Components.
   As part of the eTrust IAM installation, you will configure and install the Web Application Server.
3. Once the eTrust IAM Common Components are installed, manually enter the following URL into your internet browser:

   ```
   https://<hostname>:<sslport>/CA/IAM/Manager/index.html
   ```

   Where <hostname> is the name of the computer acting as the Web Application Server is installed and <sslport> is the Apache Tomcat SSL port number (the default value is 8443).

For more information about installing and connecting to the IA Manager, see the “Implementing the eTrust IAM Common Components” chapter in this guide.

selang

Selang remains the command line language used for managing the eTrust Access Control data base. For more information about selang, see the *selang Command Reference Guide.*

Session Administrator

The Session Administrator was new to SSO 7.0. The Session Administrator has been incorporated into the IA Manager and is automatically upgraded when you install the IA Manager from the eTrust IAM Common Components CD.

Session Administration is configured using the Policy Manager. For more information about configuring Session Administration, see the “Implementing Session Administration” chapter in this guide.

For more information about installing the IA Manager, see the *Installing the eTrust IAM Common Components* chapter of this guide.

SSO Client Upgrade

There is a new SSO Client for eTrust SSO 8.0 and you should upgrade to the new SSO Client.

Here is an overview of how to upgrade the SSO Client on one machine:

1. This step is optional. Check the SsoClnt.ini settings to make sure there is enough information to automatically create a Server Set for the new SSO Client.

   For more information see the following section SsoClnt.ini File Change.

2. Insert the eTrust SSO 8.0 CD.
3. Follow the prompts and select “Upgrading” when prompted. This will install the new SSO Client over the old one.
4. Check that the SSO Client is working correctly. You may need to manually edit the SsoClnt.ini file.

For more information about installing the SSO Client, see the “Implementing the SSO Client” chapter in this guide.

SsoClnt.ini File Changes

When you upgrade the SSO Client, as much information as possible from your old SsoClnt.ini will be transferred to the new one, but the values need to be configured correctly for the upgrade to be seamless.

Your old SsoClnt.ini file will be backed up during the update and stored in %TEMP% folder (you can find out the location either by typing 'echo %TEMP%' from command prompt, or by looking up the value of the TEMP environment variable via Control Panel), under the file name SsoClnt.original.

The SsoClnt.ini file has changed significantly from 6.5 and 7.0 to 8.0. The biggest change is that the SsoClnt.ini has a new section called Server Sets. To create a valid server set from the old SsoClnt.ini file, all the authentication information must be correct.

To automatically create a server set from a 6.5 or 7.0 SsoClnt.ini file, make sure that the following keynames are filled in:

Old Section	Token	Value
[SSO]	Servers	List the Policy Server(s). For example: Servers=Pol_Svr_01
[ssoauth]	AuthMethods	List the authentication methods. For example: AuthMethods=SSO NT
[auth.XXX]	AuthHost	List the authentication servers for each authentication method that you have listed in AuthMethods. This is mandatory, or the server set will be deemed invalid. For example: [auth.SSO] AuthHost = Auth_Svr_01

For more information about server sets, see the “Implementing the SSO Client” chapter in this guide.

Added and Removed Tokens

This table lists which tokens and sections have been added for each new release since eTrust SSO 6.5 Sp2, and which have been deprecated.

Release	Added	Removed
7.0	Adfad	Adadsf
	[sso]\DisableShutdown	[Broker]
	[sso]\EngineRegisterTimeOut	[Broker]\IniBrokerURL
	[sso]\SysErrorMessage	[ssoauth]\CacheTickets
	[sso]\DataDirectory	[comm]\UseBlockingSockets
	[GINA]	[comm]\TimeOutRecv
	[GINA]\LogonBitmap	[comm]\TimeOutSend
	[GINA]\LogonTitle	[comm]\PostUnlockCmd
	[GINA]\LockedBitmap	
	[GINA]\LockedTitle	
	[GINA]\GinaPassThrough	
	[GINA]\logonCAD	
	[Logging]	
	[Logging]\ClientConfigFile	
	[Logging]\GinaConfigFile	
	[auth.NT]\AutoNetworkAuth	
	[auth.NOVELL]\AutoNetworkAuth	
	[auth.RSA]	
	[auth.RSA]\authhost	
	[auth.LDAP]	
	[auth.LDAP]\authhost	
	[SessionManagement]	
	[SessionManagement]\ClientPortRange	
	[StationLock]\LockScreenSaver	
	[StationLock]\GINAUnlockTimeout	
	[TrayMenu]\ItemMigrateMetaframeSessions	
	[TrayMenu]\ShowTrayIcon	

