eTrust® Access Control

Implementation Guide

r8 SP1

This documentation and any related computer software help programs (hereinafter referred to as the “Documentation”) is for the end user’s informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and 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 the Documentation for their own internal use, and may make one copy of the related software as reasonably required for back-up and disaster recovery purposes, 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 provisions of the license for the product are permitted to have access to such copies.

The right to print copies of the Documentation and to make a copy of the related software is limited to the period during which the applicable 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 certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

EXCEPT AS OTHERWISE STATED IN THE APPLICABLE LICENSE AGREEMENT, 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 the Documentation is governed by the end user’s applicable license agreement.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

CA Product References

This document references the following CA products:

- eTrust® Access Control (eTrust AC)
- eTrust® Single Sign-On (eTrust SSO)
- eTrust® Web Access Control (eTrust Web AC)
- eTrust® CA-Top Secret®
- eTrust® CA-ACF2®
- eTrust® Audit
- Unicenter® TNG
- Unicenter® Network and Systems Management (Unicenter NSM)
- Unicenter® Software Delivery

Contact Technical Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at http://ca.com/support.

Contents

Chapter 3: Installing the IAM Common Components 41

Chapter 4: Installing and Customizing eTrust AC for UNIX 91

Chapter 1: Planning Your eTrust AC Implementation

This section contains the following topics:

Planning for a Security System

The primary goal of any security system is to protect an organization's information assets. To effectively implement security, you must be aware of the threats that exist at your site. You must then determine how to implement eTrust AC so that it best protects your site from these threats.

You have two basic ways to protect against unauthorized use of computer resources:

- Block unauthorized users from accessing the system.
- Block users who are authorized to access the system from accessing information to which they should not have access.

eTrust AC provides tools to protect your system in both ways. eTrust AC for UNIX also provides auditing tools that let you trace users' activities to track attempted misuse of the computer system.

Once you have determined the goals of the security project based on the threats to your site, you can write a security policy statement and put together an implementation team. The implementation team should set priorities that can help determine what data, applications, and users must be secured.

Getting Management Commitment

A management decision to install eTrust AC is not enough to guarantee adequate security at your site. For the security project to succeed, management must be actively involved. Management must decide on security policy, procedures, and resources to be allocated to the security function, and accountability of users of the computer system. Without such management support, security procedures fall into misuse and become more of an administrative chore than a viable protection scheme. In fact, such a situation could breed a false sense of security that could lead to serious security exposures.

The security administrator should work with management to prepare a clear, inclusive security policy statement. This statement should include the following:

- Corporate policy regarding full-time employees, part-time employees, contract employees, and consultants
- Corporate policy concerning outside users of the system
- Behavior expected from all users of the system
- Physical protection considerations
- Security requirements of user departments
- Auditing requirements

The resulting security policy helps to ensure an eTrust AC implementation plan that is both realistic and consistent with the installation's security policy.

Preparing an Implementation Plan

While defining the implementation plan, check repeatedly that the plan's goals come from the security policy. The new security controls should be phased-in gradually to provide users a period of adjustment.

Define a pilot group of users as a prototype for implementing eTrust AC. During the test phase, eTrust AC protects business data, jobs, and users in the pilot group. Test all eTrust AC features on the pilot group before protecting entities outside of the group. Testing with the pilot group can help you learn how to protect the rest of the organization.

In addition to deciding what to protect, the implementation team needs to consider how to phase-in the new security controls with minimum disruption of current work patterns. As you plan implementation, you should consider a period of only auditing access, and not restricting access, for various resources and classes. The resulting audit records show which users tend to require access to the resources.

Deciding How to Protect

Before you install eTrust AC, you should decide what features of the software you want to use. You can use:

- eTrust AC simply to implement native Windows security. In this case, you can use Policy Manager to implement the security features that are already familiar to you.
- A Policy Model database (PMDB), which enables you to propagate a security database with users, groups, and access rules defined in it to a set of subscribers. The PMDB regularly propagates all the updates it receives to its subscribers. This mechanism greatly eases the administrative burden on system administrators.
- eTrust AC to significantly strengthen native Windows security by guarding against more sophisticated attacks. eTrust AC lets you:
  - Limit the rights of privileged accounts such as the Windows Administrator and other members of the Administrators group
  - Assign special privileges to ordinary users, such as the ability to change user passwords for special users
  - Support multiple file systems including NTFS, FAT, CDFS, and HPFS
  - Centralize security policies and auditing across Windows and UNIX systems

Deciding on the Policy Objects to Protect

The following sections describe some of the important objects that can be used by your security policy to authorize access to your enterprise applications and data.

Users

In eTrust AC, there are different types of users. Each type of user has a certain level of authority and certain limitations. Part of developing a security policy for your organization is deciding which special privileges to grant to whom.

The user record contains information about the user associated with it, such as the user's full name, number of times the user is permitted to log on, and the type of auditing to be done on the user.

Information in a user record is stored in properties. A property is equivalent to a database field. For example, the user's first and last names are stored in the FULLNAME property of the user record.

Types of Users

The following types of users can be found in eTrust AC:

Regular users

Your organization's in-house end users-the people who carry out the business of your organization. You can limit regular users' access to the system with both native Windows and eTrust AC.

Users with special privileges (sub administrators)

Regular users who have been given the ability to perform one or more specific administrative tasks. When regular users are given the ability to carry out specific administrative functions, the workload of the Administrator is lessened. In eTrust AC, this is called task delegation.

For instance, a regular user responsible for printing can be given the ability to bring the spooler service up and down.

Administrators

Users who have the highest authority within Windows and eTrust AC. Administrators can add, delete, and update users and can perform almost all administrative tasks. With eTrust AC, you are able to limit the abilities of the Windows Administrator. The tasks of administration can be given to other users, whose accounts are not automatically known.

Group administrators

Users who can perform most administrative functions, such as adding, deleting, and updating users, within one particular group. This type of user, with its particular, limited authority, is not found in native Windows.

Password managers

Users who have the authority to modify the password settings of other users. A password manager cannot change other settings of users. This type of user is not found in native Windows.

Group password managers

Users who have the authority to modify the password settings of other users in one particular group. A group password manager cannot change other settings of users within the group. This type of user is not found in native Windows.

Auditors

Users who have the authority to read audit logs. They also determine the kind of auditing done on each login and each attempt to access a resource. This type of user is not found in native Windows.

Group auditors

Users who can read audit logs relevant to their group. They also have the authority to determine the kind of auditing done within a particular group. This type of user is not found in native Windows.

Operators

Users who can display (read) all the information in the database. This type of user is not found in native Windows.

Group operators

Users who can display all the information in the database for the group in which they are defined. This type of user is not found in native Windows.

Server

A special type of user that is really a process, which is can ask for authorization for other users.

Assigning Types

Within eTrust AC, you create a special user by assigning a user one or more authorization attributes (see page 18). The names of these attributes are ADMIN, AUDITOR, PWMANAGER, OPERATOR, and SERVER at the system level, and GROUP-ADMIN, GROUP-AUDITOR, GROUP-PWMANAGER, and GROUP-OPERATOR at the group level.

Security Policies and Users

When developing a security policy for your organization, it is necessary to decide:

- What users to define
- What special privileges, if any, to give to the defined users
- Whom to define as system administrators, group administrators, password managers, and group password managers

Groups

A group is a set of users who usually share the same access authorizations. Administrators can add users to groups, remove users from groups, and assign or deny access to system resources by group. This type of group exists in both native Windows and eTrust AC.

The group record contains information about the group. The most important information stored in the group record is the list of users who are members of the group.

Important! Authorization rules for a group record apply recursively for each user in the group's hierarchy.

Information in a group record is stored in *properties*. A property is equivalent to a database field. For example, the property SUPGROUP specifies the parent group of the group represented by the group record.

In eTrust AC, a group administrator can manage group functions for the specific group in which the group administrator is defined. A group password manager can manage the password functions of the members of the group.

Security Policies and Groups

When developing a security policy for your organization, it is necessary to decide:

- What groups to create
- Which users to join to each group
- Whether to define group administrators and group password managers, and if so, which users to give these administrative roles

Predefined Groups of Users

eTrust AC includes predefined groups to which a user can be joined. One such group is the _restricted group:

For users in the _restricted group, files that are not listed in the database are governed by the default access (defaccess) value in the _default record of the FILE class.

You add users to the _restricted group the same way you add users to any other group. For example, using selang to join pjones to the _restricted group, enter the following after the prompt:

```
eTrustAC> join pjones group(_restricted)
```

For files that are not listed in the database, this command gives pjones only the access (if any) permitted by in the _default record of the FILE class.

eTrust AC reads the list of _restricted users only when you start eTrust AC, so if a user has joined or left the _restricted group, the change is effected only when you restart seosd.

Note: Be very careful defining _restricted users. If a user is joined to the _restricted group, the FILE class's _default object has NONE as default access type, and the database contains few FILE access rules, then a _restricted user may not be able to do anything.

Remember, a user needs EXEC permission to run executables, READ and EXEC permission to load dynamic libraries, and often CREATE and WRITE authorization for various log, audit, or cfg files that the executable needs. If you plan to add users to the _restricted group with NONE as the default access type for the FILE class's _default object, consider using WARNING mode. Then the audit events show you what files your _restricted users need for their work. After awhile, you can grant the appropriate authorizations and turn WARNING mode off.

Predefined Groups for Resource Access

Other types of predefined groups in eTrust AC define the type of access that is allowed or prohibited to a particular resource. These groups include the following:

- _network

  The _network group defines access from the network to a particular resource. All users are treated as if they are members of the group; no user has to be explicitly added to the group.

  For example, you can specify that a particular resource can only be read from the network. Using selang, you would define the new resource as follows:

  ```
  newres FILE \temp\readonly
  ```

  Then specify the access allowed through the network:

  ```
  authorize FILE \temp\readonly gid(_network) access(read)
  ```

  You can also do this using Policy Manager.

  Now when accessing \temp\readonly from the network, users can read the file only if they have explicit permission to access the file in other ways.

- _interactive

  The _interactive group defines the access permitted to a particular resource from the computer on which the resource resides. For example, You can authorize READ access to a file from the computer on which it is defined, although no access is permitted to the resource from the network.

The following points are important:

- There is no connection in eTrust AC between the _network and _interactive groups. This means that there can be a rule in the _network group that defines access from the network to a specific resource. Another rule in the _interactive group can define access to the same resource.
- You do not have to add users to the _network and _interactive groups.
- These groups can protect all the Windows resources defined in the database.

Resources

An essential part of any security policy is deciding which system resources must be protected and defining the type of protection these resources are to receive. In Windows domains, system files and the Windows registry should be protected.

Domains

eTrust AC lets you protect your Windows domains by specifying which users can add or delete members in a domain and which users can create or delete trust relationships between domains.

Specify these rules in the database on the primary domain controller for your Windows domain. To protect the domain, you typically define it using the newres or chres commands, as a DOMAIN resource with a default access of NONE. To allow specific users to add or delete members from the domain, use the *authorize* command to give those users EXECUTE access. To allow specific users to create and delete trust relationships between one domain and another, use the *authorize* command to give those users CHMOD access in the DOMAIN resource for each domain.

You can also manage domains using Policy Manager. See Managing Windows Domains in the chapter “Using the Administrator Interface.”

Files

Any computer system has at least two kinds of files: system files and application files. System files are necessary for the operating system to function properly. Application files are created and used by applications and users at the site.

You should determine what kind of protection each kind of file should have and then implement this protection. One of the major benefits of eTrust AC is that it can extend protection to non-NTFS file systems.

Registry

The Windows registry is a centralized database that contains most of the operating system parameters, including the parameters that control device drivers, configuration details, and hardware, environment, and security settings.

Both native Windows and eTrust AC protect the Windows registry to ensure that an unauthorized user does not change system parameters.

Authorization Attributes

An authorization attribute is set in the user record in the database and permits the user to do things that an ordinary user cannot do. The two kinds of authorization attributes are **global** and **group**. Each global authorization attribute permits the user to perform certain types of functions on any record in the database. A group authorization attribute permits the user to perform certain types of functions within one specified group. The functions and the limits of each global and group authorization attribute are described in the following sections.

Global Authorization Attributes

Users who have a global authorization attribute set in their own user records can perform special functions on any relevant record in the database. The global authorization attributes are:

- ADMIN
- AUDITOR
- OPERATOR
- PWMANAGER
- SERVER

ADMIN

The ADMIN attribute lets a user execute almost all commands in eTrust AC. Users who are defined in the database with the ADMIN attribute can define and update users, groups, and resources in the database. This is the most powerful attribute in eTrust AC, but it does have limitations:

- If only one user in the database has the ADMIN attribute, that user cannot be deleted, and the ADMIN attribute cannot be removed from the record.
- Users with the ADMIN attribute but without the AUDITOR attribute cannot change the type of auditing that is done on a user, group, or resource. If you have the ADMIN attribute and need to change the auditing characteristics of a user, group, or resource, assign yourself the AUDITOR attribute.

SUB ADMINISTRATOR

Security administrators (users with the ADMIN attribute) can grant specific administrative privileges to regular users. These regular users are then called sub administrators. Sub administrators have privileges to manage only specified eTrust AC classes or objects. For example, a sub administrator can be authorized to manage only user and group objects. You can set a higher level of sub administration by authorizing the sub admin user the administrative privileges for specific objects in a class.

Sub administrators of users and group objects can use the Policy Manager to perform administrative tasks related to these objects.

AUDITOR

Users with the AUDITOR attribute can monitor system usage. Explicit privileges of a user with the AUDITOR attribute include the following:

- Users can display information in the database. In Policy Manager, users can select Show from the Edit menu; or users can execute the selang commands *showusr*, *showgrp*, *showres*, and *showfile*.
- Users can set the audit mode for existing records. In Policy Manager, users can update the audit modes of users and resources defined in the database. At the command prompt, they can execute the selang commands *chusr*, *chgrp*, *chres*, and *chfile*.

OPERATOR

Users with the OPERATOR attribute have READ access to all files. With this access, they can list everything in the database, and they can run backup jobs. To list database records, operators can use the selang commands showusr, showgrp, showres, and showfile. Alternatively, in Policy Manager, users can select Show from the Edit menu.

The OPERATOR attribute also gives access to the secons utility. For more information about secons, see the secons section in the “Utilities” chapter of the *Reference Guide*.

PWMANAGER

The PWMANAGER attribute gives an ordinary user the authority to use the following selang commands:

chusr

Changes the passwords of other users.

find userName

Lists the users with the specified userName.

The PWMANAGER attribute does not include authority to change the password interval of another user or to change the general password rules. For more information about password rules and intervals, see the setoptions section in the chapter “The selang Command Language” in the *Reference Guide.*

SERVER

eTrust AC, like many other security models, does not permit a regular user to ask: “Can user A access resource X?” The only question a regular user can ask is: “Can I access resource X?” However, a process that supplies services to many users, such as a database server service or an in-house application, should be permitted to ask for authorization on behalf of other users.

The SERVER attribute allows a process to ask for authorization for users.

Group Authorization Attributes

Users who have a *group authorization attribute* in their own user records can perform special functions within a specified group. The group authorization attributes are:

- GROUP-ADMIN
- GROUP-AUDITOR
- GROUP-OPERATOR
- GROUP-PWMANAGER

Group Scope

Users with a group authorization attribute can manage a certain set of records that includes the records owned by the group in which the user has a group authorization attribute. If that group is the parent of other groups, the set also includes the records owned by those groups. The whole set of records is called the group scope.

GROUP-ADMIN

Users with the GROUP-ADMIN attribute have the following access authority for the records within their group scope:

Description	Commands
Show the properties of the record	showusr, showgrp, showres, showfile
Change the properties of the record	chusr, chgrp, chres, chfile
Remove the record from the database	rmusr, rmgrp, rmfile, rmres
Join a user to or remove a user from a group	join, join-

The GROUP-ADMIN attribute also has certain limits:

- A GROUP-ADMIN user cannot delete the only ADMIN user record in the database.
- A GROUP-ADMIN user cannot remove the ADMIN attribute from the record of the last ADMIN user in the database.
- GROUP-ADMIN users without the AUDITOR attribute cannot update the audit mode. Only a user with the AUDITOR attribute can update the audit mode.
- GROUP-ADMIN users cannot set the global authorization attributes-ADMIN, AUDITOR, OPERATOR, PWMANAGER, and SERVER-for any user. Only users with the ADMIN attribute can do this.

GROUP-AUDITOR

A user with the GROUP-AUDITOR attribute can list the properties of any record within the group scope. The group auditor can also set the audit mode for any record within the group scope.

GROUP-OPERATOR

A user with the GROUP-OPERATOR attribute can list the properties of any record within the group scope.

GROUP-PWMANAGER

A user with the GROUP-PWMANAGER attribute can change the password of any user whose record is within the group scope.

B1 Security Features

eTrust AC includes the following B1 “Orange Book” features:

- Security levels
- Security categories
- Security labels

You can manage B1 security features using *selang* or Policy Manager. This section describes B1 security features and provides instructions about using selang. For instructions on using Policy Manager to assign B1 security features, see the online help.

Security Levels

When security level checking is enabled, eTrust AC performs security level checking in addition to its other authorization checking. A security level is a positive integer between 1 and 255 that can be assigned to users and resources. When a user requests access to a resource that has a security level assigned to it, eTrust AC compares the security level of the resource with the security level of the user. If the user's security level is equal to or greater than the security level of the resource, eTrust AC continues with other authorization checking; otherwise, the user is denied access to the resource.

If the SECLABEL class is active, eTrust AC uses the security level associated with the security labels of the resource and user; the security level that is explicitly set in the resource and user records is ignored.

To protect a resource by security level checking, assign a security level to the resource's record using Policy Manager or the selang commands newres or chres.

To allow a user access to resources protected by security level checking, assign a security level to the user's record using Policy Manager or the selang commands newusr or chusr.

Enabling and Disabling Security Level Checking

The following setoptions command enables security level checking:

```
setoptions class+ (SECLEVEL)
```

The following setoptions command disables security level checking:

```
setoptions class- (SECLEVEL)
```

Security Categories

When security category checking is enabled, eTrust AC performs security category checking in addition to its other authorization checking. When a user requests access to a resource that has one or more security categories assigned to it, eTrust AC compares the list of security categories in the resource record with the category list in the user record. If every category assigned to the resource appears in the user's category list, eTrust AC continues with other authorization checking; otherwise, the user is denied access to the resource.

If the SECLABEL class is active, eTrust AC uses the list of security categories associated with the security labels of the resource and user; the lists of categories in the user and resource records are ignored.

To protect a resource by security category checking, assign one or more security categories to the resource's record using Policy Manager or the selang commands newres or chres.

To allow a user access to resources protected by security category checking, assign one or more security categories to the user's record. You can assign security categories to a user by using Policy Manager or the selang commands newusr or chusr.

Enabling and Disabling Security Category Checking

The following setoptions command enables security category checking:

```
setoptions class+ (CATEGORY)
```

The following setoptions command disables security category checking:

```
setoptions class- (CATEGORY)
```

Defining Security Categories

A security category is defined by defining a resource in the CATEGORY class. The following selang command newres defines a security category:

```
newres CATEGORY name
```

where *name* is the name of the security category.

For example, to define the security category Sales, enter the following command:

```
newres CATEGORY Sales
```

To define the security categories Sales and Accounts, enter the following command:

```
newres CATEGORY (Sales,Accounts)
```

Listing Security Categories

To display a list of all the security categories defined in the database, use the show command as follows:

```
show class(CATEGORY)
```

Deleting Security Categories

You can delete a security category by removing its record from the CATEGORY class. The following rmres command removes a security category:

```
rmres CATEGORY name
```

where *name* is the name of the security category.

For example, to remove the security category Sales, enter the following command:

```
rmres CATEGORY Sales
```

Security Labels

A security label represents an association between a particular security level and zero or more security categories.

When security label checking is enabled, eTrust AC performs security label checking in addition to its other authorization checking. When a user requests access to a resource that has a security label assigned to it, eTrust AC compares the list of security categories specified in the resource record's security label with the list of security categories specified in the user record's security label. If every category assigned to the resource's security label appears in the user's security label, eTrust AC continues with the security level check; otherwise, the user is denied access to the resource.

eTrust AC then compares the security level specified in the resource record's security label with the security level specified in the user record's security label. If the security level assigned in the user's security label is equal to or greater than the security level assigned in the resource's security label, eTrust AC continues with other authorization checking; otherwise, the user is denied access to the resource.