Release	Added	Removed
	[SSO Interpreter]\ClientWaitTime	
	[ToolBar]\BuildToolBar	
	[ToolBar]\AutoLogon	
	[ToolBar]\showMOTD	
	[MetaframeMigration]	
	[MetaframeMigration]\SecondaryClient	
	[EventCommands]	
	[EventCommands]\UserLogoffCmd	
	[EventCommands]\UserLogonCmd	
	[EventCommands]\ClientShutdownCmd	
	[EventCommands]\ClientStartupCmd	
	[EventCommands]\EventTimeout	
	[AppListRefresh]	
	[AppListRefresh]\nableRefresh	
	[AppListRefresh]\TimePeriod	
	[AppListRefresh]\StartTime	
	[AppListRefresh]\EndTime	
7.0.2	[ServerSet0]	[ssoauth]
	[ServerSet0]\Name	[ssoauth]\AuthMethods
	[ServerSet0]\FailoverInterval	[ssoauth]\CacheIniFile
	[ServerSet0]\PolicyServers	[ssoauth]\AuthIniDir
	[ServerSet0]\AuthMethods	[auth.SSO]
	[ServerSet0]\AuthSSO	[auth.SSO]\authhost
	[ServerSet0]\AuthCERT	[auth.NT]\authhost
	[ServerSet0]\AuthLDAP	[auth.NOVELL]\authhost
	[ServerSet0]\AuthRSA	[auth.ENTS]\authhost
	[ServerSet0]\AuthNT	[auth.SWEC]
	[ServerSet0]\AuthNOVELL	[auth.SWEC]\authhost
	[ServerSet0]\AuthENTS	[auth.RSA]
	[ServerSet0]\AuthSWEC	[auth.RSA]\authhost
	[GlobalIni]	[auth.CERT]\authhost

Release	Added	Removed
	[GlobalIni]\UseGlobalIniFile	[auth.CERT]\etcercfg
	[GlobalIni]\GlobalIniFile	[auth.LDAP]
	[GlobalIni]\GlobalIniCachingTime	[auth.LDAP]\authhost
	[auth.CERT]\certStore	[TrayMenu]\ItemMigrate MetaframeSessions
	[auth.CERT]\defaultPkcs11Slot	
	[auth.CERT]\Pkcs11LibraryPath	
	[auth.CERT]\Pkcs11PromptText	
	[auth.CERT]\disablePasswordField	
	[auth.CERT]\Pkcs11TokenAbsenceBehavior	
	[auth.CERT]\SCWaitingTime	
8.0	[auth.NT]\NearestDomainController	[sso]\BackupServers
	[Tools]\NetWareServer	

Server-Side Architecture Upgrade

This section explains how to upgrade the server-side architecture of eTrust SSO.

SSO Server

The SSO Server was delivered with eTrust SSO 6.5. This server is automatically upgraded when you install the Policy Sever. The Policy Server is one of the eTrust IAM Common Components.

Policy Server

The Policy Server was first delivered with eTrust SSO 7.0 and is updated and delivered with eTrust SSO 8.0. This is now one of the eTrust IAM common components.

eTrust SSO is now part of a suite of products called eTrust Identity and Access Management (eTrust IAM). The eTrust IAM product suite is unified by a set of common components that create a central architecture that each of the products in the suite can integrate with.

Upgrading a Single Policy Server

When you install the IAM Common Components, the installer will upgrade your existing Policy Server and migrate your data automatically from the previous versions of eTrust Access Control and eTrust Directory to the new versions.

Upgrading a Server Farm

When you want to upgrade multiple Policy Servers in a server farm, you must first upgrade the Policy Server on each computer using the IAM Common Components installation. This installation will upgrade your existing the existing Policy Server and migrate your data automatically from the previous versions of eTrust AC and eTrust Directory to the new versions.

Once you have updated Policy Servers on every computer, you must synchronize the eTrust AC data store.

For more specific information about upgrading a server farm, see the "Implementing a Server Farm" chapter in this guide.

Changing Data Stores on the Policy Server

eTrust SSO 8.0 comes with a utility which lets you migrate an eTrust AC data sore to an LDAP data store manually if you chose to move technologies. For more information see the Migrating Users From eTrust AC to eTrust Directory section in this chapter.

IAM Common Components

The common components are:

- **Policy Server**
  This is an updated version of the Policy Server that was part of eTrust SSO 7.0.
- **Provisioning Server**
  This is a new piece of the eTrust IAM architecture that is the primary server for eTrust Admin. This server also connects the Policy Server to the Web Application Server.
- **Web Application Server**
  This is the web server that hosts the new web administration tool. This web administration tool supplements the Policy Manager.
- **Directory Server**
  This is eTrust Directory which is automatically embedded within the Policy Server and the Provisioning Server. You can install eTrust Directory on a dedicated machine.

These components each perform a particular function in the suite. You can install many common components on one computer or spread them across many computers. For scalability, most of the common components can be installed in a server farm configuration. For eTrust SSO, you would be most likely to configure the Policy Server in a server farm configuration.

To update the Policy Server from eTrust SSO 7.0 to eTrust SSO r8 from the eTrust IAM Common Components CD, you will be prompted to install this new architecture.

For more information, see the *Installing the eTrust IAM Common Components* chapter of this guide.

Data Stores

eTrust SSO comes with the following data stores:

- eTrust Access Control
- eTrust Directory

When you upgrade the Policy Server or the SSO Server, all the data currently stored in eTrust Access Control will be automatically migrated to the new eTrust Access Control, likewise all data currently in eTrust Directory will be migrated to the new eTrust Directory.

These two data stores function differently and are suited for different kinds of information. This section explains the best place to store your data.

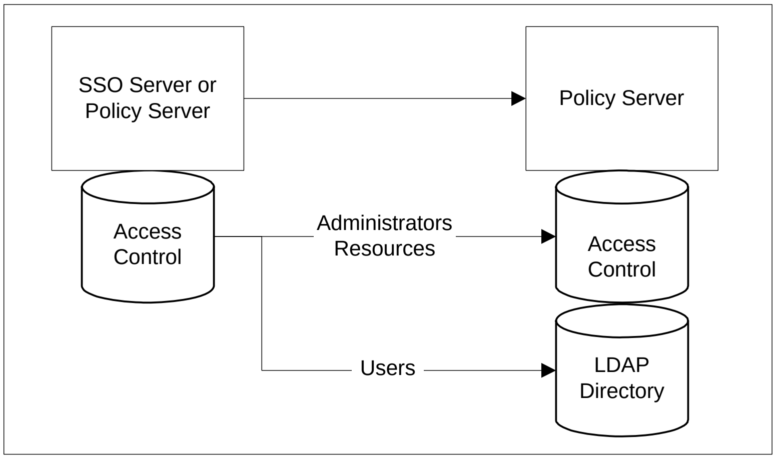
Where to Store Your User Data

If you already store your users in eTrust Directory then you do not need to read this section.

We recommend that you store your user information in eTrust Directory, especially if you have large numbers of users. eTrust SSO 8.0 uses eTrust Directory as the default user data store.

eTrust SSO 8.0 comes with a migration utility which will migrate users to eTrust Directory. For safety reasons this utility will not migrate resource data (which must stay in eTrust AC), administrators, default users or default user groups.

If you want to migrate administrators you must do it manually using selang commands. For more information, see the Migrating Administrators From eTrust Access Control to eTrust Directory section in this chapter.



Migrating Users From eTrust AC to eTrust Directory

This section explains what you need to know about migrating your user data from eTrust AC to eTrust Directory.

Before you Begin

- Ensure that you do not have any users and user groups with the same name.

  In the eTrust AC user data store it is possible for a user and a user group to have the same name. However in eTrust Directory, a group and a user cannot have the same name. The migration utility assumes that all users and groups have unique names. Therefore, before you being this migration, you must rename any duplicate group/user names as well as their authorizations.

- Determine if there are any usernames that include brackets characters:"(" or ")".

  Usernames with brackets are not supported in LDAP and will not be migrated with this utility. You should rename these users to remove the brackets.

- Determine the impact of the fact that users who are members of the default user groups in the eTrust AC data store, will not be members of those groups in eTrust Directory data store after migration.

  By default, when the Policy Server is installed, six user groups are automatically created. When you run the migration utility, those users are migrated to eTrust Directory, but they will no longer belong to those user groups.

  Here is a list of the six default user groups that are created when the Policy Server is installed.