When security label checking is enabled, the security categories and security level specified in the user and resource records are ignored; only the security level and categories specified in the security label definitions are used.

To protect a resource by security label checking, you assign a security label to the resource's record using Policy Manager or the selang commands newres or chres.

To allow a user access to resources protected by security label checking, assign a security label to the user's record using Policy Manager or the selang commands newusr or chusr.

Enabling and Disabling Security Label Checking

The following setoptions command enables security label checking:

```
setoptions class+ (SECLABEL)
```

The following setoptions command disables security label checking:

```
setoptions class- (SECLABEL)
```

Defining Security Labels

You can define a security label by defining a resource in the SECLABEL class. The following newres command defines a security label:

```
newres SECLABEL name \
category(securityCategories) \
level(securityLevel)
```

where:

name

specifies the name of the security label.

securityCategories

specifies the list of security categories. If more than one security category is specified, separate the security category names with a space or a comma.

securityLevel

specifies the security level. Specify an integer between 1 and 255.

For example, to define the security label Managers to contain the security categories Sales and Accounts and a security level of 95, enter the following command:

```
newres SECLABEL Manager category(Sales,Accounts) level(95)
```

Listing Security Labels

To display a list of all the security labels that are defined in the database, use the show command as follows:

```
show class(SECLABEL)
```

Deleting Security Labels

You can delete a security label by removing its record from the SECLABEL class. The following rmres command removes a security label:

```
rmres SECLABEL name
```

where *name* is the name of the security label.

For example, to remove the security category Managers, enter the following command:

```
rmres SECLABEL Managers
```

Using a Warning Period

In addition to deciding what to protect, the implementation team must consider how to phase in the new security controls with minimum disruption to current work patterns. As you plan implementation, you should consider a period of auditing access only-not restricting access-for resources and classes. The resulting audit records show which users tend to require access to the resources.

eTrust AC also provides the option of specifying restrictions but substituting a warning message for the enforcement of the restrictions. You can control which resources are protected in this manner by using the WARNING parameter when you define the rules for your resources.

When warning mode is enabled for a resource and the user is not authorized to access the resource in the requested manner, eTrust AC issues a warning message, logs the access, and gives the user access to the resource.

Note: If you use warning mode during eTrust AC implementation, make sure you have enough disk space for the audit logs and set the size limit of the audit log higher.

Educating and Training Staff

Part of the security administrator's job is to tell the system users what they need to know to work without disruption when eTrust AC is installed.

The amount of detailed information each user needs to know about eTrust AC depends on the functions you authorize the person to use. Examples of information required by various types of system users include:

- All users defined in the database
  - Users must know to identify themselves to the system by a user name and a password and how to change a password. They should also be aware of the significance of their password to system security.
  - If you want to implement checking of the password policy, users may need to be familiar with the Password Manager.
  - Users should be aware of the **secons -d-** and **secons** -**d+** commands that disable and enable concurrent logins.
  - Users may be interested in the sesudo command, which enables user substitution based on predefined access rules with or without password checking.
- Technical support personnel

  Users who install eTrust AC need to be familiar with migration considerations and with the steps required to install or reinstall eTrust AC (see page 95). Users who maintain the database must be familiar with the database utilities.

  Note: For more information about database utilities, see dbmgr in the *Utilities Guide for UNIX* or the *Reference Guide for Windows*.
- Group administrators

  Users who have one of the group authorities, who have a group attribute (such as GROUP-ADMIN), or who own group records need group information (see page 14).

  Note: For more information about groups, see the group selang commands in the *Reference Guide*.
- Auditors

  Users with the AUDITOR attribute should be familiar with the auditing tools-Policy Manager and the seaudit utility.

  Note: For more information about Policy Manager, see the *User Guide for UNIX* or the *Administrator Guide for Windows*. For more information about the seaudit utility, see the *Utilities Guide for UNIX* or the *Reference Guide for Windows*.

- Programmers writing unauthorized applications

  Programmers can use the eTrust AC* function library in their applications to request security-related services, including controlling access to protected resources (by using the SEOSROUTE_RequestAuth function). Your installation can create installation-defined resource classes. If your installation creates records in those classes, an application can issue a SEOSROUTE_RequestAuth command to check whether a user has sufficient authority to complete an action. The level of authority required for a particular user action is determined by the way the application invokes the SEOSROUTE_RequestAuth function.

  Note: For more information about the eTrust AC API, see the *SDK Guide*.

- Programmers writing authorized applications

  Programmers writing authorized applications (programs that run with the SERVER attribute) can use the eTrust AC* function library to request security-related services, including:

  – User identification and verification

  – User logout service

  – User authorization request

Implementation Tips

This section provides some miscellaneous implementation information to consider once you have installed eTrust AC.

Types of Security

You can handle security at your site by using one of the following approaches:

- Whatever is not explicitly allowed is forbidden. This is the ideal approach, but it is impossible to use during implementation. Since no rules exist that allow anything to be done on the system, the system blocks all attempts to define access rules. It is like locking yourself out of your car with the keys still in the ignition.
- Whatever is not specifically forbidden is allowed. This approach may be less secure, but it is the only way to implement a security system.

eTrust AC lets you start with the second approach and, once access rules have been defined, switch to the first approach. Default and universal access (_default) rules let you define approach and switch protection policy at any time.

Accessors

An *accessor* is any entity that can access system resources. Accessors fall into three categories:

- A person who is associated with a specific user name
- A person who is a member of a group that has access authority
- A production process that is associated with a certain user name

The most common type of accessor is a user, a person who can perform a login and for whom access authorities should be assigned and checked. One of the most important features of eTrust AC is accountability. Each action or access attempt is performed on behalf of a user who is held responsible for the request.

eTrust AC lets you define groups of users. Users are usually grouped together by projects, departments, or divisions. By grouping users together, you can significantly reduce the amount of work needed to administer and manage security, by specifying a standard set of user properties for a group or by specifying similar access privileges and restrictions.

You can define new users and groups and modify existing users and groups through Policy Manager, which is described in the online help.

Resource Classes and Access Rules

When installed, eTrust AC immediately begins intercepting system events and checking for users' authority to access resources. Until you tell eTrust AC how to restrict access to your system's resources and which resources to restrict, the result of all authorization checks is to permit access.

The properties of a protected resource are stored in a resource record, and resource records are grouped into classes. The most important information contained in a resource record is its access rules. An *access rule* governs the permission of one or more accessors to work with one or more resources. Several ways to define access rules are:

- An access control list (a specific list of the accessors authorized to access the resource and the exact access they can have), also called an ACL
- A negative access control list (a specific list of the accessors for which access should be denied), also called NACL
- A default access for the resource, which specifies access rules for accessors not specifically listed in an ACL
- A universal access (the _default record for a class), which specifies access for resources that do not yet have specific resource records in that class
- A program ACL, which defines access for a specific accessor through a specific program.
- A conditional ACL, which makes access dependent on some condition. For example, in a TCP record, you can define access to a specific remote host through a specific accessor.
- An Inet ACL, which defines access for inbound network activity through specific ports.

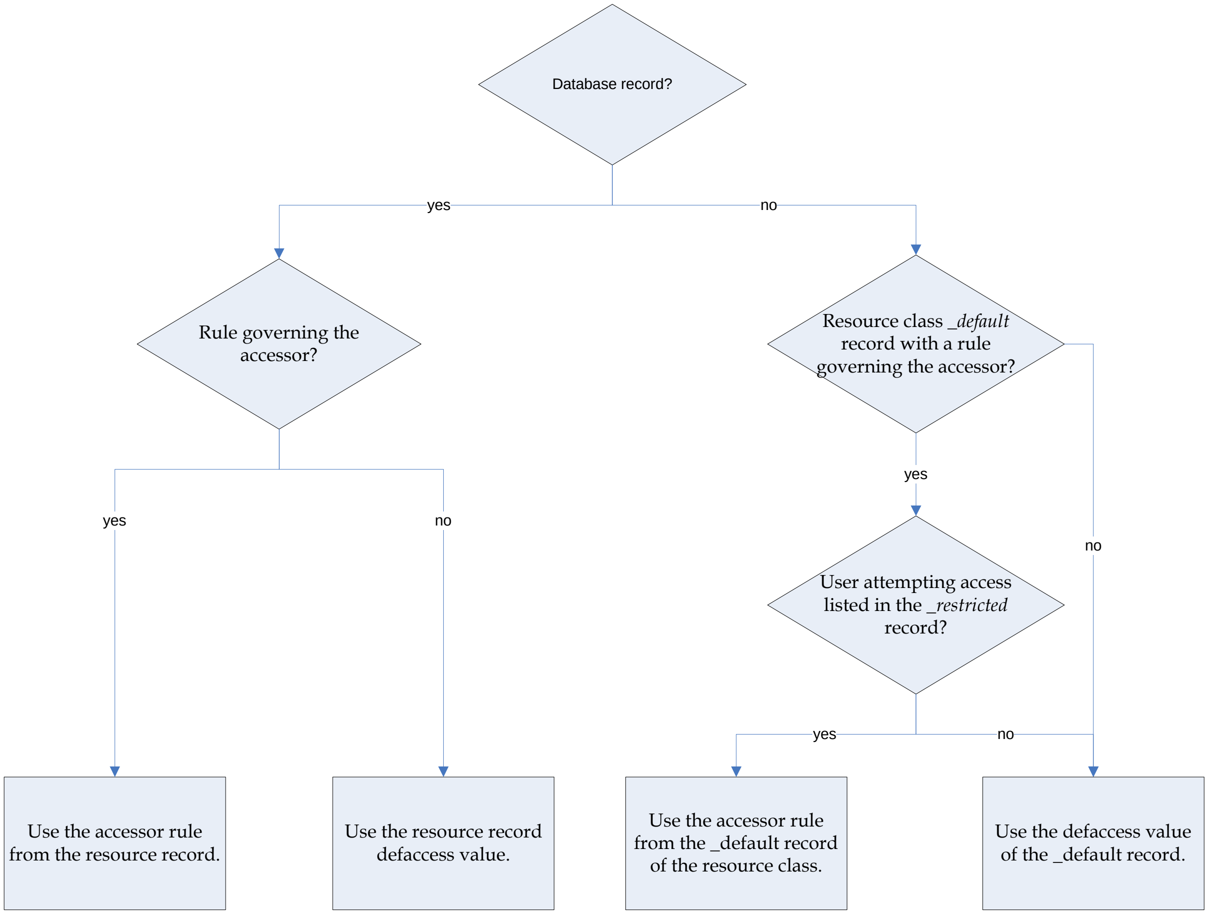
Using defaccess and _default

When access to a resource is requested, the database is searched in the following order to determine how the request should be treated, and eTrust AC uses the first access rule that is found. Notice the distinction between *default access* (defaccess) and _default.

1. If the resource has a record in the database, and the record has a rule governing the accessor, then eTrust AC uses that rule. (The accessor can be a user or a group.)
2. If the resource record exists but does not have a rule governing the accessor, that *record's* default access rule-its *defaccess value*-is applied to the accessor.

3. If the resource record does not exist, but in the resource class the _default record has a rule governing the accessor, then eTrust AC uses that rule.

4. If the resource record does not exist, and in the resource class the _default record does not have a rule governing the accessor, then the _default record's default access rule-its defaccess value-is applied to the accessor. For files, this applies only to _restricted users (see page 15).


Database record?
yes
no
Rule governing the accessor?
Resource class _default record with a rule governing the accessor?
yes
no
yes
no
User attempting access listed in the _restricted record?
yes
no
Use the accessor rule from the resource record.
Use the resource record defaccess value.
Use the accessor rule from the _default record of the resource class.
Use the defaccess value of the _default record.

Note: For more information about resource classes and access rules see the *Reference Guide*.

Improving Performance

eTrust AC sometimes reduces performance of the system it is running on due to multiple access checks for accessed entities (files, registry keys, and the like). To improve the performance of your systems with eTrust AC, a cache tool is used in kernel mode.

A cache “remembers” the previous answer to an authorization request (permit or deny). When a similar authorization is requested, the request is answered with the last response that the cache stored. This saves time because eTrust AC does not have to reevaluate the request; eTrust AC can return the answer immediately. When rules are changed, the cache is automatically and immediately synchronized.

Chapter 2: Component Installation Overview

This section contains the following topics:

Implementation Strategy

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

1. Install the eTrust Identity and Access Management Common Components
2. Install the Policy Manager (administrator workstations)
3. Populate the Data Stores

After each installation and configuration step, we strongly recommend that you verify that the component added is working as expected.

Step 1: Install the eTrust Identity and Access Management Common Components

eTrust Identity and Access Management is a combination of products and services that facilitates management and enforces secure access to information assets.

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

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

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

Provisioning Server

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

The Provisioning Server should be installed and configured via the eTrust Identity and Access Management Common Components installation.

After installation, check that all servers are accessible from the end-user networks.

Web Application Server

The Web Application Server hosts IA Manager infrastructure. IA Manager is a GUI (graphical user interface) that lets administrators manage eTrust AC and other products in the suite if they have them installed, from a central web-based interface using their web browser.

The Web Application Server should be installed and configured via the eTrust Identity and Access Management Common Components installation.

After installation, check that all servers are accessible from the end-user networks.

Policy Server

The Policy Server resides on a central UNIX or Windows server. You can control the Policy Server from the command line, using Policy Manager or using IA Manager.

All Policy Servers should be installed and configured via the eTrust Identity and Access Management Common Components installation.

You can install a server farm within the eTrust AC architecture. This helps with load balancing and failover, as well as scalability.

After installation, check that all servers are accessible from the end-user networks. If possible, use the default name that the installation procedure suggests for the Policy Server.

When the servers are installed, the databases should be populated with the rules that will allow eTrust AC to be administrated from an administration workstation using Policy Manager.

Next, the replication mechanisms of the server farm are implemented and tested. When installing more than one server, use DNS name resolution, if possible, to map pre-selected names to the specific Policy Server hosts. This allows flexibility in locating and upgrading the servers.

Directory Server

The Directory Server is used to store configuration information for the other Common Components.

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

The Directory Server should be installed and configured via the eTrust Identity and Access Management Common Components installation.

After installation, check that all servers are accessible from the end-user networks.

Step 2. Install Policy Manager

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 Policy Manager to communicate with both UNIX and Windows Policy Server computers.

You should install Policy Manager on all computers that your administrators use to control the Policy Server. Once you have installed Policy Manager on an initial machine, you must set access rights for any other machines that will be authorized to access Policy Manager.

Step 3. Populate the Data Stores

You can populate these data stores in two ways. If you are importing a large amount of data to a data store, you might want to use a command line tool, such as a selang script, to import data into the eTrust AC 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 AC database. If you are just entering small amount of information, you might use 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 AC (Data Store)

The eTrust AC is a database that stores all information about:

- Resources
- Applications
- Access control rules
- Administrators

You can use either eTrust AC, eTrust Directory, or another LDAP directory to store information about:

- Users
- User groups
- Logon information

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

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

eTrust Directory (LDAP Data Store)

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

You can use eTrust Directory to store information previously stored on eTrust AC. eTrust Directory can store information about:

- 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 AC data store for all information that does not relate to users, user groups and logon information.

Chapter 3: Installing the IAM Common Components

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

This section contains the following topics:

Before You Begin

Before you install any of the products that make the eTrust Identity and Access Management suite, you must install the Common Components.

The Common Components installation program coordinates the installation of the eTrust Identity and Access Management Common Components across multiple computers. During installation on the first computer, the configuration information is collected and stored in a networked data store. Installations on additional computers use this configuration information 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 only requires you to enter local configuration information.

After installing the Common Components, you need to install the software components specific to the point product you purchased. You can install these components from your eTrust product CD.

Plan Your Installation

A typical installation of the eTrust Identity and Access Management Common Components 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. When planning the software configuration for your unique needs, consider the following:

- The eTrust Identity and Access Management 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 workload on designated servers
- Operating systems installed on the designated servers

These factors influence the optimal eTrust Identity and Access Management architecture and the best location for the computer roles you want to assign.

During the installation you can select a Custom or Express installation. If you choose the Express installation, all required components are installed and configured to the current computer. You cannot install any of the eTrust Identity and Access Management Common Components on additional computers when using the Express installation option.

Note: You cannot install eTrust Identity and Access Management Common Components on multiple computers concurrently. You must successfully complete the installation on each computer before moving to the next computer.

Notes on Possible Architectures

This section lists some points to consider when choosing the architecture for your eTrust Identity and Access Management product.

The Directory Server role is 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.

Do not install the Web Application Server and Workflow Server roles on computers already running as web servers to avoid potential port conflicts. You can install these roles to the same computer.

Upgrading an Existing eTrust Product

eTrust Admin cannot be upgraded by the eTrust Identity and Access Management Common Components installer. You will need to upgrade an existing eTrust Admin computer to version 8.1 before running the eTrust Identity and Access Management Common Components installation program. Existing eTrust Admin r8.1 computers will be integrated into the eTrust Identity and Access Management 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.

You cannot upgrade your Provisioning Server if it does not support an eTrust Admin Option that you have installed on your current Provisioning Server. eTrust Admin is now released with a two-tier set of options. Only Tier 1 options are supported in the initial release of eTrust Admin. For more information, see the eTrust Admin Readme.

Upgrades of existing SSO Server 6.5, or Policy Server 2.0 (SSO 7.0) computers are supported by the installation program. When running the installation program, 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 a special configuration (DXlink for example), you will need to recreate it after the upgrade.

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

Two Methods of Installation

You can install the Common Components using either of the following methods:

- Installation wizard
- Command prompt

Both methods automate the installation of the Common Components using the installation program.

Checklist

Prior to installation, ensure that you have considered the following:

- The role or roles that will be assigned to each computer. At the very least, designate a Directory Server, and run the installation program on that computer first.
- If you choose to make the initial computer a Provisioning Server, it will be assigned as the root Provisioning Server. Therefore, you should start the installation process on the computer that is either *not* a Provisioning Server, or is the root Provisioning Server.
- If you are upgrading server roles, you have the computer names and the administrative passwords for those computers that are currently performing those roles.

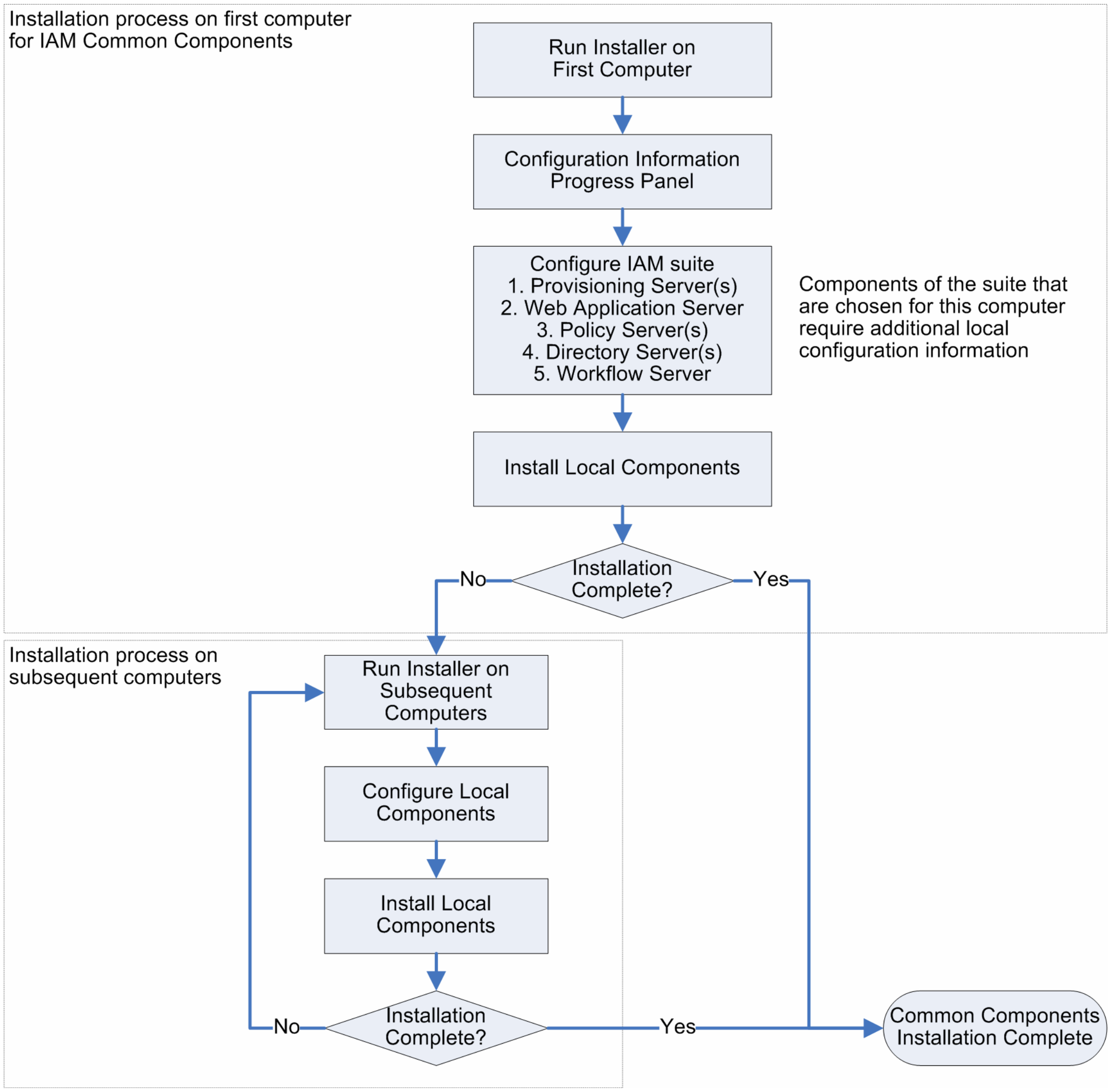
  Note: If you are upgrading, you must backup all user data stores prior to installing the Common Components to avoid losing data.
- SMTP server name.
- The system administrator's email address.
- The list of Provisioning Server options for each Provisioning Server you want to install. See the eTrust Admin options guides for more information about Provisioning Server options.
- If you are installing on a UNIX platform, ensure you have the correct umask settings (umask 022) before executing the setup file from that shell.
- If you are upgrading a Provisioning Server, check that your currently installed eTrust Admin options are available in the installer. You will not be able to upgrade the Provisioning Server if installed options are not available on the CD.

Installation Using the Installation Wizard

You can use an installation wizard to drive the Common Component installation.

The installation wizard installs (as a minimum) a Directory Server on the first computer where the Common Components are installed. This computer stores the configuration information that is later accessed by other computers included in the installation.

The complete installation process is illustrated in the following graphic. Installing on the first computer requires you to provide a large amount of information which is then 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
No
Installation Complete?
Yes
Installation process on subsequent computers
Run Installer on Subsequent Computers
Configure Local Components
Install Local Components
No
Installation Complete?
Yes
Common Components Installation Complete

Install the Common Components on the First Computer

You can install the eTrust Identity and Access Management Common Components on one computer, or on multiple computers. The following procedure describes the installation of the Common Components on the first computer.

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

1. Insert the first eTrust Identity and Access Management Common Components CD into your CD drive.

   The product explorer for the eTrust Identity and Access Management suite 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. Choose the Installation page from the left navigation pane.

   The Installation page appears.

3. Click Install eTrust IAM Common Components.

   The product explorer closes and the installation wizard starts loading and appears after a short delay.

Note: You can also start the installation on a UNIX Computer (see page 69).

Elements in the Installation Wizard

During the installation process you are prompted for information that is used to configure the suite for your needs.

The following sections gives you background information for each page of the installation wizard you may encounter, to help you provide the correct information.

The actual pages displayed and the order encountered depends on your specific installation. The pages here are sorted into an alphabetical order based on the page titles.

Application Server: Port Numbers

This page of the installation wizard lets you configure the port numbers used by your custom Web Application Server. It contains the following options:

SSL HTTP Port

Specifies the secured port number that eTrust Identity and Access Management uses by default to connect with the web applications (for example, IA Manager).

HTTP Port

Specifies the non-secured port on which your web application server listens for connections.

Note: The installation wizard checks that these ports are busy before letting you proceed so you must have your custom web application server already installed.

Choose the setup type that best suits your needs

This page of the installation wizard contains the following options:

Custom

Specifies an installation that lets you control options related to the installation of each of the common components.

Note: You must choose this option if you want to configure multiple computers to perform eTrust Identity and Access Management server roles.

Express

Specifies a simplified installation that uses pre-determined settings for installing the Common Components. On a Windows computer this option installs all Common Components on the same computer.

Note: On a UNIX computer the Express option installs the Directory Server role on this computer and prompts you to nominate a Windows computer for the remaining server roles.

Configuration Information: Default Location

This page of the installation wizard contains the following options:

Enter the top-level location for these components

Defines the top folder where the common components are installed.

Note: If you choose the Custom installation type, this is only a default location and you can modify the installation location for each component.

Browse

Opens a dialog that lets you locate and specify the location for where the common components are installed.

Point Product Choice

This page of the installation wizard contains the following option:

Point Product Choice

Specifies the products from the eTrust Identity and Access Management suite that you intend to install. This tailors the installation of the eTrust Identity and Access Management Common Components to the products that you select so that only the relevant software is installed.

Note: Your selection does not trigger the installation of the selected product itself. After you have completed the installation of the eTrust Identity and Access Management Common Components, run the installation program on your separate point product CD to complete the installation of your product.

Configuration Information: Progress

This page of the installation wizard displays the current status of your installation and contains the following option:

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

Specifies the server role you want to configure next.

Note: The order of server role configuration is important and cannot be changed. You can only use this selection to return to a previously configured role and make changes.

Directory Server: Assign Computer(s)

This page of the installation wizard lets you assign the role of Directory Server. It contains the following options:

Enter machine names, separated by commas, to add them to the list below

Defines a comma-separated list of computers that you can then add to the list of computers that can be assigned a server role.

Apply

Verifies that the current computer can locate the specified computers on the network and adds them to the list of computers that can be assigned a server role.

Indicate which machine(s) will be assigned the role of Directory Server

Specifies which computers will be assigned the role of Directory Server.

Note: Only the selected computers 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.

Directory Server: Install Locations

This page of the installation wizard lets you choose where to install the Directory Server and its database. It contains the following options:

Directory Server Install Location

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

Advantage Ingres Install Location

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

Limit: The Advantage Ingres installation path must not exceed 71 characters. This is due to a Windows path length limitation.

Advantage Ingres Database Location

Defines the installation location for the Advantage Ingres database on this computer.

Limit: The Advantage Ingres installation path must not exceed 71 characters. This is due to a Windows path length limitation.

Directory Server: Insufficient Kernel Parameters

eTrust Directory and the Policy Server require specific kernel parameters to be configured on your computer before the products can be installed.

If the eTrust Identity and Access Management installation program detects that you have incorrect kernel parameters you will be prompted with this warning screen. If this happens, you must continue through the installation to finish configuring your suite. After providing this configuration information, you will be asked to reboot your machine. The installer will make the required change automatically. Once you have rebooted your computer, restart the eTrust Identity and Access Management installation program to complete the software installation.

Directory Server: UNIX Timezone

You will only see this page of the installation wizard when you are installing the Common Components on a UNIX computer. It contains the following option:

Current Time Zone

Specifies the correct region or timezone difference from Greenwich Mean Time.

Documentation Options

This page of the installation wizard asks you whether you want to view the Readme when the installation completes. It has the following options:

Yes

Specifies that the Readme will be displayed when the installation completes.

No

Specifies that you the Readme will not be displayed when the installation completes.

Note: The Readme file contains important information relating to the installation of Common Components.

eTrust IAM Install DSA Password: Enter Password

This page of the installation wizard contains the following options:

IAM Install Password

Defines the password that protects the configuration information you are entering for the eTrust Identity and Access Management Common Components installation.

Note: You will need this password when installing the eTrust Identity and Access Management Common Components on additional computers or modifying the installation.

Confirm Password

Defines the IAM Install Password again to make sure there are no mistakes in entering the password.

Express Install: UNIX Platform

This page of the installation wizard appears if you chose to perform an Express install on a UNIX platform because server roles that are not compatible with UNIX need to be installed on a Windows computer. The role installed on the UNIX computer will be the Directory Server role.

Windows Machine Name

Defines the name of the Windows computer where you want to install the Windows-only server roles.

Please read the following license agreement carefully

This page of the installation wizard asks you to read and confirm your acceptance of the license agreement. It has the following options:

I agree

Specifies that you agree with the terms of the license agreement.

Note: You cannot select this option until you have scrolled to the bottom of the displayed license agreement.

I disagree

Specifies that you do not agree with the terms of the license agreement.

Note: You cannot continue with the installation without agreeing to the license agreement.

Policy Manager: Terminal Machines

This page of the installation wizard lets you assign the role of Policy Manager terminals. It contains the following options:

Enter machine names, separated by commas, to add them to the list below

Defines a comma-separated list of computers that you can then add to the list of computers that can be assigned a server role.

Apply

Verifies that the current computer can locate the specified computers on the network and adds them to the list of computers that can be assigned a server role.

Note: 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 other computers.

Policy Server: Assign Computer(s)

This page of the installation wizard lets you assign the role of Provisioning Server. It contains the following options:

Enter machine names, separated by commas, to add them to the list below

Defines a comma-separated list of computers that you can then add to the list of computers that can be assigned a server role.

Apply

Verifies that the current computer can locate the specified computers on the network and adds them to the list of computers that can be assigned a server role.

Indicate which machine(s) will be assigned the role of Policy Server

Specifies which computers will be assigned the role of Policy Server.

Note: Only the selected computers 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 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.

Note: When you are integrating an existing Policy Server computers, you should assign the role of Policy Server to your existing Policy Server computers.

Policy Server: Configuration

This page of the installation wizard lets you configure a Policy Server. It contains the following options:

PS Admin Username

Defines 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).

Default: ps-admin

PS Admin Password / PS Admin Password Confirm

Defines the password for the new PS Admin account that will be created on the Policy Server(s).

LDAP Admin Username

Defines the name that the Policy Server will use 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).

Default: ldap-admin

LDAP Admin Password / LDAP Admin Password Confirm

Defines 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 and store this information in a safe place.

Policy Server: Configure Session Management

This page of the installation wizard lets you determine whether Session Management is enabled. Session Management enables limits to be placed on individual SSO clients connecting to the Policy Server. See the *eTrust SSO Administrators Guide* for information about Session Management.

The page contains the following options:

Disabled

Specifies that Session Management will be disabled.

Enabled

Specifies that session management for SSO clients from eTrust SSO 7.0 and 8.0 is enabled. Clients using eTrust SSO 6.5 will have unlimited sessions.

Required

Specifies that all eTrust SSO users automatically have a default session profile. This setting prevents eTrust SSO 6.5 clients from connecting to the Policy Server.

Policy Server: Install Location

This page of the installation wizard lets you configure where software related to the Policy Server is installed on this computer. It contains the following options:

Policy Server Install Location

Defines the install location for the Policy Server software on this computer.

eTrust Access Control Install Location

Defines the install location for the eTrust Access Control software on this computer.

Policy Server: Password Policy Check Failed

This page of the installation wizard indicates that there was a problem validating the provided password on the target computer. It contains the following option:

<Policy_Server_Admin_Name> Password / <Policy_Server_Admin_Name> Password Confirm

Defines a password that complies with the password restrictions on this computer.

Provisioning Server: ACAS Option

This page of the installation wizards lets you configure the eTrust Access Control Policies (ACP) option when chosen. It contains the following options:

ACAS Username

Indicates the username that can be used to administer the ACAS option on this Provisioning Server.

ACAS Password / Confirm ACAS Password

Defines the password that will be used with the ACAS username.

Provisioning Server: ACC Option: Access Control Install Location

This page of the installation wizard contains the following option:

Access Control Install Location

Defines the installation location for the Access Control software on this computer.

Provisioning Server: Alternates for <computername>

This page of the installation wizard lets you provide load sharing for a Primary Provisioning Server without introducing a new domain. It contains the following options:

Enter machine names, separated by commas, to add them to the list below

Defines a comma-separated list of computers that you can then add to the list of computers that can be assigned a server role.

Apply

Verifies that the current computer can locate the specified computers on the network and adds them to the list of computers that can be assigned a server role.

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

Note: Computers already performing the role of Alternate Provisioning Servers are listed at the bottom of the screen. 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)

This page of the installation wizard lets you assign the role of Provisioning Server. It contains the following options:

Enter machine names, separated by commas, to add them to the list below

Defines a comma-separated list of computers that you can then add to the list of computers that can be assigned a server role.

Apply

Verifies that the current computer can locate the specified computers on the network and adds them to the list of computers that can be assigned a server role.

Indicate which machine(s) will be assigned the role of Primary Provisioning Server

Specifies which computers will be assigned the role of Primary Provisioning Server.

Note: Only the selected computers will be configured to run as a Provisioning Server. You can select multiple computers if you want to run multiple provisioning domains.

Note: When you are integrating an existing Provisioning Server you should assign the role of Provisioning Server to your existing eTrust Admin r8.1 Server. You will need to separately upgrade your provisioning server to r8.1 before installing with the eTrust Identity and Access Management Common Components installation program.

Provisioning Server: Configuration

This page of the installation wizard lets you configure a single Provisioning Server. It contains the following options:

LDAP Port

Indicates the fixed port number used by this Provisioning Server

Provisioning Server Administrator Username

Indicates the user name for the Provisioning Server administrator account on this computer (etaadmin).

Domain Name

Defines the Admin domain created on the Provisioning Server. This can be any acceptable Directory common name string.

Default: The hostname of one of the computers listed as a Provisioning Server.

Note: 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

Defines the description recorded for the administrative user on this computer, such as their name or position title.

Parent of <*computername*>

Defines the parent of the computer that you are configuring as the primary Provisioning Server. This in turn defines relationship of this computer to the root Provisioning Server.

Note: Select ‘None (Root)’ if the currently listed computer is the root Provisioning Server.

Slapd Service Password / Slapd Service Password Confirm

Defines the password required to administer the slapd service on this computer.

Enable Alternate Machines

Specifies whether you want to assign alternate Provisioning Servers to loadshare the role of Provisioning Server for the currently listed computer.

Provisioning Server: Previous Install Detected

This page of the installation wizard appears when a previous installation of the Provisioning Server is detected. It asks you how you want to handle the Provisioning Server repository backup and restore during the upgrade and contains the following options:

Automatic Backup and Restore

Specifies that the installation wizard will perform the necessary backup and restore of the Provisioning Server repository without user intervention.

Manual Backup and Restore

Specifies that the installation wizard relies on a manual backup of the Provisioning Server repository and requires you to manually restore the repository after the back up.

Manual Backup and Automatic Restore

Specifies that the installation wizard relies on a manual backup of the Provisioning Server repository but will perform the recovery automatically at the end of the installation.

Location to Backup Provisioning Server

Defines the location where the backup of the Provisioning Server restore will be placed by the installation wizard.

Provisioning Server: Internal User Passwords

This screen lets you configure passwords for the Provisioning Server internal users. It has the following options:

Domain Server Password / Domain Server Password Confirm

Defines the password for the domain of the current Primary Provisioning Server.

Superagent Password / Superagent Password Confirm

Defines the Superagent password for the current Primary Provisioning Server. The Supeagent server, also known as the eTrust Admin Superagent service, is the component that loads each namespace option’s agent module.

Repository Password / Repository Password Confirm

Defines the password for the current Provisioning Server repository.

Provisioning Server: Install Locations

This page of the installation wizard lets you configure where software related to the Provisioning Server is installed on this computer. It contains the following options:

Provisioning Server Install Location

Defines the install location for the Provisioning Server software on this computer.

CA_APPSW Install Location

Defines the install location for the CA_APPSW software on this computer.

eTrust Common Services Install Location

Defines the install location for the eTrust Common Services software on this computer.

Provisioning Server: Options

This screen lets you select the options you want to install for the Provisioning Server.

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

Some of these options have prerequisites that you must meet before you can successfully install them. See the eTrust Admin Options guides to review the prerequisites for options you want to install.

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

Provisioning Server: Original Internal User Passwords

This screen asks you to enter passwords for the Provisioning Server internal users. It has the following options:

Current Domain Server Password

Defines the password of the domain of the current Primary Provisioning Server installation.

Current Superagent Password

Defines the Superagent password for the current Primary Provisioning Server installation.

Provisioning Server: Password Policy Check Failed

This page of the installation wizard indicates that there was a problem validating the provided password on the target computer. It contains the following option:

Slapd Service Password / Slapd Service Password Confirm

Defines the password that complies with the password restrictions on this computer.

Starting the Installation

This page of the installation wizard contains the following options:

Have you already begun your eTrust Identity and Access Management installation on another machine?

Specifies whether you already performed some of the installation on another computer.

- **No** specifies that no Common Components have been installed on other computers yet.
- **Yes** specifies that you have already started installing Common Components on another computer.

Machine Name

If you chose Yes above, defines the name of the computer were you begun the installation of the Common Components.

IAM Install DSA Password

If you chose Yes above, defines the password you used to protect the configuration information for the Common Components on the first computer you on which installed the Common Components.

Note: If you have already started this installation on another computer, you need to complete the installation on subsequent computers (see page 68).

Tomcat: Install Location

This page of the installation wizard contains the following option:

Tomcat Install Location

Defines the installation location for the Apache Tomcat software on this computer.

Tomcat: Install Option

This page of the installation wizard asks you to specify whether you want to use an existing installation of Apache Tomcat. It has the following options:

YES

Specifies that you want to install Apache Tomcat 4.1.29 on the Web Application Server.

NO

Specifies that Apache Tomcat 4.1.29 is already installed on the Web Application Server and you wish to use this existing installation.

Note: We 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 Identity and Access Management web applications.

Tomcat: JDK Install Location

This page of the installation wizard contains the following option:

JDK Install Location

Defines the installation location for the JDK software on this computer.

Tomcat: JDK Install Option

This page of the installation wizard asks you to specify whether you want to use an existing installation of the Java 2 Software Development Kit (JDK) version 1.4.2_X. It has the following options:

YES

Specifies that you want to install JDK 1.4.2_04 on this computer.

NO

Specifies that JDK 1.4.2_X is already installed on this computer.

Note: If you already have JDK 1.4.2_04 installed on the current computer you must select No. If you select Yes in this case, the installation will fail.

Tomcat: Port Numbers

This page of the installation wizard lets you define the port numbers that are required for configuring Apache Tomcat. It contains the following option:

SSL HTTP Port

Defines the port number used by Tomcat for accepting secure connections.

HTTP Port

defines the port number used by Tomcat for accepting non-secure connections.

Shutdown Port

Defines the port number used to manually shutdown Tomcat.

Tomcat: Windows Service Name

Apache Tomcat is installed as a Windows Service. This page of the installation wizard contains the following option:

Tomcat Windows Service Name

Defines the Windows Service name to for Tomcat on this computer.

Web Application Server: Assign Computer

This page of the installation wizard lets you assign the role of Web Application Server. It contains the following options:

Enter machine names, separated by commas, to add them to the list below

Defines a comma-separated list of computers that you can then add to the list of computers that can be assigned a server role.

Apply

Verifies that the current computer can locate the specified computers on the network and adds them to the list of computers that can be assigned a server role.

Click to mark the machine that will be assigned the role of Web Application Server

Specifies which computer will be assigned the role of Web Application Server.

Note: The Workflow Server must be installed before the Web Application Server. If you choose the current computer as the Web Application Server then you must also choose this same computer as the Workflow Server.

Web Application Server: Configuration

This page of the installation wizard lets you configure the Web Application Server. It contains the following options:

LDAP Hostname

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

ETA Server Domain

Indicates, if known, the eTrust Admin Server Domain name associated with the selected LDAP host.

LDAP Port

Indicates, if known, the unsecured port number (default 20389) that the Directory Server Agent (DSA) uses to connect with the Provisioning Server.