  - _abspath
  - _interactive
  - _network
  - _pr-adms
  - _restricted
  - _surrogate

Migrating the User Data Store

If you choose to migrate your user data from eTrust Access Control (eTrust AC) to eTrust Directory you can use the migration utilities provided with eTrust SSO 8.0. These scripts work for both Windows and UNIX operating systems.

To migrate user information from an eTrust AC to an eTrust Directory (LDAP) data store, follows these steps:

1. To backup and convert the user data, open a command prompt and type the following:

   ```
   MigrateUsers –migrate "<backup directory>"
   ```

   Where <backup directory> is a directory you define to store the backup user data. This command retrieves the information from the eTrust AC data store and converts it to an LDIF format.

   For example:

   ```
   MigrateUsers –migrate "C:\Program Files\AC_Backup"
   ```

   If you do not specify a location for the backup directory the default location for Windows is `C:\ac_backup` and for UNIX is `/ac_backup`.

2. To restore the user data, open a command prompt and type the following:

   ```
   MigrateUsers –restore –admin <eTrust AC administrator name> -
   password <password> "<backup directory>"
   ```

   This command will upload the user data in LDIF format into eTrust Directory. For example:

   ```
   MigrateUsers –restore –admin ps-admin -password secret
   "C:\AC_Backup"
   ```

   Note: You must use the same directory as specified in step 1.

3. Delete the backup directory once the user data has been verified.

What Does Not Get Migrated

The MigrateUsers utility deliberately does not migrate eTrust AC administrator users or any of the default users or groups which are listed here:

- ps-admin
- pswd-pers
- nobody
- RSV
- _undefined
- _seagent
- _abspath
- _interactive
- _network
- _ps-adms
- _restricted
- _surrogate

Chapter

15 Uninstalling

This chapter tells you how to uninstall eTrust SSO. You can uninstall every component using the Product Explorer wizard, except a UNIX installation of the Policy Server.

This chapter covers uninstalling the following eTrust SSO components:

- SSO Client
- SSO Client components
- Policy Manager
- IAM Common Components
- Authentication Agent
- Password Synchronization Agent
- Documentation

You can also uninstall every component using the Windows Add/Remove programs utility located in Control Panel. That method is not documented in this chapter.

About the Product Explorer

You can use the Product Explorer to either install or uninstall any eTrust SSO component. In addition to this, you can use the Product Explorer to modify some of the components.

You can tell if a component is already installed because it appears in bold in the Product Explorer window.

Uninstalling the SSO Client

You can either choose to uninstall the SSO Client or just some SSO components.

SSO Client Uninstall

This procedure tells you how to uninstall the SSO Client.

1. Open the eTrust Single Sign-On **8.0** 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 PE_i386.exe file.

2. Select the **Single Sign-On Client 8.0** option.

   The **Uninstall** button becomes active.

3. Click the **Uninstall** button.

   The Welcome screen appears.

4. Click the **Next** button.

   The **Program Maintenance** dialog appears.

5. Select the **Remove** option and click the **Next** button.

   The **Remove the Program** dialog appears.

7. Click the **Remove** button.

   The eTrust SSO Client will be uninstalled and the **InstallShield Wizard Completed** dialog appears.

8. Click the **Finish** button.

   The eTrust SSO Client is now uninstalled.

   You may be asked to restart the machine.

Modify or Delete SSO Client Components

This procedure tells you how to uninstall the SSO Client components without uninstalling the SSO Client itself. The components that you can remove include:

- GINA Upgrade
- Station Lock
- Gina Pass Through
- Authentication Methods

1. Open the eTrust Single Sign-On 8.0 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 PE_i386.exe file.

2. Select the **Single Sign-On Client 8.0** option.

   The **Uninstall** button becomes active.

3. Click the **Uninstall** button.

   The Welcome screen appears.

4. Click the **Next** button.

   The **Program Maintenance** dialog appears.

5. Select the **Modify** option and click the **Next** button.

   The **Custom Setup** dialog appears.

6. Use the drop-down menus for each SSO Client component to select or remove it from the current client installation, and click the **Next** button.

   The **Ready to Modify the Program** dialog appears.

7. Click the **Install** button.

   The eTrust SSO Client will be modified as you specified and the **InstallShield Wizard Completed** dialog appears.

8. Click the **Finish** button.

   The eTrust SSO Client is now modified.

   You may be asked to restart the machine.

Uninstalling the SSO Server

The SSO Server was delivered with eTrust SSO 6.5. This server is no longer supported. You should remove the SSO Server from your system. You should upgrade to the eTrust IAM Common Components instead.