LDAP TLS Port

Indicates, if known, the secured port number (default 20390) that the Directory Server Agent (DSA) uses to connect with the Provisioning Server.

SMTP Server

Defines the SMTP Server name that will provide email capability to the Web Application Server.

Administrator Email Address

Defines the administrator's email address. This address is used if you configure the system to notify the administrator of certain events.

SPML Service Name

Indicates the SPML Service name used by the Web Server.

Web Application Server: Manual Deployment

This page of the installation wizard contains the following option:

Do you wish to deploy the Apache Tomcat, or manually deploy the Web Applications Yourself?

Specifies whether you want to use Apache Tomcat to deploy the eTrust Identity and Access Management Web applications.

- **Use Apache Tomcat** specifies that the installation wizard will install Tomcat on the Web Application Server and automatically deploy the Web applications to it.
- **Manually deploy the web applications** specifies that the installation wizard will not install Tomcat on the Web Application Server.

  Note: If you choose to this option, you need to perform manual steps in order to deploy the Web applications to your custom Web Application Server software. For more information, see the appendix "Installing eTrust Identity and Access Management Web-Based Interfaces on Custom Application Servers" in the *eTrust Admin Implementation Guide*.

Web Application Server: Install Locations

This page of the installation wizard lets you configure where software related to the Web Application Server is installed on this computer. It contains the following options:

IA Manager Install Location

Defines the installation location for the IA Manager software on this computer.

eTrust IAM Self Service Install Location

Defines the installation location for the Self Service software on this computer.

eTrust IAM Self Service Configuration Install Location

Defines the installation location for the Self Service Configuration software on this computer.

eTrust IAM SPML Service Install Location

Defines the installation location for the SPML Service software on this computer.

Web Application Server: JRE Install Location

This page of the installation wizard contains the following option:

JRE Install Location

Defines the installation location for the JRE software on this computer.

Web Application Server: JRE Install Option

This page of the installation wizard asks you to specify whether you want to use an existing installation of Java 2 Runtime Environment (JRE). It has the following options:

YES

Specifies that you want to install JRE 1.4.2_04 on this computer.

NO

Specifies that 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

This page of the installation wizard lets you assign the role of Workflow Server. It contains the following options:

Enter machine names, separated by commas, to add them to the list below

Defines a comma-separated list of computers that you can then add to the list of computers that can be assigned a server role.

Apply

Verifies that the current computer can locate the specified computers on the network and adds them to the list of computers that can be assigned a server role.

Click to mark the machine that will be assigned the role of Workflow Server

Specifies which computer will be assigned the role of Web Application Server.

Note: If you chose the current computer as the Web Application Server then you must also choose this same computer as the Workflow Server.

Workflow Server: Configuration

This page of the installation wizard lets you configure the Web Application Server. It contains the following options:

LDAP Hostname

Specifies which Provisioning Server will provide the LDAP information required by the Workflow Server.

LDAP Port

Indicates, if known, the unsecured port number (default 20389) that the Directory Server Agent (DSA) uses to connect with the Provisioning Server.

Workflow Server: Install Locations

This page of the installation wizard lets you configure where software related to the Workflow Server is installed on this computer. It contains the following options:

Workflow Install Location

Defines the installation location for the Workflow software on this computer.

Ingres Install Location

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

Note: This version of Advantage Ingres is different from 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 settings relevant to the local installation of the software being placed on the computer.

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

1. Insert the first eTrust Identity and Access Management Common Components CD into your CD drive.

   The product explorer for the eTrust Identity and Access Management suite 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. Choose the Installation page from the left navigation pane.

   The Installation page appears.

3. Click Install eTrust IAM Common Components.
4. The product explorer closes and the installation program starts loading and appears after a short delay.
5. Click Next.

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

6. Click Yes, and enter the name of the computer where you started your eTrust Identity and Access Management installation and your IAM Install Password.
7. Click Next.

When the installation program connects to the computer and loads your configuration successfully the Configuration Information Progress screen appears; you will be prompted for additional information (see page 46) 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.

After 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 installation program 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 Common Components are fully installed.

Installation on a UNIX Platform

The Directory Server role can be installed on UNIX platforms as listed in the IAM Readme file.

Note: Due to the multi-CD setup process necessary when installing IAM Common Components, you may need to unmount/mount CDs during installation. UNIX systems may not allow a drive to be unmounted if the application was started from a CD mount point.

To start the install of the IAM Common Components on a UNIX system:

1. Insert Disk 1 of the IAM Common Components into the CD drive
2. Open a console and mount the CD drive
3. Set the umask value to 022
4. Navigate to root (cd /) and type the following command related to your UNIX system.

   ```
   /mnt/cdrom/install/setupsolarisSparc.bin
   /mnt/cdrom/install/setuplinux.bin
   /mnt/cdrom/install/setuphp11x.bin
   /mnt/cdrom/install/setupaix.bin
   ```

   where /mnt/cdrom is the mount point for your UNIX system.

Installation from the Command Prompt

The 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 click Start, Run, and enter **cmd**.
3. Navigate to the Install directory on the CD.
4. Enter **setupwin32.exe –console** and click Enter.

The command prompt installation procedure follows the same steps as the installation wizard.

Reconfiguring the eTrust Identity and Access Management Suite

The installation program lets you reconfigure the computers running the eTrust Identity and Access Management Common Components. You are able to add (but not remove) point products and can also change the computer roles for individual computers.

To reconfigure the eTrust Identity and Access Management Common Components on a computer running Windows, follow these steps:

1. Insert the first eTrust Identity and Access Management Common Components CD into your CD drive.

   The product explorer for the eTrust Identity and Access Management suite 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. Choose the Installation page from the left navigation pane.

   The Installation page appears.

3. Click Install eTrust IAM Common Components.

   The product explorer closes and the installation wizard starts loading and appears after a short delay.

4. On the Starting the Installation screen, click Yes and provide the computer name of one of the Directory Servers and IAM Install DSA Password before clicking Next.

   The eTrust IAM: Reconfiguration screen appears.

5. Select either of the following and click Next.

   Reassign and add machines

   Changes the roles performed by computers in your eTrust Identity and Access Management suite.

   Add supported Point Products

   Adds a point product to your suite and change the roles performed by computers in your eTrust Identity and Access Management suite.

6. Follow the prompts to reconfigure your eTrust Identity and Access Management suite. The Configuration Information: Progress screen (see page 48) lets you 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.

Remove the Common Components

eTrust Identity and Access Management Common Components can be installed across multiple computers. Therefore, removing eTrust Identity and Access Management 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 Take care when uninstalling these components.

The process for removing the Common Components from a single computer is as follows:

1. Uninstall the eTrust Identity and Access Management products from the computer.

   For information about performing this task see to the relevant product implementation guide.

2. Uninstall the eTrust Identity and Access Management Common Components

   For more information, see Removing eTrust Identity and Access Management from each Computer (see page 73).

The following sections explain how to uninstall the eTrust Identity and Access Management Common Components:

- eTrust Identity and Access Management Common Components (excluding third party components)
- CA Tomcat 4.1.29
- JDK
- JRE

You can uninstall every component of the eTrust Identity and Access Management Common Components using the Add/Remove Programs window from the Windows Control Panel.

Removing eTrust Identity and Access Management from Each Computer

When more than one computer has eTrust Identity and Access Management 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 eTrust Identity and Access Management from a computer that is the last remaining Directory Server until eTrust Identity and Access Management 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 Common Components from the current computer, follow these steps:

1. From the Start menu, click 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 click Change/Remove.

   The eTrust Identity and Access Management 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 Directory Server that also has the IAM Install DSA installed. By default, this is only the computer where you first installed eTrust Identity and Access Management Common Components.

   The Summary page appears.

   Note: You must not choose the local computer's machine name until the eTrust Identity and Access Management 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 eTrust Identity and Access Management Common Components from this computer. If you wish to remove eTrust Identity and Access Management 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 Identity and Access Management Common Components.

To uninstall Tomcat, follow these steps:

1. From the Start menu, click Settings, Control Panel, Add/Remove Programs.

   The Add/Remove Programs window appears.

2. Select CA Tomcat 4.1.29, and 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, click 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 Identity and Access Management Common Components.

To uninstall the JDK after uninstalling the Common Components, follow these steps:

1. From the Start menu, click 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 eTrust Identity and Access Management.

Important! Do not uninstall JRE from a computer running eTrust Identity and Access Management Common Components. Remove the Common Components first.

To uninstall JRE, follow these steps:

1. From the Start menu, click 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 click Remove. The JRE uninstaller launches.
3. Follow the prompts to uninstall the JRE.

Customizing Identity and Access Manager

Identity and Access Manager (IA Manager) can be customized to more closely align with your corporate standards and specific requirements.

Styling the Interface

The typefaces and color scheme used by IA Manager are controlled by cascading style sheets (CSS). These files can be modified to manipulate the styling aspects of the interface.

Changes to the CSS files should be made by someone familiar with HTML and style sheet syntax. Backup the file before making changes.

There are two primary CSS files that manage most style aspects of IA Manager. By default, these files are located in:

```
\Program Files\CA\eTrust Identity and Access Manager\Manager\default.css
```

```
\Program Files\CA\eTrust Identity and Access
Manager\Manager\SSOSessionManager\etrust.css
```

Important! We strongly recommend that you carefully consider any changes to minimize the impact on overall structure and screen geometry.

Changing Images

Images used in the default IA Manager interfaces may be replaced with your own branding images. It is important to replace these images with others of the same pixel dimensions to avoid screen layout issues.

If you are replacing these graphics you must maintain the same file names, file formats and pixel dimensions of the existing default images. It is recommended that you make copies of images before overwriting them.

The location of the image files can be customized during installation although by default the path is:

```
\Program Files\CA\eTrust Identity and Access Manager\Manager\Pix\
```

Localization of IA Manager

IA Manager has been certified for the following languages:

- English
- Chinese
- French
- German
- Italian
- Japanese
- Korean
- Portuguese
- Spanish

IA Manager automatically displays screens in one of these languages based on the language settings in the browser used to access IA Manager.

If the browser language settings are not set to one of the supported languages, the screens will be displayed in English by default. To select the language used for IA Manager, open the Preferences from the Preferences link in the upper right corner of every window, then select the language.

Modifying Field Labels and Behaviors

Fields in IA Manager screens can be customized by changes to the XML files specific to that particular screen.

The types of changes possible include:

- Changing the field status between hidden, visible (but not editable) and editable
- Restricting the data that can be placed in fields—either length or character types

The primary .xml files to customize are located by default in:

```
\Program Files\CA\eTrust Identity and Access Manager\WEB-INF\Languages\
```

Administration of eTrust Identity and Access Management

The features and functions for administration of eTrust Identity and Access Management are built into IA Manager. This section covers some of the tasks and activities you might need to perform after eTrust Identity and Access Management is installed.

Starting the eTrust Identity and Access Management Web Applications

The eTrust Identity and Access Management web applications are installed by the Common Components installation program. These applications are:

- Identity and Access Manager (IA Manager)
- Self Service Configuration
- Self Service
- SPML Service Configuration

Each of these web applications starts with a login screen that requires a username and password to access them. Most of these applications are typically accessed only by help desk staff and network administrators although the Self Service application may be configured for a wider group of users.

Each of the installed web applications are available using a program shortcut created on the computer where the eTrust Identity and Access Management Common Components are installed. The shortcuts are located in the Windows Start menu under Programs, Computer Associates, eTrust, eTrust Identity and Access Management.

During rollout of eTrust Identity and Access Management to your organization, you should implement a method for authorized users to easily access these web applications such as providing a desktop shortcut, browser bookmark, Intranet link or Start menu on all desktops.

To start one of the web applications, follow these steps:

1. Manually enter the relevant URL into your internet browser:

   - IA Manager - https://*<hostname.company.com>*:*<sslport>*/CA/IAM/Manager/
   - Self Service Configuration - https://*<hostname.company.com>*:*<sslport>*/CA/IAM/Config/
   - Self Service - https://*<hostname.company.com>*:*<sslport>*/CA/IAM/SelfService/
   - SPML Service Configuration - http://*<hostname.company.com>*:*CA Portal*/iamspml

   where:

   – *<hostname.company.com>* is the fully qualified hostname of the computer acting as the Web Application Server.

   – *<sslport>* is the Apache Tomcat SSL HTTP port number (the default value is 8443).

   – *CA Portal* is the Apache Tomcat HTTP port number (the default value is 8080).

   The login prompt appears.

2. Log in by entering the required fields and clicking the Log In button.

   User Name

   Enter an authorized username, such as etaadmin.

   Password

   Enter the password for the specified user. The initial password for etaadmin will have been provided when installing the Common Components.

   Admin Server

   Required by SPML Service Configuration application only. Enter the name of the Provisioning Server for the specified user.

   Domain

   Required by SPML Service Configuration application only. Enter the name of the domain.

   The relevant web application interface opens.

IA Manager Manual Configuration

During installation you configure some of the functionality of IA Manager however some parameters must be changed manually after installation.

Note: Always make a backup copy of the configuration file before you modify it.

To manually configure the parameters of IA Manager, follow these steps:

1. Using Windows Explorer, browse to the IA Manager directory. By default this directory is Program Files\CA\eTrust Identity and Access Manager\WEB-INF.

   The contents of this directory appear in the right pane.

2. Right-click the etwebadmin.properties file and click Open With.

   The Open With dialog appears.

3. Select a text editor such as Notepad and click OK.

   The etwebadmin.properties file opens.

4. Change the appropriate configuration values, and then save and close the file.

   Note: Modify only those values that display in the Configuration Parameters list.

   The text editor closes.

5. Restart the Apache Tomcat service in Windows Services.

   The manual changes are applied.

Configuration Parameters

You can modify many default configuration values during the installation of IA Manager. After installation, these configuration values can be changed by editing the configuration file manually.

Note: Parameters, paths, or text strings that contain spaces must be entered in quotation marks ("xxx") preceded by a back slash (\). For example, enter \"C:\Program Files\CA\".

During silent mode installation, configuration values with a command line parameter can be set from the command line. However, not all configuration parameters have a command line parameter.

def_search_results

Defines the maximum number of search results to return in the search pane.

Default: 100

eta_domain

Command Line Parameter: ETASERVERDOMAIN

Defines the eTrust Admin Server domain name. This is usually the name of the computer on which eTrust Admin Server is installed, unless changes were made during that installation.

Default: localhost_name

ldap_host

Command Line Parameter: LDAPHOSTNAME

Identifies the computer that serves as the LDAP host. This is the computer on which eTrust Admin Server is installed.

Default: localhost_name

ldap_port

Command Line Parameter: LDAPPORT

Defines the LDAP port number.

Default: 20389

ldap_tlsPort

Command Line Parameter: LDAPTLSPORT

Defines the LDAP port number using TLS/SSL encryption.

Default: 20390

ldap_useTls

Indicates whether to use TLS/SSL encryption. 1 indicates to use TSL/SSL encryption; 0 indicates not to use the encryption.

Default: 1

log_error_detail

Indicates the level of errors logged. Enter a level from 1 to 4.

Default: 4

log_enabled

Indicates whether to enable logging. 1 indicates that logging is enabled; 0 indicates that it is disabled.

Default: 1

Max_Picture_Size_Kilobytes

Defines the maximum file size (in kb) that can be uploaded as a user photograph.

Default: 25

pass_rst_req_enabled

Indicates whether a user can request a password reset. 1 indicates that this option is enabled; 0 indicates that this option is disabled.

Default: 1

pass_rst_req_smtp

Command Line Parameter: SMTPSERVER

Defines the SMTP mail server.

Default: your_smtp_server

pass_rst_req_user

Command Line Parameter: ADMINEMAIL

Defines the administrator's email address.

Default: admin@your_company.com

self_admin_unlock_account_enabled

Indicates whether the administrator can unlock an account. 1 enables this option; 0 disables this option.

Default: 1

web_admin

Defines the user name of the Web application administrator.

Default: etawebad

Note: You can modify the web_admin attribute only if the password for the web_admin user is **changeoninstall**.

Troubleshooting IA Manager

IA Manager has many components which may require separate administrative tasks. This section describes some of the more common administrative tasks that you may perform.

Start or Restart a Windows Service

The Windows services required by IA Manager include:

- Apache Tomcat Service—The default service name is *CA Tomcat 4.1.29 eTrustIAMWebServer*.
- Advantage Ingres—The default service name is *Ingres Intelligent Database [ET]*.
- Directory Web Server—The default service name is *eTrust Directory Web Server*.
- SSO Session Administrator—The default service name is *eTrust SSO Session Administrator*.

To start a service running in Microsoft Windows Services, follow these steps:

1. Open the Windows Control Panel from the Start menu. Double-click Administrative Tools and then Services.

   The Services dialog appears.

2. Locate the appropriate service and right-click it.

   A pop-up menu appears.

3. If it is not already started, select Start from the pop-up menu. If it is already started, select Restart.

   The service will be listed as Started.

   Note: This service should start automatically after you have installed the IA Manager and also every time you start your machine. Verify that the service is listed as Automatic to ensure that it starts on a computer reboot.

4. Repeat this procedure for any other services, as necessary.

Stop a Windows Service

If a Windows service conflicts with services required by IA Manager, it may be necessary to stop the Windows service.

To stop a service in Microsoft Windows Services, follow these steps:

1. Open the Windows Control Panel from the Start menu. Double-click Administrative Tools and then Services.

   The Services dialog appears.

2. Locate the appropriate service and right-click it.

   A pop-up menu appears.

3. Select Stop from the pop-up menu.

   The selected service stops.

Note: After you stop a conflicting process, you must start or restart the service that was in conflict. For more information, see Start a Windows Service.

Securing your eTrust Identity and Access Management Web Applications

The eTrust Identity and Access Management suite of products rely on web applications which are secured using the SSL protocols with self-signed certificates. To fully secure your product suite you should replace the self-signed certificates with certificates signed by a certifying authority.

If your organization does not have an internal certifying authority:

1. Use Self Signed host certificates. This is how the default eTrust Identity and Access Management installation is created as it is impossible for the installer to create widely trusted certificates. Although this installation is not optimal, it can be useful for testing. If you wish to install self signed certificates on a web server not installed by the eTrust Identity and Access Management installation see Replace the Tomcat SSL Certificate.

   Using Self Signed certificates has the following drawbacks:

   - Client computers cannot be assured of the identity of the web servers.
   - Each time a browser connects to a web server a warning about invalid certificates will be presented. This can confuse users and be a potential source of help desk calls.

2. Use host certificates from a trusted Certifying Authority. This is the recommended option.

   - Obtain host certificates and private keys for all web server hosts from a trusted Certifying Authority such as Verisign or Thawte.
   - Install these host certificates and keys in your Tomcat keystore on each web server host. See Replace the Tomcat SSL Certificate.

If your organization has an internal certifying authority:

1. Issue host certificates and private keys for all web server hosts.
2. Install these host certificates and keys in your Tomcat keystore on each web server host. See Replace the Tomcat SSL Certificate.
3. Install the host certificates in the browser keystore on all client computers.
4. Install the host certificates in the Tomcat keystore on all server computers.

Configure SSL Support for Tomcat

eTrust Identity and Access Management web application servers must have Tomcat configured to use SSL protocol. This is the default when installing Tomcat using the eTrust Identity and Access Management Common Components installation program; however, if you installed Tomcat independently, it may not be configured with SSL support.

Note: The following procedure is provided for reference only. You may want to configure your SSL certificate differently or change your keystore password to one of your own choosing for better security.

To install and configure SSL support for Tomcat using a self-signed certificate, follow these steps:

1. Verify that JDK version 1.4.2_04 is installed by checking the Add/Remove Programs list in your Control Panel for the program Java 2 SDK, SE v 1.4.2_04.

2. Create a new keystore containing one self-signed certificate by entering the appropriate command from the command prompt.

   On Windows systems, you should enter:

   ```
   %JAVA_HOME%\bin\keytool -genkey -alias tomcat -keyalg RSA -keystore
   \path\keystore_filename
   ```

   On UNIX systems, you should enter:

   ```
   %JAVA_HOME%/bin/keytool -genkey -alias tomcat -keyalg RSA -keystore
   \path\keystore_filename
   ```

   The keystore creation process begins.

3. Enter the keystore password when prompted.

   Note: The default password used by Tomcat is *changeit* (all lower case). If preferred, you can specify a custom password, but you must then specify the custom password in the server.xml configuration file also (see Step 8).

   The keystore creation process continues.

4. Enter general information for the certificate when prompted. The general information includes company, contact name, and so on. This information displays to users who attempt to access a secure page in your application, so make sure that the information provided here is appropriate.

   The keystore creation process continues.

5. Enter the key password when prompted. This password is created specifically for this certificate (as opposed to any other certificates stored in the same keystore file). You must use the same password for this and the keystore password.

   A keystore file with a certificate that your server can use is created.

6. Browse to the <*Tomcat_installation_directory*>\conf\ directory and open the server.xml file in a text editor.

The default location for the <*Tomcat_installation_directory*> when installed from the IAM Common Components CD is C:\Program Files\CA\SharedComponents\Tomcat\4.1.29.

7. Ensure that the SSL Coyote HTTP/1.1 Connector entry is not commented out in the file. The connector information looks similar to the following:

```
<!-- Define an SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector className="org.apache.catalina.connector.http.HttpConnector"
      port="8443" minProcessors="5" maxProcessors="75"
      enableLookups="true" acceptCount="10" debug="0" scheme="https"
      secure="true">
 <Factory className="org.apache.catalina.net.SSLServerSocketFactory"
      clientAuth="false" protocol="TLS"/>
</Connector>
-->
```

   If the Connector element is commented out, you must remove the comment tags (<!-- and -->) around it.

8. Configure the SSL Coyote HTTP/1.1 Connector entry to include the keystoreFile and keystorePass attributes for the Factory element.

   keystoreFile

   Specifies the location where the keystore file is located

   keystorePass

   Specifies the keystore (and certificate) password

   The connector information should look similar to the following:

```
<Connector className="org.apache.catalina.connector.http.HttpConnector"
      port="8443" minProcessors="5" maxProcessors="75"
      enableLookups="true" acceptCount="10" debug="0" scheme="https"
      secure="true">
 <Factory className="org.apache.catalina.net.SSLServerSocketFactory"
      keystoreFile="your_keystore_full_path"
      keystorePass="your_keystore_password"
      clientAuth="false" protocol="TLS"/>
</Connector>
```

9. Save the file and close it.

   SSL support and self-signed certificates are configured for Tomcat.

10. Restart the Tomcat server.

Note: For more information, see the *SSL Configuration HOW-TO* document for Tomcat 4.1 on the Apache Jakarta Project web site.

Replace the Tomcat SSL Certificate

Your Tomcat SSL Certificate enables users browsing to your web pages to transmit and receive secure information. Certificates may be self-signed or provided by an independent third party. You can update your Tomcat SSL Certificate to improve the security of the information shared through web browsers.

To replace the Certificate for Tomcat SSL support, follow these steps:

1. Browse to the <*Tomcat_installation_directory*>\conf\ directory and open the server.xml file in a text editor.

   The default location for this file is C:\Program Files\CA\SharedComponents\Tomcat\4.1.29\conf\server.xml.

   The text file opens.

2. Search for the following text: keystoreFile. Change the attributes to present the replacement information.

   keystoreFile

   Specifies the location in which the keystore file is located.

   keystorePass

   Specifies the keystore (and certificate) password.

   The file reflects these changes.

3. Save the file and close it.

   The information is stored.

Note: For more information, see the SSL Configuration HOW-TO document for Tomcat 4.1 on the Apache Jakarta Project web site.

Resolving Port Conflicts Manually

This section is included for resolving Apache Tomcat port conflicts. For information about how to resolve Apache Tomcat port conflicts not covered here, see your Apache Tomcat documentation or the Apache Tomcat web site.

If you cannot run a particular installation of Apache Tomcat, one or more of the ports for which it is configured may currently be in use by another program (for example, another installation of Tomcat or some other web server). To rectify this problem, you must reconfigure the "broken" Tomcat to use different values for the Shutdown port, the Non-SSL HTTP port, and the SSL HTTP port.

To reconfigure the port values, follow these steps:

1. Browse to the <*Tomcat_installation_directory*>\conf\ directory and open the server.xml file in a text editor.

   The default full path for this file is C:\Program Files\CA\SharedComponents\Tomcat\4.1.29\conf\server.xml.

2. Search for the following text: Server port=.

   The text is highlighted.

3. Change the value that appears after Server port =. For example, if the number is 8005, change it to 9005.

   Note: The new port number must be greater than 1024 and less than 41152, and must not be in use by any other program on your computer.

   The number you entered now appears as the new port number for Tomcat's Shutdown port.

4. Now, search for the following text: Define a non-SSL Coyote HTTP.

   The text is highlighted.

5. From this position in the file, search for the following text: port=.

   The text is highlighted.

6. Change the value that appears after port=. For example, if the number is 8080, change it to 9080.

   Note: The new port number must be greater than 1024 and less than 41152, and must not be in use by any other program on your computer.

   The number you entered now appears as the new port number for Tomcat's non-SSL HTTP port.

7. Now, search for the following text: Define a SSL Coyote HTTP.

   The text is highlighted.

8. From this position in the file, search for the following text: port=.

   The text is highlighted.

9. Change the value that appears after port=. For example, if the number is 8443, change it to 9443.

   Note: The new port number must be greater than 1024 and less than 41152, and must not be in use by any other program on your computer.

   The number you entered now appears as the new port number for Tomcat's SSL HTTP port.

10. Return to the beginning of the file and search for all instances of the following text: redirectPort=. For each instance, change the value that appears after redirectPort= to the same number that you entered for the new port number for Tomcat's SSL HTTP port.

    Note: Tomcat's SSL HTTP Port and Redirect port must use the same number.

11. Save the file, close it, and try to run this particular installation of Apache Tomcat again. Verify that Tomcat started correctly by entering the following URL in your web browser: http://localhost:8080/index.jsp. If you see the Apache Tomcat web page, it has started correctly. If not, Tomcat has not started.

    If Tomcat starts correctly, you have successfully resolved your Tomcat port conflicts.

Note: For more information about how to start Tomcat, see Start Apache Tomcat or see your Apache Tomcat documentation.

Chapter 4: Installing and Customizing eTrust AC for UNIX

This chapter guides through the eTrust AC for UNIX installation process. When you have finished installing eTrust AC following the instructions in this chapter, your system should contain a copy of the eTrust AC software and an elementary eTrust AC database. The chapter then explains how to start eTrust AC and how to use its commands. Later, by editing the database, you can define access rules to protect your system.

This section contains the following topics:

Before You Begin

Before you can install eTrust AC, you must make sure certain preliminary requirements are met and several items of necessary information are available.

Operating System Support and Requirements

You can install eTrust AC on any one of the supported versions of the UNIX operating system. Make sure you have checked the Operating System Support and System Requirements sections of the Readme file for this product.

Defining Administration Terminals

You can administer eTrust AC policy from a central place using PMDB, or by connecting to the computer either with command line (selang) or through the Policy Manager GUI and updating the policy directly on the computer.

In order to update the computer's policy directly, you need the write access on the terminal you are managing from and the admin attribute on the computer policy in the eTrust AC database.

By default, eTrust AC installation sets up terminal authority only for the local computer terminal. You can change that by either disabling this option from a local terminal or adding more terminals that can manage remotely.

To add administration option for terminal my_terminal to machine my_machine using user <my_user>, write the following selang rules:

```
eTrustAC> nr terminal <my_terminal> owner(nobody) defaccess(r)
(localhost)
Successfully created TERMINAL <my_terminal>

eTrustAC> auth terminal <my_terminal> uid(<my_uid>) access(all)
(localhost)
Successfully added <my_uid> to <my_terminal>'s ACL
```

Note: These rules also allow everyone to login from this terminal (regular login, not management), and allow my_uid both regular login and eTrust AC management option.

Installation Notes

When installing eTrust AC (whether for the first time or as part of an upgrade), note the following:

- Read the *eTrustACDir*/README.TXT file

  (where *eTrustACDir* is the installation directory).

- If your environment is set up with a PMDB hierarchy or you are setting such an environment, we *recommend* that you:

  – Install or upgrade the Deployment Map Server (DMS) computer first.

    This is only required if you are going to use advanced policy-based management, and ensures that the DMS registers each Policy Model node and its subscribers.

  – Install or upgrade each computer in your hierarchy bottom-up (subscribers first).

    Upgraded PMDBs having subscribers with an earlier version may result in erroneous commands being sent. This can happen as a result of new PMDBs containing classes and properties that do not exist in the earlier version PMDBs.

  – Choose to install a Deployment Map Agent (DMA) on each computer with at least one PMDB if you are going to use advanced policy-based management.

  – Backup the PMDB:

    a. Shut down the Policy Model daemons using the following command:

       ```
       sepmd -k pmd_name
       ```

       All daemons are shut down when eTrust AC is shut down.

    b. Copy the *eACInsatllDir*/policies directory to a backup location.

- eTrust AC selang commands from r5.1 are supported in later versions so earlier PMDBs can propagate to eTrust AC r8 SP1 subscribers but not vice versa.

- If you are upgrading from an earlier version:

  – Programs that should be bypassed by STOP will now be defined as database rules; SPECIALPGM records of a *stop* type.

  – Programs that should be bypassed by SURROGATE will now be defined as database rules; SPECIALPGM records of a *surrogate* type.

  Note: The upgrade process converts old definitions (kept in a file) to the new database rules. You will need to add these new rules to any existing selang scripts.

- You can upgrade the existing seos.ini and pmd.ini files, or create new ones.

Either way, the installation script saves a copy of the old seos.ini file as seos_ini.back and a copy of each pmd.ini file as pmd_ini.back (in its respective Policy Model directory).

- If you are upgrading from eTrust AC r5.1 SP2 or earlier versions on Solaris, AIX, HP-UX, or Linux platforms, you must reboot the computer during installation. However, if this is a first-time installation of eTrust AC, you do not have to reboot during the installation process.
- If you are upgrading an existing database, we recommend that you:
  - Back it up first.

    Use dbmgr -b to backup the database.
  - Ensure that there are no subscribers in *sync* mode.

    Use sepmd -L to verify subscriber's status.

If you are using a regular installation (not a native installation), you will use five files from the eTrust AC media:

- A script that installs eTrust AC from the tar file. Its name is install_base.
- A compressed tar file containing all the eTrust AC files. Its name is *_opSystemVersion_eTrustACVersion*.tar.Z. For example, if you are installing eTrust AC r8 on IBM AIX version 5 then your tar file is _AIX5_800.tar.Z
- A compressed tar file named pre.tar containing messages for installation as well as the license agreement.

  After you have read the license agreement file, you can continue the installation by entering the command found at the end of that file. If you are running a silent install (using -autocfg), you can use the -command flag with the command that can be found at the bottom of the license agreement file. If you are using a response file (-autocfg file_name), you do not need to use the -command flag. To get the license file name and location, you must run install_base -h. You can also get the file name and location if you enter the wrong command.
- A script that installs Remote Status View (RSV) from the tar file. Its name is install_rsv.
- A compressed tar file containing all the Remote Status View (RSV) files. Its name is RSV_800.tar.Z

Note: To install the standalone Policy Manager, use the installation instructions provided in the *User Guide*. The installation files for the Policy Manager are available on the eTrust AC for UNIX CD #2.

Install eTrust AC

The easiest way to install eTrust AC is to use the install_base script interactively. You can also run a silent install of eTrust AC.

Note: Before you run the install_base script, make sure you decide which functionality you want to install and review the install_base command (see page 97) so you know how to initiate the installation of this functionality. You may also want to learn first how the install_base script works (see page 102).

To install eTrust AC

1. If you already have eTrust AC installed and it is running, shut it down by logging in as an administrator and entering the following commands:

   ```
   # eTrustACDir/bin/secons -sk
   # eTrustACDir/bin/SEOS_load -u
   ```

   Note: If the eTrust AC version you have installed is 5.1 or earlier, issue the following command instead:
   # eTrustACDir/bin/secons -s

2. Log in as *root*.

   In order to install eTrust AC, you need to have root permissions.

3. Mount the CD-ROM drive.

   Important! If you are installing on HP from a CD-ROM, you need to ensure the proper reading of file names from the CD-ROM. To prevent the file names from being forced into a shortened and all-uppercase format, enter the **pfs_mountd &** and the **pfsd &** commands and make sure that the following four daemons are invoked: pfs_mountd, pfsd.rpc, pfs_mountd.rpc, and pfsd. For more information, see the man pages of the particular pfs* daemons and commands.

4. Read the license agreement.

   To run the install_base script you need to accept the End User License Agreement. After you have read the license agreement, you can continue the installation by entering the command found at the end of that file. To get the license file name and location, run install_base -h.

5. Run the install_base script from the CD, by using the install_base command (see page 97).

   The install_base script starts and, based on your choices, prompts you for the appropriate installation questions.

   Note: The installation script finds the appropriate compressed tar file, so typing the name the tar file for your platform is optional.

6. Append the *eTrustACDir*/bin directory to your path (where *eTrustACDir* is the installation directory).

7. Check the seos.ini (see page 126) file tokens to make sure that the settings meet your requirements.

   If necessary, modify the settings.

8. For upgrades from version 5.x, reboot the computer by entering:

   ```
   reboot
   ```

   Now the eTrust AC installation is complete; however, it is not yet running.

9. To give yourself access to the eTrust AC man pages, add the directory *eTrustACDir*/man to your MANPATH.

   For example, if you are using csh, for the sake of your current session, enter the command:

   ```
   # setenv MANPATH $MANPATH:eTrustACDir/man
   ```

   where *eTrustACDir* is the installation directory for eTrust AC.

   For the sake of future sessions, add a similar line to your .login, .profile, or .cshrc file.

Example: Install the client and server packages with default features

The following command shows how you would initiate the install_base interactive script to install the client and server packages with all default eTrust AC features. During the installation you will be asked to answer questions related to installing the client and server packages of eTrust AC.

```
# /cdrom/Unix/Access-Control/install_base
```

Note: As we did not specify a package to install, the install_base command installs both client and server packages.

Example: Install the admin package to a custom directory

The following command shows how you would initiate the install_base interactive script to install the administration tools package to the /opt/CA/AC directory.

```
# /cdrom/Unix/Access-Control/install_base -admin -d /opt/CA/AC
```

Note: To install the admin package to a custom directory we must have already installed the client package to the same directory.

Example: Install the client and server packages with STOP enabled

The following command shows how you would initiate the install_base interactive script to install the client and server packages and enable the Stack Overflow Protection option.

```
# /cdrom/Unix/Access-Control/install_base -stop
```

Note: As we did not specify a package to install, the install_base command installs both client and server packages.

install_base Command—Run Installation Script

The install_base command runs the installation script and installs one or more of the eTrust AC packages with one or more of the selected installation options.

install_base [*tar_file*] [*packages*] [*options*]

tar_file

(Optional). Defines the name of the tar file containing the eTrust AC installation files for your platform. The installation script finds the appropriate compressed tar file automatically, so typing the name of your tar file is optional.

packages

(Optional) Defines the eTrust AC packages you want to install. If you do not specify any packages, the installation script installs both the client and server packages unless you are upgrading eTrust AC, in which case the installation script installs the same packages you already have installed.

Note: You must install the client package before you install any other package. You can, however, specify to install the client package together with any other package.

The following are the eTrust AC packages you can install:

-admin

Installs the administration tools package that includes the Motif GUI.

-all

Installs all eTrust AC packages. These are the client package, server package, API package, Unicenter security integration and migration package, MFSD package, the administration tools package, and the documentation package. It also enables STOP (-stop option).

-api

Installs the API package that includes API libraries and sample programs.

-client

Installs the client package that has the core eTrust AC functionality required for a standalone computer.

-doc

Installs the documentation package that includes user documentation in a PDF format. eTrust AC installs the documentation in the eTrust AC installation directory under a Doc subdirectory.

-mfsd

Installs the MFSD package that includes the mainframe synchronization daemon.

Note: You must install the server package before you install the MFSD package.

-server

Installs the server package includes more binaries and scripts (selogrcd, sepmd, sepmdd, sepmdadm, secrepsw, and the web-based utility RSV). These complement the client package. For example, sepmdd lets you set the computer with a Policy Model.

-uni

Installs the Unicenter security integration and migration package that supports eTrust AC integration with CAUTIL, Workload Management, and Event Management components of Unicenter, and the Unicenter EMSec API.

Note: Unicenter security integration and migration is only available for AIX, HP-UX PA-RISC, Solaris SPARC, and Linux x86 platforms.

options

(Optional). Defines additional installation options you want to set.

Note: Installation options that affect eTrust AC functionality, (for example, -stop) can only be specified when you install the *client* package. Installation options that affect the installation process (for example, -verbose) can be specified with any package.

The following are the options you can specify:

-advreport

Specifies that the installation asks you questions for configuring advanced policy management and reporting functionality on this computer.

Note: You can also configure advanced policy management and reporting (see page 128) after the installation is complete.

-autocfg [<*response_file*>]

Runs the installation in silent mode (not in interactive mode). If a response file is specified, the installation uses the preferences stored in the file to automatically respond to the interactive installation process. If you do not specify a response file, or if the response file is missing any options, the installation uses preset defaults. To create a response file use the *-savecfg* option.

Important! If you do not specify a response file, you must use the *-command* option when using the *-autocfg* option.

When running a silent installation, consider the following:

- You cannot change the encryption key.
- Only the client and server packages are installed by default.

  To install any other package or feature, you must specify the appropriate option as you would in a normal installation.
- The install_base command does not print installation details on the screen during installation.

  To view installation messages on the screen during installation, use the *-verbose* option.

-command <*command*>

Defines the command that specifies that you accept the license agreement. This command can be found at the end of the license agreement and you must use it when you use the -autocfg option. To locate the license agreement file, run *install_base -h*.

Note: The license agreement is only available while the help is displayed. When you finish reading the help, the license agreement is deleted.

-d *target_dir*

Defines a custom installation directory. The default installation directory is /opt/CA/eTrustAccessControl.

Important! You cannot put the eTrust AC database in a mounted network file system (NFS).

-*dns* | -nodns

Creates a lookaside database with or without DNS hosts. The -nodns option specifies that eTrust AC will not perform an nslookup on any hosts in the DNS during installation.

-force

Forces the installation to ignore an active new subscriber update (*sepmd -n* and *subs <pmdb> newsubs(sub_name)*) and continue the installation. By default, the installation stops and asks you to finish the subscriber update first.

Note: If you use this option, the new subscriber update will fail.

-force_encrypt

Forces the installation to accept a non-default encryption key without warning you.

Important! After the upgrade is complete, your encryption key is set to the default.

Note: eTrust AC also provides AES (128bit, 192bit, and 256bit), DES, and 3DES encryption options that you can choose.

-force_install

Forces the new installation over the version already installed.

-force_kernel

Forces the installation to continue without warning you it cannot unload your old kernel.

Note: You may need to reboot the computer after the installation is complete.

-g *groupname*

Defines the name of the group owner of eTrust AC files. The default value is 0.

-h | -help

Displays help for this command.

-ignore_dep

Specifies that the installation does *not* check for dependency with other products.

-key <*encryption_key*>

Restores your encryption key during an upgrade.

Note: During an upgrade you must use the same encryption key that you used before the upgrade.

-lang <*lang*>

Defines the language in which to install eTrust AC. For a list of supported languages and character sets, read the description for this option when you display the help (install_base -h).

-lic_dir <*license_dir*>

If the license program is not already installed, defines the license program installation directory.

Note: The license program will be installed to the specified directory only if $CASHCOMP variable is not defined in your or the computer's environment (it can be defined in /etc/profile.CA). Otherwise, it will be installed to $CASHCOMP. If $CASHCOMP is not defined and you do not specify -lic_dir, the license program will be installed to the /opt/CA/SharedComponents directory. CAWIN is installed to the same directory as the license package.

-nolog

Specifies that a log is not kept for the installation process. By default, all transactions associated with the installation process are stored to *eTrustACDir*/eTrustAC_install.log (where *eTrustACDir* is the installation directory for eTrust AC).