Uninstalling on Windows

To remove the SSO Server from your Windows computer, follow these steps:

1. From the Windows Start Menu, select Control Panel, Add or Remove programs.
2. Browse for SSO Server and click the Change/Remove button.
3. Follow the prompts to remove this program.

Uninstalling on Windows Using Command Line

To remove the SSO Server from your Windows computer using command line instructions, follow these steps:

1. Open a Command Window.
2. Type the following command:

   ```
   %windir%\IsUninst.exe -f"<SSO Server Installation path>\Uninst.isu"
   -c"<SSO Server Installation path >\SsodUnInst.dll"
   ```

   Where %WinDir% is the value of the WinDir environment variable on the local machine, for example, C:\WINNT\.

Uninstalling on UNIX

To remove the SSO Assistant from your UNIX computer using command line instructions, follow these steps:

1. Open a Command Window
2. Stop the SSO Server process (ssod) by typing:

   ```
   ps -ef | grep ssod
   kill <PID>
   ```

3. Remove the SSO Server installation directory by typing:

   ```
   rm -rf /usr/sso
   ```

Uninstalling the SSO Assistant

The SSO Assistant was delivered with eTrust SSO 6.5. This administration tool is no longer supported. You should remove the SSO Assistant from your system. You should use the IA Manager and the Policy Manager instead.

For further information about uninstalling the SSO Assistant, see the “Uninstalling eTrust SSO” chapter in this guide.

Uninstalling on Windows

To remove the SSO Assistant from your computer, follow these steps:

1. From the Windows Start Menu, select Control Panel, Add or Remove programs.
2. Browse for SSO Assistant and click the Change/Remove button.
3. Follow the prompts to remove this program.

Uninstalling on Windows Using Command Line

To remove the SSO Assistant from your Windows computer using command line instructions, follow these steps:

1. Open a Command Window.
2. Type the following command:

   ```
   %windir%\IsUninst.exe -f"<SSO Assistant Installation
   path>\Uninst.isu"
   ```

   Where %WinDir% is the value of the WinDir environment variable on the local machine, for example, C:\WINNT\.

Uninstalling the Policy Manager

This procedure tells you how to uninstall the Policy Manager on Windows.

1. Open the eTrust Single Sign-On **8.0** 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 PE_i386.exe file.

2. Select the **Policy Manager for Windows** option.

   The **Uninstall** button becomes active.

3. Click the **Uninstall** button.

   The Welcome screen appears.

4. Click the **Next** button.

   The **Program Maintenance** dialog appears.

5. Select the **Remove** option and click the **Next** button.

   The **Remove the Program** dialog appears.

7. Click the **Remove** button.

   The Policy Manager will be uninstalled and the **InstallShield Wizard Completed** dialog appears.

8. Click the **Finish** button.

   The **Policy Manager** is now uninstalled.

Uninstalling eTrust IAM Common Components

eTrust IAM Common Components can be installed across multiple computers. Therefore, removing eTrust IAM potentially involves removing software from multiple computers stored in multiple locations.

Note: Some of these components, such as Apache Tomcat, the Java™ 2 Software Development Kit (JDK) and the Java™ 2 Runtime Environment (JRE), can be used by other software on your computer, so care must be taken when uninstalling these components.

The process for removing eTrust IAM Common Components from a single computer is as follows:

1. Uninstall the eTrust IAM products from the computer
2. Uninstall the eTrust IAM Common Components

   For more information, see Removing IAM from each Computer.

The following sections explain how to uninstall the eTrust IAM Common Components:

- IAM Common Components (excluding third party components)
- CA Tomcat 4.1.29
- JDK
- JRE

You can uninstall every component of the IAM Common Components using the Add/Remove Programs window from the Windows Control Panel.

Removing IAM from each Computer

When more than one computer has eTrust IAM software requiring removal, it is important to perform this task on the machines not acting as a directory server first. The directory server machines hold system configuration information that must be updated correctly to ensure all components are removed from the system. You cannot uninstall IAM from a computer that is the last remaining Directory Server until eTrust IAM Common Components have been removed from all other computers. The last computer involved in the uninstallation must play the role of directory server.

To uninstall the IAM Common Components from the current computer, follow these steps:

1. From the Start menu, choose Settings, Control Panel, Add/Remove Programs.

   The Add/Remove Programs window appears.