-no_tng_int

Specifies for the installation not to attempt to set up selogrd integration with Unicenter Event Management.

If you do not specify this option, the installation script checks whether Unicenter Event Management is installed. If the script finds that Unicenter Event Management seems to be installed, it sets up selogrd integration with Unicenter Event Management by adding the following line to selogrd.cfg:

```
uni hostname
```

-post <*program_name*>

Specifies a program to run after the installation is complete.

-pre <*program_name*>

Specifies a program to run before the installation starts.

-rootprop

Specifies that sepass changes to the root password are sent to the Policy Model.

Note: You can set this after the installation is complete using the AllowRootProp token of the seos.ini file. For more information about the seos.ini initialization file, see the *Reference Guide*.

-savecfg <*response_file*>

Stores your responses to the interactive installation for later use by the -*autocfg* option.

-stop

Enables the use of the STOP (Stack Overflow Protection) feature.

-system_resolve

Specifies to use system functions, which define a bypass for network caching on your system.

Note: You cannot use this option on IBM AIX platforms.

-verbose

Specifies that installation messages are displayed on the screen during installation. This is the default in an interactive installation and you only need to specify this option if you want to see these messages when you use the *-autocfg* option.

How the install_base Script Works

The install_base script performs the following steps:

1. The install_base script extracts the data from the tar.Z file into the installation location (default or as specified by *target_dir*).
2. Different platforms cause different actions:
   - For Sun Solaris, the install_base script adds the eTrust AC *syscall* script to the file /etc/name_to_sysnum. The original file is saved as /etc/name_to_sysnum.bak. It then creates the file /etc/rc2.d/S68SEOS that forms part of the boot sequence.
   - For IBM AIX, it loads the SEOS_syscall script.
3. The script allocates, initializes, and formats the eTrust AC database and builds the seos.ini file. The database files are placed in the *eTrustACDir*/seosdb directory (where *eTrustACDir* is the eTrust AC installation directory.)
4. Determines if the machine is NIS+. If it is, it sets the nis_env token in the [passwd] section to **nisplus**; otherwise, if the machine is NIS, it sets the token to **nis**. In addition, if rpc.nisd is running, the script sets the NisPlus_server token in the [passwd] section to yes.
5. Under supported 32-bit platforms Sun Solaris, IBM AIX, HP-UX, and Linux the install_base script determines if the machine is running under NIS or DNS (using caching). If it is, the script automatically creates a lookaside database and sets two tokens in the [seosd] section of the seos.ini file to yes: under_NIS_server and use_lookaside.

   Note: On other platforms the script prompts you for whether you want to install a lookaside database and for the target installation directory.

6. Prompts you for the following additional information: (You can modify these settings any time after installation.)

   - The name for the group of auditors that can read the audit file.
   - Whether you want to add all your UNIX users, user groups, and hosts to the eTrust AC database now.
   - Whether you want your database to be subscribed to a PMDB; and if so, to which one.

     Your answer does not actually subscribe your database to a PMDB; it only lets the specified PMDB make updates to this database when you create the subscription later.

     Two safe responses to this question include:

If you want to:	Respond with:
Allow your database to be subscribed to a specific PMDB	The name of the PMDB in the format *pmd_name@hostname*
Prevent your database from being subscribed to any PMDB (at least until you specify otherwise)	The Enter key.

     A third response, _NO_MASTER_ , allows your database to be subscribed to any PMDB. However, this can be a dangerous response, because it removes the selection of the PMDB from your control.

   - The password Policy Model name.
   - What users will be security administrators for eTrust AC.
   - Whether you want to replace the default encryption method.

     Note: Communication between eTrust AC and a Policy Manager instance on a different server is encrypted. By default, eTrust AC uses a fast and efficient scrambling algorithm for encryption. Installations of eTrust AC and Policy Manager use the same encryption key, enabling encrypted communication as soon as the installation is complete.

     eTrust AC also provides AES (128bit, 192bit, and 256bit), DES, and 3DES encryption options that you can choose.

   - Whether you want to set a new encryption key.

     Note: See sechkey in the *Utilities Guide* for information about encryption.

- Whether you want to install the Baseline Security rules.

  Baseline Security rules offer administrators an opportunity to install a package containing two sets of rules to better protect your system, password and log files. One set of rules applies to all platforms to protect eTrust AC files. The other set protects UNIX files and is specific to the Sun Solaris, HP-UX, IBM AIX, and Digital DEC UNIX platforms. You cannot install one set of rules without the other. Baseline Security rules install in Warning mode providing you with information but not actual protection. That is why we recommend that you remove the Warning mode as soon as you become familiar with the rules.

- Whether you want to be able to start eTrust AC from a remote host.

7. Calls another script (if you specify the *-advreport* option to install advanced policy management and reporting) and prompts you for the following information:

   - Whether you want to install a Deployment Map Server (DMS); and if so:
     - The DMS name (a PMDB to use for data repository).
     - DMS administrator names.
     - DMS administration terminals.
   - Whether you want to install a Deployment Map Agent (DMA); and if so:
     - The names of the DMS databases to send notifications to.
     - DMA administrator names.
     - DMA administration terminals.
   - The names of DMS databases to send calculation deviation results to (if you did not install a DMA).

8. Prompts you for whether you want to view the readme file.

Install eTrust AC from Unicenter Software Delivery

To install eTrust AC with Unicenter Software Delivery, follow these steps:

Note: The eTrust AC installation CD contains a directory named SDPackages. This directory contains several files that are required to install eTrust AC using Unicenter Software Delivery.

1. To register the eTrust AC Unicenter Software Delivery package, insert the eTrust AC installation CD into your drive.

   The Product Explorer appears.

2. Register the Unicenter Software Delivery package by clicking Supporting Products, and then clicking Registering in Unicenter Software Delivery.

3. Click the package to install. (For example, you might choose **eTrustAccessControlHPUX**.)

   The License Agreement window displays.

4. Scroll down to the end of the license and accept the license by clicking **I agree**.

   The Choose Products to Register window displays again with the package you selected marked.

5. Click Next to proceed with the registration process.

6. Enter the server name for the Unicenter Software Delivery server, and click Next.

   The package is registered on the server you selected.

7. To install the package, open the installation procedure in the All Software\Software *Library\package* directory on the Unicenter Software Delivery server explorer and drag it into the agent or agent group you want to install in.

Silent Install eTrust AC from Unicenter Software Delivery

From the UNIX command line, you can create a response file for silent installations, register the package, install eTrust AC to agent machines, and uninstall eTrust AC.

Generate a Response File

To generate a response file from the UNIX command line, follow these steps:

1. Enter the following commands on the server:

   ```
   mkdir my_tmp_reginfo/HPUX
   cd my_tmp_reginfo/HPUX
   cp cdrom/SDPackages/eTrustAccessControl.HPUX.@pif
   pifask -f ./eTrustAccessControl.HPUX.@pif -r ./eTrustAccessControl.resp
   ```

   Dialogs will open, simulating installation.

2. Complete the dialogs.

   As the process completes, you will receive a message that the response file is created.

   Note: The response file must be in UNIX format. You can FTP from UNIX using the FTP bin option.

3. Copy the response file back to the to the SDPackages directory.

Register the Package

To register the package from the UNIX command line, follow these steps:

1. Log in to the Unicenter Software Delivery server as root, mount the installation CD, and change the directory to /*cdrom*/SDPackages.

2. Run the **sdregister** command with the platform you want to register the package on:

   ```
   ./sdregister -d platform_dir
   ```

   where *platform_dir* is the name of the subdirectory in the SDPackages directory containing files for the platform you want to register on.

   A message appears, confirming registration of the software package.

3. Accept the license agreement by scrolling to the end of the agreement and clicking Yes.

4. Enter the server name, user name, and password to register with.

   The command line registers the package for you.

Install the Package

To install eTrust AC using Unicenter Software Delivery, follow these steps:

1. On the computer serving as the Unicenter Software Delivery server, enter the sdcmd installation command for your platform. For example, you might enter the following:

   ```
   >sdcmd install item="eTrustAccessControl(HPUX)" version=5500 after=exacttime
   computer=computer_name\ procedure="Install Package with
   eTrustAccessControl.resp"
   ```

2. Enter the following command to show the status of the installation

   ```
   >sdcmd computer_name action=listJobs name=computer_name
   ```

3. After a message appears that states EXECUTION_OK, check that eTrust AC installed as you desired on *computer_name*.

Uninstall the Package

To uninstall eTrust AC using Unicenter Software Delivery, follow these steps:

1. On the computer serving as the Unicenter Software Delivery server, enter the following command:

   ```
   >sdcmd uninstall item="eTrustAccessControl(HPUX)" version=5500
   procedure="Uninstall Package" installed with="Install Package with
   eTrustAccessControl.resp" after=exacttime computer=computer_name
   ```

2. After a message appears that states: EXECUTION_OK, check that eTrust AC is uninstalled on *computer_name*.

Install eTrust AC Using RPM Package Manager

The RPM Package Manager (RPM) is a command-line utility that lets you build, install, query, verify, update, and erase individual software packages. It is intended for use on UNIX platforms.

Note: For more information, see the RPM Package Manager website at http://www.rpm.org and the UNIX man pages for RPM.

Instead of a regular installation, you can use the RPM packages eTrust AC provides. This lets you manage your eTrust AC installation with all your other software installations performed using RPM.

eTrust AC RPM Packages

eTrust AC includes four RPM packages (each package is built separately). These packages let you install, query, verify, update, and uninstall eTrust AC components. The RPM packages are located in the NativePackages/RPMPackages folder of the eTrust AC UNIX native packages CD (CD #3).

Note: The packages are stored in subdirectories (one for each supported platform), and the actual file name for each package depends on the OS you are deploying on.

The following are the packages and their descriptions:

ca-lic

Installs the CA license program which is a prerequisite for all other packages.

ca-cs-cawin

Installs the CAWIN shared component which must be installed before installing any eTrust AC package.

CAeAC

Installs the core eTrust AC components. This is the main eTrust AC installation package and combines the server, client, documentation, TNG integration, API, and mfsd packages which are traditionally packaged separately.

CAeACgui

Adds the eTrust AC administration GUI component.

Note: You need to know the name of the package to perform some rpm commands (such as removing a package). To determine the name of a package using the package file, enter the following command:

```
rpm -q -p RPMPackage_filename
```

Remove Existing eTrust AC RPM Packages from the RPM Database

If you have already installed an eTrust AC RPM package that you created by yourself, you have to remove it from the RPM database so that the database reflects which packages you have installed. If you do not remove the existing package and install the new package, the RPM database will show that both the old package and the new one are installed while on your file system, files from the newer package overwrite existing files. For RPM to upgrade a package, it has to have the same name as the currently installed package.

Note: Removing the package does not remove any eTrust AC files and the program upgrades as specified.

To remove the package from the RPM database, use the following command:

```
rpm -e --justdb your_eTrustACPackageName
```

Install eTrust AC RPM Packages

To manage the eTrust AC installation with all your other software installations, install the eTrust AC RPM Packages. The actual rpm command you need to use varies depending on many variables (for example, whether you are upgrading or installing for the first time, or whether you want to install to the default directory or not). Some command examples are available below.

You can find the RPM packages for each of the supported Linux operating systems in the NativePackages/RPMPackages directory of the eTrust AC UNIX native packages CD (CD #3).

Note: The following procedure installs eTrust AC with the default settings. Alternatively, you may want to customize the eTrust AC package before installing it (see page 112).

To install eTrust AC RPM packages

1. Use the rpm command to install the *ca-lic* package.

   The license program installs.

   Note: For more information about the prerequisite package version, see the *readme* file.

2. Use the rpm command to install the *ca-cs-cawin* RPM package.

   CAWIN installs.

   Note: If you installed the license program to a custom directory, you need to specify the same custom directory for the CAWIN package. For more information about the prerequisite package version, see the *readme* file.

3. Use the rpm command to install the *CAeAC* package.

   eTrust AC installs.

   Important! If you are upgrading an existing eTrust AC package, you must unload SEOS syscall before you try to install the new package. Otherwise, the installation will not succeed.

4. (Optional) Install the *CAeACgui* package.

   eTrust AC administration GUI installs.

Example: Install eTrust AC on a new computer

The following example shows how you can install the default eTrust AC package that you can find on the eTrust AC UNIX native packages CD (mounted to /mnt/AC_CD3) on a Red Hat Linux x86 ES 3.0 computer where there is no CA software installed. To do this, you install the license program package, CAWIN package, and eTrust AC package (in that order) using the following commands:

```
cd /mnt/AC_CD3/NativePackages/RPMPackages/LINUX
```

```
rpm -i ca-lic-01.0063-0000.i386.rpm ca-cs-cawin-11.0.6.0.i386.rpm \
CAeAC-800sp1-601.i386.rpm
```

Example: Install eTrust AC and the prerequisite packages to a custom directory

The following example shows how you can install the default eTrust AC and the prerequisite packages that you can find on the eTrust AC UNIX native packages CD (mounted to /mnt/AC_CD3) to custom directories on a Red Hat Linux Itanium IA64 ES 4.0. To do this, use the following commands:

```
cd /mnt/AC_CD3/NativePackages/RPMPackages/LINUX_IA64
rpm -i --prefix /opt/CA/shared ca-lic-01.0063-0000.ia64.rpm
rpm -i --prefix /opt/CA/shared ca-cs-cawin-11.0.6.0.ia64.rpm
rpm -i --prefix /opt/CA/AC CAeAC-800sp1-601.ia64.rpm
```

Note: You must install the license program and CAWIN to the same custom directory.

Example: Upgrade the eTrust AC package

The following example shows how you can install the default eTrust AC that you can find on the eTrust AC UNIX native packages CD (mounted to /mnt/AC_CD3) on top of a currently installed eTrust AC RPM package on a Red Hat Linux Itanium IA64 ES 4.0 without removing the package first. The example assumes that the prerequisite versions of the license program and CAWIN are already installed and that the currently installed package is of the same name. To do this, use the following commands:

```
cd /mnt/AC_CD3/NativePackages/RPMPackages/LINUX_IA64
rpm -i --force CAeAC-800sp1-601.ia64.rpm
```

Customize the eTrust AC RPM Packages

If you want to install eTrust AC with custom settings using RPM Packages, you need to customize the package before you install it. You customize the package by extracting the installation parameters file from the package, modifying it as required, and then loading it back into the package.

Note: Follow the steps in the following procedure to customize any of the eTrust AC RPM packages. We recommend that you do not modify the packages manually. Instead, use the customize_eac_rpm script as described.

To customize the eTrust AC packages

1. Copy the package you want to customize from the /NativePackages/RPMPackages/*OS* directory of the native packages CD (CD #3) to a temporary location on your file system.

   where *OS* is the appropriate subdirectory name of your operating system.

   In the read/write location on the file system, the package can be customized as required.

2. (Optional) Enter the following command to set the language of the installation parameters file:

   ```
   customize_eac_rpm -r -l lang [-d pkg_location] pkg_filename
   ```

   where *lang* is the language you want for the installation parameters file, *pkg_location* is the directory where you placed your package on the file system, and *pkg_filename* is the file name of the package.

   Note: For a list of supported languages you can specify, run customize_eac_rpm -h. By default, the installation parameters file is in English.

3. (Optional) Enter the following command to change the installation directory:

   ```
   customize_eac_rpm -i install_loc [-d pkg_location] pkg_filename
   ```

   where *install_loc* is the location where you want eTrust AC installed.

4. Enter the following command to get the installation parameters file:

   ```
   customize_eac_rpm -g -f tmp_params [-d pkg_location] pkg_filename
   ```

   where *tmp_params* is the full path and name for the extracted installation parameters file.

5. Edit the installation parameters file to suit your installation requirements.

   This file lets you set the installation defaults for the package. For example, activate the POSTEXIT token (remove the preceding # character) and point it to post-installation script file you want to run.

6. Enter the following command to set the installation parameters in your customized package:

```
customize_eac_rpm -s -f tmp_params [-d pkg_location] pkg_filename
```

You can now use the package to install eTrust AC with the customized defaults.

customize_eac_rpm Command—Customize RPM Package

The customize_eac_rpm command runs the eTrust AC RPM package customization script.

Remarks

- The script works on any of the available eTrust AC RPM packages.

  Note: The script is not intended for use with the CAWIN and license program packages.

- To customize a package, the package must be in a read/write directory on your file system.

This command has the following format:

```
customize_eac_rpm -r [-d pkg_location] [-l lang] pkg_filename
customize_eac_rpm -i install_loc [-d pkg_location] pkg_filename
customize_eac_rpm -s -f tmp_params [-d pkg_location] pkg_filename
customize_eac_rpm -g [-f tmp_params] [-d pkg_location] pkg_filename
```

pkg_filename

The file name of the eTrust AC package you want to customize.

Note: If you do not specify the -d option, you must define the full pathname of the package file.

-d *pkg_location*

(Optional). Specifies the directory where you placed your package on the file system. If you do not specify a directory where the package is located, the script assumes the full pathname to the package file is *pkg_filename*.

-f *tmp_params*

(Optional). Specifies the full path and name of the installation parameters file to create or retrieve information from.

Note: If you do not specify a file when using the -g flag, the installation parameters are directed to the standard output (stdout).

-g

Gets the installation parameters file and places it in the file specified by the -f flag.

-h

Displays command usage and what languages the installation parameters file is available in when used to follow the -l option.

Note: You can find the list of languages eTrust AC itself supports in the comment for the LANGUAGE token in the installation parameters file. Set the installation language using this token.

-i *install_loc*

Sets the installation directory for the package to *install_loc*.

-l *lang*

Sets the language of the installation parameters file to *lang*. You can only specify the -l flag when using the -r flag.

Note: For a list of supported languages you can specify, run *customize_eac_rpm -l -h*. By default, the installation parameters file is in English.

-r

Resets the package to use default values as in the original package.

-s

Sets the specified package to use inputs from the customized installation parameters file specified by the -f flag.

Uninstall eTrust AC RPM Packages

To uninstall an eTrust AC RPM package installation, you need to uninstall the eTrust AC packages in the reverse order of their installation.

To uninstall eTrust AC packages

1. Uninstall the last eTrust RPM package you installed.

   For example, if you installed the GUI package, uninstall this first.

   ```
   rpm -e guiPackage_name
   ```

2. Uninstall the main eTrust AC package.

   ```
   rpm -e CAeACPackage_name
   ```

3. Uninstall the CAWIN package.

   ```
   rpm -e ca-cs-cawinPackage_name
   ```

Install eTrust AC Using Solaris Native Packaging

Solaris native packaging is provided as command-line utilities that let you create, install, remove, and report on individual software packages.

Note: For more information about Solaris native packaging, see the Sun Microsystems website and the man pages for pkgadd, pkgrm, pkginfo, and pkgchk.

Instead of a regular installation (see page 95), you can use the Solaris native packages eTrust AC provides. This lets you manage your eTrust AC installation with all your other software installations performed using Solaris native packaging. The eTrust AC packages are particularly suited for installing eTrust AC on all zones across your Solaris 10 system.

Important! To uninstall eTrust AC after a package installation, you must use the *pkgrm* command. Do not use uninstall_eTrustAC script.

eTrust AC Solaris Native Packages

eTrust AC includes two Solaris native packages (each package is built separately). These packages let you install, and remove eTrust AC components. The following are the packages and their descriptions:

CAeAC

Installs the core eTrust AC components. This is the main eTrust AC installation package and combines the server, client, documentation, TNG integration, API, and mfsd packages which are traditionally packaged separately.

CAeACgui

Adds the administration GUI component.

Install eTrust AC Solaris Native Packages

The eTrust AC Solaris native packages let you install eTrust AC on Solaris easily.

Note: The following procedure installs eTrust AC with the default settings. Alternatively, you may want to customize the eTrust AC package (see page 117) before installing it.

To install the eTrust AC Solaris native packages

1. Run the following command:

   ```
   pkgadd -d <pkg_location> CAeAC
   ```

   where <*pkg_location*> is the directory where the eTrust AC package (CAeAC) is located.

   Note: You can find the Solaris native packages in the NativePackages/_SOLARIS directory of the eTrust AC UNIX native packages CD.

2. (Optional) Install the GUI package:

   ```
   pkgadd -d <pkg_location> CAeACgui
   ```

   eTrust AC is now fully installed but not started.

Customize the eTrust AC Solaris Native Packages

If you want to install eTrust AC with custom settings using Solaris native packaging, you need to customize the package before you install it. You customize the script by extracting the installation parameters file from the package, modifying it as required, and then loading it back into the package.

Note: Follow the steps in the following procedure to customize any of the eTrust AC Solaris packages. We recommend that you do not modify the packages manually. Instead, use the customize_eac_pkg script as described.

To customize the eTrust AC packages

1. Copy the package you want to customize from the /NativePackages/_SOLARIS directory of the Solaris native packages CD (CD #3) to a temporary location on your file system.

   You need to copy the package's directory and its entire content. In the read/write location on the file system, the package can be customized as required.

   Important! When you copy the package, you must make sure that file attributes for the entire directory structure of the package are preserved or Solaris native packaging tools will consider the package corrupt. We recommend that you use a recursive cp command with the -p switch to preserve file attributes. For example, to copy the eTrust AC package from the CD to the current directory use:
   cp –Rp /<*cd_drive*>/NativePackages/_SOLARIS/CAeAC .

2. (Optional) Copy the customize_eac_pkg script file and the pre.tar file to a temporary location on your file system.

   You only need to have pre.tar file in the same directory as the script file if you want script messages in a language other than English. The pre.tar file is compressed tar file containing installation messages and the eTrust AC license agreement.

   Note: You can find the customize_eac_pkg script and the pre.tar files on the eTrust AC CD in the same location where the Solaris native packages are. The pre.tar file can also be found in the /Unix/Access-Control directory on CD #1.

3. (Optional) Enter the following command to set the language of the installation parameters file:

   ```
   customize_eac_pkg -r -l <lang> -d <pkg_location> <pkg_name>
   ```

   where <*lang*> is the language you want for the installation parameters file, <*pkg_location*> is the directory where you placed your package on the file system, and <*pkg_name*> is the name of the package.

   Note: For a list of supported languages you can specify, run *customize_eac_pkg -h*. By default, the installation parameters file is in English.

4. (Optional) Enter the following command to change the installation directory:

   ```
   customize_eac_pkg -i <install_loc> [-d <pkg_location>] [<pkg_name>]
   ```

   where <*install_loc*> is the location where you want eTrust AC installed.

5. Enter the following command to get the installation parameters file:

   ```
   customize_eac_pkg -g -f <tmp_params> -d <pkg_location> <pkg_name>
   ```

   where <*tmp_params*> is the full path and name for the extracted installation parameters file.

6. Edit the installation parameters file to suit your installation requirements.

   This file lets you set the installation defaults for the package. For example, activate the POSTEXIT token (remove the preceding # character) and point it to post-installation script file you want to run.

7. Enter the following command to set the installation parameters in your customized package:

   ```
   customize_eac_pkg -s -f <tmp_params> -d <pkg_location> <pkg_name>
   ```

   You can now use the package to install eTrust AC with the customized defaults.

customize_eac_pkg Command—Customize Solaris Native Package

The customize_eac_pkg command runs the eTrust AC Solaris native package customization script.

Remarks

- The script works on any of the available eTrust AC Solaris native packages (see page 115).
- To customize a package (see page 117), the package must be in a read/write directory on your file system.

  Important! When you copy the package, you must make sure that file attributes for the entire directory structure of the package are preserved or Solaris native packaging tools will consider the package corrupt.
- For localized script messages, you need to have pre.tar file in the same directory as the script file.

```
customize_eac_pkg -r [-d <pkg_location>] [-l lang] [<pkg_name>]
customize_eac_pkg -i <install_loc> [-d <pkg_location>] [<pkg_name>]
customize_eac_pkg -s -f <tmp_params> [-d <pkg_location>] [<pkg_name>]
customize_eac_pkg -g [-f <tmp_params>] [-d <pkg_location>] [<pkg_name>]
```

<pkg_name>

(Optional). The name of the eTrust AC package you want to customize. If you do not specify a package, the script defaults to the main eTrust AC package (CAeAC).

-d *<pkg_location>*

(Optional). Specifies the directory where you placed your package on the file system. If you do not specify a directory where the package is located, the script defaults to /var/spool/pkg.

-f *<tmp_params>*

(Optional). Specifies the full path and name of the installation parameters file to create or retrieve information from.

Note: If you do not specify a file when using the -g flag, the installation parameters are directed to the standard output (stdout).

-g

Gets the installation parameters file and places it in the file specified by the -f flag.

-h

Displays command usage and what languages the installation parameters file is available in.

Note: You can find the list of languages eTrust AC itself supports in the comment for the LANGUAGE token in the installation parameters file. Set the installation language using this token.

-i <*install_loc*>

Sets the installation directory for the package to <*install_loc*>.

-l <*lang*>

Sets the language of the installation parameters file to <*lang*>. You can only specify the -l flag when using the -r flag.

Note: For a list of supported languages you can specify, run *customize_eac_pkg -h*. By default, the installation parameters file is in English.

-r

Resets the package to use default values as in the original package.

-s

Sets the specified package to use inputs from the customized installation parameters file specified by the -f flag.

Starting eTrust AC

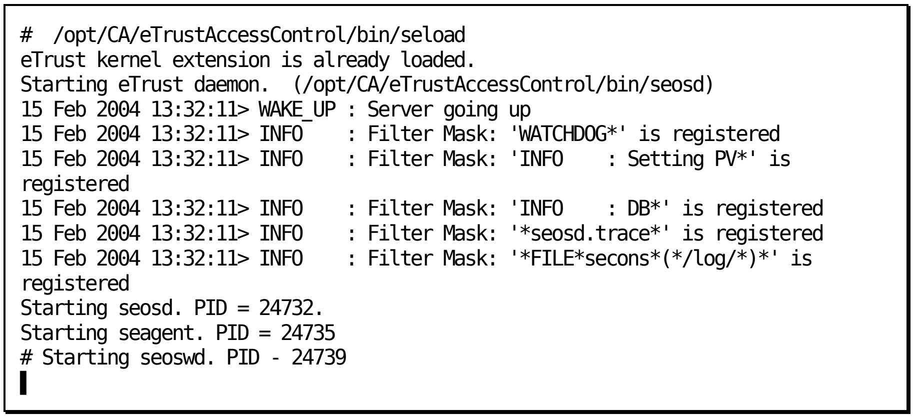
Assuming you are working in an X Windows environment, invoke eTrust AC, verify that it is correctly installed on your system, and perform the following steps to initiate important protection:

1. If you have not rebooted since installing eTrust AC, you may need to reboot now. See Step 10 in the Installation Procedure for specifics for your platform.
2. Open two windows under root (superuser) authority.
3. In either window, enter the command:

   ```
   # seload
   ```

   Wait while the seload command starts three eTrust AC daemons: the Database Server, the Agent, and the Watchdog.

   Wait for all the following messages to display.



```
#  /opt/CA/eTrustAccessControl/bin/seload
eTrust kernel extension is already loaded.
Starting eTrust daemon.  (/opt/CA/eTrustAccessControl/bin/seosd)
15 Feb 2004 13:32:11> WAKE_UP : Server going up
15 Feb 2004 13:32:11> INFO    : Filter Mask: 'WATCHDOG*' is registered
15 Feb 2004 13:32:11> INFO    : Filter Mask: 'INFO    : Setting PV*' is
registered
15 Feb 2004 13:32:11> INFO    : Filter Mask: 'INFO    : DB*' is registered
15 Feb 2004 13:32:11> INFO    : Filter Mask: '*seosd.trace*' is registered
15 Feb 2004 13:32:11> INFO    : Filter Mask: '*FILE*secons*(*/log/*)*' is
registered
Starting seosd. PID = 24732.
Starting seagent. PID = 24735
# Starting seoswd. PID - 24739
▌
```

4. After you have started the daemons, go to the other window and enter the command:

   ```
   # secons -t+ -tv
   ```

   eTrust AC accumulates a file of messages reporting operating system events. The secons -tv command displays the messages on the screen as well.

5. In the first window, where you gave the seload command, enter the following command:

   ```
   # who
   ```

   Watch the second window, where eTrust AC is writing the trace messages, to see whether eTrust AC intercepts the execution of the who command and reports on it. eTrust AC is correctly installed on your system if it reports interception of the who command.

6. If you want, enter more commands to see how eTrust AC reacts to them.

   The database does not yet contain any rules for blocking access attempts. Nevertheless, eTrust AC monitors the system so that you can see how the system behaves with eTrust AC installed and running, and which events eTrust AC intercepts.

7. Shut down the seosd daemon, by entering the following command:

   ```
   # secons -s
   ```

   The following message displays on the screen:

   ```
   seosd is now DOWN !.
   ```

Customizing eTrust AC

Implementing full-scale security using eTrust AC requires the definition of the security policies you want enforced. The time taken to make these definitions depends on the size of your site and the way you choose to manage security.

For instance, at a university you would probably not define most students to eTrust AC; they would get access based solely on resource _default settings. At a bank, however, you would probably define every user to eTrust AC and set access lists for every resource to allow specific users access to specific resources. Thus, for the same number of users, implementing eTrust AC at the university would take less time than implementing it at a bank.

As security administrator, you must define the objectives of the project. Decisions regarding site policy must be made carefully. eTrust AC includes several files that you can customize to help you implement the security policies of your site.

Registering Trusted Programs

A trusted program is a program that can be executed only as long as it has not been altered. Ordinarily it is a setuid/setgid program. eTrust AC also allows you to specify regular programs as trusted. When you are sure that the program has not been tampered with, register it in the PROGRAM class, where eTrust AC can guard its integrity.

You may want to use trusted programs together with *program pathing*, so users can perform certain tasks only by means of trusted programs. See the *Getting Started* for more information about program pathing.

eTrust AC can help you with a script to register a whole collection of setuid and setgid programs as trusted.

1. To save yourself the effort of remembering all your setuid and setgid programs, use the seuidpgm program that follows. It scans your file system, locates all setuid and setgid programs, and creates a script of selang commands that will register them all in the PROGRAM class.

   Issue this command:

   ```
   # seuidpgm -q -l -f / > /opt/CA/eTrustAccessControl/seuid.txt
   ```

   Run as shown, seuidpgm does the following:

   - Scans the entire file system (starting from /).
   - Remains quiet (the -q option suppresses the “cannot chdir” messages).
   - Ignores any symbolic links (-l).
   - Registers the programs in both the FILE and PROGRAM classes (-f).
   - Outputs the commands to file init2.

   For a complete description of the seuidpgm program, see the *Reference Guide*.

2. Using a text editor, check the seuid.txt file to be sure that it includes all the setgid/setuid programs that you want to have trusted, and no other programs. Edit the file if necessary.

3. Use selang to run the edited file of commands. If the seosd daemon is not running, include the -l switch.

   ```
   # selang [-l] -f /opt/CA/eTrustAccessControl/seuid.txt
   ```

   It may take a few minutes for selang to finish.

4. Restart the seosd daemon if it is not already running. Then check whether your system works as expected and whether setuid programs can be invoked.

5. It is advisable to change the default access of the PROGRAM class to NONE to prevent new untrusted setuid or setgid programs from being added and run without the knowledge of the security administrator.

   Enter the following command to set that default access value:

   ```
   chres PROGRAM _default defaccess(none)
   ```

Note: Veteran eTrust AC users will remember the UACC class in this connection. That class still exists and can be used to specify the default access of a resource. However, for ease of use we recommended that for specifying the default access of a class, you use the class's _default record instead. The _default specification overrides any UACC specification for the same class.

The records in the PROGRAM class representing the setuid, setgid, and regular programs that you have registered store the following attributes of the executable files.

- Device-number
- Inode
- Owner
- Group
- Size
- Creation Date
- Creation Time
- Last-Modification Date
- Last-Modification Time
- MD5 Signature
- SHA1 Signature
- Checksum CRC (Cyclical Redundancy Check)

The most important attribute of each program you register is that the program is *trusted*. That is, the program is considered OK to run. Any change in any of the attributes listed previously causes the program to lose its trusted status, and then eTrust AC can prevent the program from running.

Warning Mode

If you are not sure whether you have successfully registered all the appropriate programs in the database, use the following command to watch for unregistered programs:

```
chres PROGRAM _default warning
```

The warning property puts the PROGRAM class into Warning mode, meaning that a special audit record appears as a warning each time an unregistered setuid or setgid program is used but the use of such programs *is not prevented*.

Using the Audit Log

You can search for untrusted records manually in the audit log, or you can set special notification instructions to be informed when certain programs become untrusted. The special notification is especially helpful so that users do not have to contact you to use a program that has become untrusted; instead, you can check the file as soon as you receive a notification that it has become untrusted.

To set up special audit notifications, see File Notifications in the chapter “Auditing Events.”

Protection

To prevent execution of setuid and setgid commands that are not trusted, issue the following command:

Note: eTrust AC automatically includes the user “nobody” in the database.

```
newres PROGRAM _default defaccess(none) \
owner(nobody) audit(all)
```

eTrust AC then protects you against back doors and Trojan horses by requiring approval from you before allowing any new or changed program to run.

Now suppose, for example, that you have received a new, useful program that is a setuid program. You are sure it is not a Trojan horse, and you want all users to be able to execute it. To register the program as trusted, issue the following command:

```
newres PROGRAM program-pathname \ defaccess(EXEC)
```

Retrusting Untrusted Programs

If a program has been untrusted by eTrust AC because of a change in its size, its modification date, or any other monitored property, the program will run again only if you *retrust* it, registering a new approval for it in the database. To retrust a program:

```
editres PROGRAM progam_name trust
```

Note: You can also retrust a program with the seretrust utility. For more information about this utility and its options, see the *Utilities Guide*.

Initialization Files

This section describes various files that eTrust AC reads at initialization time. By default, eTrust AC places the initialization files in the directory containing the file seos.ini, which is the installation directory for eTrust AC.

seos.ini

The seos.ini file sets global parameters. The structure of the file and supported tokens are documented in the file itself and in the Administrator Guide appendix “The seos.ini Initialization File.”

The seos.ini file, as installed, is protected and cannot be updated while eTrust AC is running, though all users can always access it on a READ basis. Enter the following command in order to allow an authorized user to update the file while eTrust AC is running:

```
newres FILE eTrustACDir/seos.ini owner(authUser) defacc(read)
```

where *eTrustACDir* is the installation directory for eTrust AC, by default /opt/CA/eTrustAccessControl.

This command establishes that the default access for the file is READ; however, only the owner of the file, *authUser*, can update the file.

Note: It is important that the default access for the seos.ini file be READ because many utilities access seos.ini during their processing. If they cannot read the file, they will fail.

trace_file_type Token

The [seosd] section of the file contains a token named trace_file_type. The default value of the token is text, but you can assign it the value binary instead.

In previous versions of eTrust AC, the trace file-not the audit log, which is selective, but the file in which *all* events are recorded-was a text file. Now, by changing the value of the trace_file_type token, you can use a space-saving binary file instead, which still displays as text by the secons -tv utility.

If you do change the value of the token and a trace file already exists, the existing trace file is saved with the file name extension .backup and then a new trace file is started in the format you specified.

Other Tokens

The following additional tokens are of interest.

Section	Token	Description
seosd		
	trace_to	Determines where trace messages are sent. Valid values are: **file**; **none**; and **file,stop** (stop after initialization; this is the default).
	trace_file	If the trace_to token is set to file, the name of the file in which the trace messages are written.
	trace_filter	The name of the file containing the trace filter masks.
	under_NIS_server	Determines whether the files are on an NIS file server. Valid values are yes, no, and DNS.
logmgr	audit_log	The name of the audit log file.
	error_log	The name of the error log file.
	audit_size	The size, in KB, of the audit log file.
	error_size	The size, in KB, of the error log file.
message	filename	The name of the file containing the error messages.
seos	SEOSPATH	The home directory of eTrust AC. The default setting is /opt/CA/eTrustAccessControl.

Note: For more information about the seos.ini file, see the *Reference Guide*.

Trace Filter File

This optional file contains entries that specify filter masks for filtering out eTrust AC trace messages and trace messages that are sent to the audit file (for use with the "trace" audit mode).

The trace filter file specifies the trace messages that are to be filtered out (that is, those messages that are not to appear in the trace or audit file). Each line specifies a mask that identifies a group of messages to be suppressed. For example, the following file suppresses all messages that begin with WATCHDOG or INFO and all messages that end with BYPASS.

```
WATCHDOG*
*BYPASS
INFO*
```

By default, eTrust AC uses a trace filter file named trcfilter.init. Edit the file as required. To add remarks (comment lines) to the file, place a semicolon (;) at the beginning of the line.

Note: For more information, see the seosd utility in the *Utilities Guide*.

Advanced Policy Management and Reporting

Advanced policy management and reporting lets you deploy multiple-rule policies (script files) in a configured hierarchy. It complements the rule-based policy management enabled by the Policy Model service. Using this policy-based method, you can store, deploy, and remove (undeploy) deployed policy versions, and create reports on deployment status, deployment deviation, and deployment hierarchy.

Note: For more information about central policy management, see the *Administrator Guide*.

Configure Your Hierarchy for Advanced Policy Management and Reporting

If you are setting your PMDB hierarchy to use a Deployment Map Server (DMS) for advanced policy-based management, you need to install a DMS in a central location and then install a DMA on each computer with at least one PMDB. You then need to configure each end-point for policy deviation calculations (see page 129).

Note: Use the *-advreport* option of the install_base command (see page 97) to do this during the installation.

To configure your hierarchy for advanced policy management and reporting, use the dmsmgr utility.

Note: For more information about the dmsmgr utility, see the *Utilities Guide*.

Configure an End-Point for Policy Deviation Calculations

Each end-point must be configured to allow policy deviation calculation. Normally, you do this during the installation using the *-advreport* option of the install_base command (see page 97). This procedure is aimed at achieving this post-installation instead.

To configure an end-point for policy deviation calculations, enter the following selang command:

```
so dms+(<DMS@host>)
```

where *<DMS@host>* is the name of your DMS specified in that format.

sesu and sepass Utilities

We recommend that you use sepass instead of the operating system's passwd command and sesu instead of the su command. To do this, you need to save the original system binaries and replace them with symbolic links to sepass and sesu respectively. Once this is done, you need to make sure you can always use these utilities.

On most operating systems, the sepass and sesu utilities run even when eTrust AC is not loaded. However, on some operating systems (for example, AIX) these utilities do not work when eTrust AC is not loaded. For these operating systems, eTrust AC provides wrapper scripts.

sesu and sepass Wrapper Scripts

The sesu and sepass wrapper scripts are found in the following directory:

```
<eTrustAC_InstallDir>/samples/wrappers
```

This directory contains the following files:

File	Description
sesu_wrap.sh	Wrapper script for sesu
sepass_wrap.sh	Wrapper script for sepass
README	A text file with usage and conceptual information for these wrappers

Use the Wrapper Script to Run sesu

Using the wrapper scripts to run the sesu utility lets you run it on operating systems where it does not work when eTrust AC is not loaded.

Note: You only need to follow this procedure if the sesu utility does not run when eTrust AC is not loaded.

To use wrapper scripts to run sesu

1. Open the sesu_wrap.sh script in a text editor.

   The wrapper script displays in the text editor.

2. If necessary, change the following two variables:

   SEOSDIR

   Defines the eTrust AC installation directory. By default, this is set to the default installation directory:
   `/opt/CA/eTrustAccessControl`

   SYSSU

   Defines the name of the original su system binary that you need to replace. By default, this is set to:
   `/usr/bin/su.orig`

3. Replace the su symbolic link to point to the sesu_wrap.sh wrapper script rather than to the sesu utility.

   Whenever you run su, the sesu wrapper script runs the sesu utility.

Use the Wrapper Script to Run sepass

Using the wrapper scripts to run the sepass utility lets you run it on operating systems where it does not work when eTrust AC is not loaded.

Note: You only need to follow this procedure if the sepass utility does not run when eTrust AC is not loaded.

To use wrapper scripts to run sepass

1. Open the sepass_wrap.sh script in a text editor.

   The wrapper script displays in the text editor.