2. Select CA eTrust Identity and Access Management from the list of programs, and then click Change/Remove.

   The eTrust IAM Uninstaller appears.

3. Click Next.

   The IAM Installation Enter Password page appears.

4. Enter the IAM Installation computer name and password, and then click Next. The IAM Installation computer name can be any of the computers running eTrust Directory.

   The Summary page appears.

   Note: You must not choose the local computer's machine name until the eTrust IAM components are removed from all other computers.

5. Click Next to uninstall IAM from this computer.

   The uninstallation now takes place. A page appears to inform you that the uninstaller has finished. Click Next to end the process.

You have now successfully removed IAM Common Components from this computer. If you wish to remove IAM Common Components from other computers, you will need to perform the same steps on those computers.

Removing Tomcat

Uninstalling the Common Components does not uninstall Tomcat.

Important! *Do not uninstall Tomcat from a computer running eTrust IAM Common Components.*

To uninstall Tomcat, follow these steps:

1. From the Start menu, choose Settings, Control Panel, Add/Remove Programs.

   The Add/Remove Programs window appears.

2. Select CA Tomcat 4.1.29, and then click Remove. The Tomcat uninstaller launches.
3. Follow the prompts to uninstall Tomcat.

   The uninstaller removes Tomcat.

If you have successfully removed the software, the CA Tomcat 4.1.29 eTrustIAMWebServer service (or the non-default name you chose previously no longer appears in the list of services. To verify this, select Start, Settings, Control Panel, System, Advanced, Environment Variables.

Removing JDK

The JDK program is not removed when you uninstall the Common Components or CA Tomcat 4.1.29.

Important! *Do not uninstall JDK from a computer running the CA Tomcat 4.1.29 installed by eTrust IAM Common Components.*

To uninstall the JDK after uninstalling the Common Components, follow these steps:

1. From the Start menu, choose Settings, Control Panel, Add/Remove Programs.

   The Add/Remove Programs window appears.

2. Select Java 2 SDK, SE v.1.4.2_04, and then click Remove. The JDK uninstaller launches.
3. Follow the prompts to uninstall the JDK.

Removing JRE

JRE is not uninstalled when you uninstall IAM.

Important! *Do not uninstall JRE from a computer running eTrust IAM Common Components. Remove the Common Components first.*

To uninstall JRE, follow these steps:

1. From the Start menu, choose, Settings, Control Panel, Add/Remove Programs.

   The Add/Remove Programs window appears.

2. Select Java 2 Runtime Environment, SE v.1.4.2_04, and then click Remove. The JRE uninstaller launches.

3. Follow the prompts to uninstall the JRE.

Uninstalling an Authentication Agent

This procedure tells you how to uninstall an Authentication Agent.

1. Open the eTrust Single Sign-On 8.0 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 PE_i386.exe file.

2. Select the Authentication Agent you wish to uninstall.

   The Uninstall button becomes active.

3. Click the Uninstall button.

   The Welcome screen appears.

4. Click the Next button.

   The Program Maintenance dialog appears.

5. Select the Remove option and click the Next button.

   The Remove the Program dialog appears.

7. Click the Remove button.

   The Authentication Agent will be uninstalled and the InstallShield Wizard Completed dialog appears.

8. Click the Finish button.

   The Authentication Agent is now uninstalled.

Uninstalling the Password Synchronization Agent

This procedure tells you how to uninstall the Single Sign-On Password Synchronization Agent.

1. Open the eTrust Single Sign-On **8.0** 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 PE_i386.exe file.

2. Select the **Single Sign-On Password Synchronization Agent** option.

   The **Uninstall** button becomes active.

3. Click the **Uninstall** button.

   The **Windows Installer** confirmation dialog appears.

4. Select **Yes** to confirm that you want to uninstall.

   A notice that you must restart your computer appears.

5. Select **Yes** to restart the computer now, or **No** to restart the computer later.

   After rebooting, the Password Synchronization Agent is uninstalled.

Uninstalling the Documentation

This procedure tells you how to uninstall the eTrust SSO documentation.

1. Open the eTrust Single Sign-On **8.0** 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 PE_i386.exe file.

2. Select any of the items in the Documentation Folder.

   The **Uninstall** button becomes active.

3. Click the **Uninstall** button.

   The **Windows Installer** confirmation dialog appears.

4. Select **Yes** to confirm that you want to uninstall the documentation.

   The eTrust SSO documentation is now uninstalled.

Index