2. If necessary, change the following two variables:

   SEOSDIR

   Defines the eTrust AC installation directory. By default, this is set to the default installation directory:
   `/opt/CA/eTrustAccessControl`

   SYSPASSWD

   Defines the name of the original sepass system binary that you need to replace. By default, this is set to:
   `/usr/bin/passwd.orig`

3. Replace the passwd symbolic link to point to the sepass_wrap.sh wrapper script rather than to the sepass utility.

   Whenever you run passwd, the sepass wrapper script runs the sepass utility.

Maintenance Mode Protection (Silent Mode)

eTrust AC has a maintenance mode, also known as silent mode, for protection when the eTrust AC daemons are down for maintenance. In this mode, eTrust AC denies events while these daemons are down.

When eTrust AC is running, it intercepts security sensitive events and checks whether the event is allowed. Without activating maintenance mode, all events are permitted when eTrust AC services are down. With active maintenance mode, events are denied when eTrust AC daemons are down, stopping user activity while the system is maintained.

Maintenance mode can be tuned, and it is disabled by default.

When the eTrust AC security services are down:

- If maintenance mode is active, all security sensitive events are denied, except for special cases and for events executed by the maintenance user.
- If maintenance mode is disabled, eTrust AC does not intervene and execution is passed to the operating system.

When maintenance mode is activated and security is down, the prevented events are not logged in the audit log file.

In order to enable maintenance mode, follow these steps:

Important! If root is not the maintenance user, make sure you have an open session for the maintenance user as you will not be able to log in otherwise.

1. Make sure the eTrust AC daemons are down.
2. Using seini utility, change the token silent_deny value to *yes*.

   The token is located under SEOS_syscall section.

   ```
   seini -s SEOS_syscall.silent_deny yes
   ```

3. Change the token silent_admin value to the numeric UNIX UID that you want to let access the computer while eTrust AC daemons are down.

   ```
   seini -s SEOS_syscall.silent_admin <maintenance_UID>
   ```

   Note: *root* is the default maintenance mode user (UID 0).

   Important! If the maintenance user is not *root*, you must make the eTrust AC authorization daemon setuid to the root user so that you can start eTrust AC in maintenance mode. To make this change enter the following command:
   chmod 6111 seosd

4. Start eTrust AC daemons with seload command.

   Note: If the maintenance mode user is not root, start eTrust AC daemons with seosd command.

Installing Unicenter Security Integration Tools

Use one of two types of Unicenter Security integration installations for UNIX environments.

Full Integration

The full integration installation is useful for eTrust AC installations with Unicenter Security in use. The integration imports data from Unicenter Security to eTrust AC, so eTrust AC becomes the security system used on that host or group of hosts.

Minimal Integration

The minimal integration installation is useful for eTrust AC installations without Unicenter Security or for installations that include Unicenter Security, but it is not in use.

To Install eTrust AC with Full Integration of Unicenter Security

Important! To run the migration, you must log on as root; you cannot run the su (substitute user) command to change to root after you install eTrust AC.

For **full** integration of Unicenter Security and eTrust AC, do the following:

1. Install eTrust AC without populating the eTrust AC database.

   To avoid populating the database, accept the default of No when the following prompt appears on the screen:

   ```
   Import users, groups and hosts now? [y/N] :
   ```

2. Run the uni_migrate_master.sh script on the master node.

   Note: The master node is the machine that hosts the Unicenter Security database.

3. Run the uni_migrate_node.sh script on each satellite node (that is, every Unicenter Security-controlled machine).

4. Run the uni_migrate_node.sh script on the master node.

   The master node is the last machine to disable Unicenter Security after all the other nodes have been integrated.

5. Manually edit the $CAIGLBL0000/secopts file to set the value for the SSF_SCOPE_DATA and SSF_SCOPE_KEYWORD keywords to **NO**.

The installation scripts perform the following tasks:

- Execute a shell script, defclass.sh, to define user-defined security asset types as eTrust AC classes in the eTrust AC database.
- Run a program, migopts, to read and translate the current Unicenter Security environment to a similar eTrust AC environment.
- Run a program, exporttngdb, to read and translate current Unicenter Security database objects to eTrust AC database objects.
- Stop and disable the Unicenter Security daemons.

For **minimal** integration of Unicenter Security and eTrust AC, complete the following steps:

1. Run the uni_migrate_node.sh script on all nodes.
2. Manually edit the $CAIGLBL0000/secopts file to set the value for the SSF_SCOPE_DATA and SSF_SCOPE_KEYWORD keywords to **NO**.

Installation Notes

- We do not recommend running Unicenter TNG login intercepts after running the Unicenter Integration and Migration Installation. When the Unicenter Integration and Migration Installation has completed successfully, Unicenter TNG login intercepts are disabled.
- Unicenter TNG Data Scoping and Keyword Scoping rules (rules that target Unicenter TNG asset types with a -DT or -KW suffix) are not supported by the eTrust AC Migration process. Rules of this type are ignored during the migration process.
- Unicenter Security rules that have been implemented against any of the following Unicenter Security asset types are obsolete because Unicenter Security is no longer in use: CA-USER, CA-ACCESS, CA-USERGROUP, CA-ASSETGROUP, CA-ASSETTYPE, and CA-UPSNODE. Rules that target any of these asset types, or any of their derivatives, are ignored during the migration process.

  The -e (-edit) flag available for uni_migrate_node.sh and uni_migrate_master.sh allows you to see and edit the rule entering the eTrust AC database.
- If you want full or minimal Unicenter TNG integration, then you must install the Unicenter Integration and Migration package with the -uni option to the install_base script. The Unicenter Integration and Migration Installation installs the Unicenter Integration and Migration scripts and binary files in the *eTrustACDir*/tng directory.
- Do not use selang -c during migration if you are listing more than one command. Instead, use selang -f input_file_name.

Implementing eTrust AC on Solaris 10 Zones

Solaris 10 provides virtualized OS services which look like different Solaris instances, called *zones*. All Solaris 10 systems contain a master zone, called the *global zone*. Non-global zones run alongside it, and you can configure, monitor, and control them from the global zone.

You can protect each zone (or selected zones) in your environment using eTrust AC. This lets you define different rules and policies for each zone, and therefore defining different access restrictions for each zone.

Installing eTrust AC on Solaris 10 zones is no different to a regular installation, and you can do it by either one of the following methods:

- Install eTrust AC on all zones using Solaris native packaging (see page 115).

  eTrust AC is designed to be installed and uninstalled using Solaris native packaging tools (pkgadd and pkgrm).

  If you install using the Solaris native package installation, you cannot install eTrust AC on selected zones. You can either install on the global zone, *or* on *all* zones, including non-active zones and any zones that are created in the future.

  If you installed using Solaris native packaging, use the native packaging to uninstall eTrust AC from all zones.

- Install eTrust AC in each zone using the install_base script (see page 95).

  The install_base script installs eTrust AC in the zone you are executing the script in.

  For eTrust AC to work in any non-global zone, you must also install eTrust AC in the global zone.

  If you installed eTrust AC using the install_base script, you can uninstall it from individual non-global zones. However, the eTrust AC kernel can be uninstalled only from the global zone *and* only after eTrust AC has been stopped in all zones.

  Important! If you uninstall eTrust AC from the global zone using install_base before you uninstall from all zones, users may be locked out of the zones. We recommend you use Solaris native packaging to install and uninstall eTrust AC on Solaris zones.

Zone Protection

eTrust AC protects Solaris 10 zones in the same way it protects any computer. Each zone is protected in isolation from any other zones, with each rule you define in eTrust AC applying only to users working in that zone. Rules you apply in the global zone, even those that cover resources that are visible in a non-global zone, only apply to users who access them from the global zone.

Note: Make sure you protect non-global zone resources in both the non-global and the global zone as necessary.

Example: Global zone rules and non-global zone rules

In the following example, we define rules to protect a non-global zone (myZone1) file. All system files are always visible from the global zone.

The file we want to protect is /myZone1/root/bin/kill (path from global zone). To protect this file, we define the following eTrust AC rules:

- In the global zone:

  ```
  nu admin_pers owner(nobody)
  nr FILE /myZone1/root/bin/kill defaccess(none) owner(nobody)
  authorize FILE /myZone1/root/bin/kill uid(admin_pers) access(all)
  ```

- In myZone1 (the non-global zone):

  ```
  nu admin_pers owner(nobody)
  nr FILE /bin/kill defaccess(none) owner(nobody)
  authorize FILE /bin/kill uid(admin_pers) access(all)
  ```

Using these rules in both the global and non-global zones, we defined a user (admin_pers), defined our file as resource to be protected, and authorized our user to access the file. Without doing this in both zones, we would leave the resource exposed.

Starting and Stopping eTrust AC in a Zone

Starting and stopping eTrust AC in Solaris 10 zones is generally done in the same way you would normally start and stop eTrust AC on any Solaris computer.

The following exceptions apply to starting eTrust AC in zones:

- You can load the eTrust AC kernel module (SEOS_load) from the global zone only.
- You must load the eTrust AC kernel module in the global zone before you can start eTrust AC in any non-global zone.

  Once the eTrust AC kernel module is loaded in the global zone, you can then start and stop eTrust AC in any non-global zone and in any order.

The following exceptions apply to stopping eTrust AC in zones:

- You cannot unload the eTrust AC kernel module when one or more zones has maintenance mode (see page 132) enabled.
- You can stop eTrust AC in all zones in any order by issuing the *secons -s* command in each zone.
- You should stop the last zone with the *secons -sk* to disable event interception and prepare the eTrust AC kernel module for unloading.
- You can unload the eTrust AC kernel module (SEOS_load -u) from the global zone only.

  Note: The SEOS_load -u command ensures that eTrust AC is not running on any non-global zone before unloading it.

Start eTrust AC in A Non-global Zone

You can start eTrust AC from any non-global zone just as you would normally, but you must first load the eTrust AC kernel module in the global zone.

To start eTrust AC in a non-global zone

1. In the global zone, enter the SEOS_load command to load the eTrust AC kernel module.

   The eTrust AC kernel loads and you can now start eTrust AC in any zone.

   Note: The eTrust AC kernel loads but eTrust AC does not intercept events in the global zone.

2. In the non-global zone, enter the seload command to start eTrust AC in that zone.

   The non-global zone is protected by eTrust AC.

   Note: You can also start eTrust AC in the non-global zone remotely. For more information, see the seload command in the *Utilities Guide*.

zlogin Utility Protection

The zlogin utility lets an administrator enter a zone. You should add a LOGINAPPL resource for this utility to control who can log in to any non-global zone.

eTrust AC comes with a predefined LOGINAPPL resource for protecting the zlogin utility.

Complete the Installation on a New Zone

If you install eTrust AC using Solaris native packaging on all zones, eTrust AC also automatically installs on any zones you create after the original installation. However, while the post-installation eTrust AC procedure scripts need to run from within the non-global zone, for new zones, Solaris native packaging runs these scripts from the global zone. For these zones, you must complete the installation from within the new zone.

Important! You need to do this only for new zones that are created *after* eTrust AC was installed on all zones using Solaris native packaging.

1. Start and log in to the new zone.

2. Run the Solaris native packaging post-installation script (postinstall).

   The post-installation is <*eTrustAC_Dir*>/lbin/postinstall. For example, for a default installation directory, run:

   ```
   /opt/CA/eTrustAccessControl/lbin/postinstall
   ```

Starting eTrust AC Automatically

After you have tested eTrust AC and experimented with its features, you are ready to implement eTrust AC protection.

To arrange for the seosd daemon to start automatically upon boot, so that your resources are protected immediately, use the *eTrustACDir*/samples/system.init/*sub-dir* directory, where *sub-dir* is the directory for your operating system. Each sub-directory contains a README file with instructions for performing this task on the respective operating system.

Chapter 5: Installing and Customizing eTrust AC for Windows

This section contains the following topics:

About eTrust AC for Windows Installations

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

Note: For more information about installation considerations, known issues, and supported operating systems, see the *readme* file.

Installation Methods

eTrust AC for Windows can be installed by one of three methods:

Graphical installation

The graphical installation program leads you through the various steps required for installing eTrust AC. Use this method to familiarize yourself with the installation options.

Command line

The command line interface to the installation program lets you:

- Set custom defaults for running the graphical installation program

  You can pass defaults to the graphical installation program from the command line. Use this method to create a batch file that opens the installation program with the preset defaults you want to use, but lets you customize options for each installation.

– Perform a silent installation

  You can silently install eTrust AC, rather than just pass defaults to the graphical installation program, using the command line. Use this method to push the installation to remote computers.

Unicenter Software Delivery

You can create a package for distributing eTrust AC with Unicenter Software Delivery.

Custom Installations

The interactive installation program lets you select between two installation types. The default installation type, called *Typical*, lets you easily configure the installation to include the most commonly used features and functionality. If you want to install and configure other features that are not included in a Typical installation, you need to select a *Custom* installation.

You should perform a custom installation on any Windows computer on which you want to do one or more of the following:

- Integrate eTrust AC and Unicenter Security components.
- Install mainframe password synchronization.
- Install the eTrust AC SDK samples.
- Enable the STOP feature.
- Enable Task Delegation.
- Create PMDBs to propagate access rules to other PMDBs or to eTrust AC databases on other computers.
- Configure advanced policy management on eTrust AC end-points.
- Install a Deployment Map Server (DMS).
- Install a Deployment Map Agent (DMA).
- Import users and groups from Windows.

Upgrades and Reinstallations

When upgrading eTrust AC, note the following:

- Read the readme file.

  You can find the readme file (README.HTML) in the Doc\language directory of the eTrust AC for Windows CD.

  The readme file contains information about supported platforms, installation considerations, general considerations, known issues, and other important information you should read before installing eTrust AC.

- To upgrade, you must have eTrust AC version 5.1, or later, installed.

  To upgrade from an earlier version (for example eTrust AC r4.1), upgrade to an intermediate version first (for example eTrust AC r8) and then to eTrust AC r8 SP1.

- We recommend that you perform a scaled-down internal testing of the new release before you upgrade your production environment.

- You must reboot the computer when you upgrade eTrust AC for the installation to complete.

  Future patches may not require a reboot.

- If your environment is set up with a PMDB hierarchy or you are setting such an environment, we recommend that you:

  – Install or upgrade the Deployment Map Server (DMS) computer first.

    This is only required if you are going to use advanced policy-based management, and ensures that the DMS registers each Policy Model node and its subscribers.

  – Install or upgrade each computer in your hierarchy bottom-up (subscribers first).

    Upgraded PMDBs having subscribers with an earlier version may result in erroneous commands being sent. This can happen as a result of new PMDBs containing classes and properties that do not exist in the earlier version PMDBs.

    Note: A PMDB hierarchy running on a single computer can be upgraded simultaneously.

  – Do *not* upgrade during PMDB or policy updates.

  – Back up subscriber and PMDB policies.

  – Choose to install a Deployment Map Agent (DMA) on each computer with at least one PMDB if you are going to use advanced policy-based management.

Note: Earlier PMDB versions are permitted to have later versions of subscribers, but not vice versa. As commands in earlier versions are supported in later versions, earlier PMDBs can propagate to eTrust AC r8 SP1 subscribers.

- You must use the same encryption key that was used before the upgrade.
- The installation program automatically saves and upgrades registry settings of your previous installation. If an earlier version's registry key was relocated, the upgrade process copies your previous settings to the new location (for example, in r5.2 the STOP settings are located under the FsiDrv registry key and in r8 SP1 the settings appear under the STOP registry key).

  In eTrust AC r8 SP1, registry settings are stored in the following location:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrustAccessControl
  ```

- If you already have a version of eTrust AC installed on the computer, you must decide whether you want to continue using the data in your current database or whether you want to delete it and create a new, empty database.

  In order to continue with the installation you must select to reuse your data; eTrust AC will transfer all data into the new database.If you want to create a new, empty database, first uninstall eTrust AC to delete the existing database, and then install eTrust AC again.

  Important! If you choose to delete your current database, you lose all eTrust AC data: users, groups, and resources that you have defined in the database, as well as the access rules that protect the resources.

Policy Model Installations

If your environment is set up with a PMDB hierarchy or you are setting such an environment, we *recommend* that you:

- Install or upgrade the Deployment Map Server (DMS) computer first.

  This is only required if you are going to use advanced policy-based management, and ensures that the DMS registers each Policy Model node and its subscribers.

- Install or upgrade computers in your hierarchy bottom-up (subscribers first).

  If upgraded PMDBs have subscribers with an earlier version, erroneous commands may be sent. This is because new PMDBs may contain classes and properties that do not exist in the earlier version PMDBs.

- Install a Deployment Map Agent (DMA) on each computer with at least one PMDB.

  This is only required if you are going to use advanced policy-based management.

The Product Explorer

The eTrust AC Product Explorer lets you browse through the eTrust AC features you can install from the product CD. Using the Product Explorer, you can select which component of eTrust AC you want to install on this computer, learn a little about these features, and initiate their installation. You can also view system requirements for installation components, or open the readme file and the documentation for viewing.

Note: If you have Autorun enabled, the Product Explorer automatically displays when you insert the eTrust AC CD into your CD-ROM drive.

Unicenter Integration

When you integrate eTrust AC and Unicenter Security components, consider the following:

- Once you run the Unicenter Integration and Migration Installation process successfully, you should verify that Unicenter TNG login intercepts are disabled.

  We do not recommend running Unicenter TNG login intercepts after running the Unicenter Integration and Migration Installation process.

- Unicenter TNG Data Scoping rules (rules that target Unicenter TNG asset types with a -DT suffix) are ignored during the migration process.

  These rules are not supported by the eTrust AC Migration process.

- Unicenter Security rules that have been implemented against any of the following Unicenter Security asset types are obsolete because Unicenter Security is no longer used: CA-USER, CA-ACCESS, CA-USERGROUP, CA-ASSETGROUP, CA-ASSETTYPE, and CA-UPSNODE.

  Rules that target any of these asset types, or any of their derivatives, are ignored during the migration process.

- If you upgrade Unicenter TNG or apply Unicenter TNG fixes after running the Unicenter Integration process, then you must ensure sure that the CAUSECR.DLL under the %CAIGLBL000%\BIN directory has not been replaced and is the same as the CAUSECR.DLL.EAC file in the eTrust AC installation path bin directory.

- If eTrust AC is uninstalled, the CA_ROUTER_CAUSECU Unicenter Security option is reset to one, the SETLOCAL CAIACTSECSV Unicenter Security option is reset to yes, and CAUSECR.DLL file in the %CAIGLBL000%\BIN directory is replaced by the Unicenter default. You may need to customize these options after the uninstall process.

Installing eTrust AC for Windows

Depending on the installation method (see page 142) you choose, you need to follow the appropriate instructions for that method.

The easiest way to install eTrust AC is to use the Product Explorer. The Product Explorer lets you browse through the eTrust AC features you can install from the product CD and then select the features you want to install.

Install eTrust AC Using the Graphical Installation Program

To view the installation options and choose which ones meet your needs, you can use the graphical installation program to install eTrust AC. This lets you learn the installation options as you install eTrust AC.

To install eTrust AC using the graphical installation program

1. Log on to the Windows system as a user with Windows administrative privileges (that is, as the Windows administrator or a member of the Windows Administrators group.)
2. Close any applications that are running on your Windows system.
3. Insert the eTrust AC distribution CD in your CD-ROM drive.

   If you have Autorun enabled, the Product Explorer automatically appears. Otherwise, navigate to the CD-ROM drive and double-click the ProductExplorerx86.EXE file.
4. From the Product Explorer main menu, expand the Components folder, select eTrust Access Control for Windows, and click Install.

   The Choose Setup Language window appears.
5. Select the language you want to install eTrust AC with and click OK.

   The eTrust AC installation program starts loading and after a short while the Introduction screen appears.

   Note: If the installation program detects an existing installation of eTrust AC, you are prompted to select whether to keep your current eTrust AC database. If you want to keep it, click *Yes* to continue with the installation. If you want to replace the database with a new one, click *No* to exit the installation, uninstall eTrust AC, and install eTrust AC again.
6. Follow the instructions on the installation screens.

   Depending on the choices you make, you may need to provide answers in various installation screens (see page 149).

   The installation program installs eTrust AC. Be sure to view the readme file to find out the latest information that is not included in the documentation. When the installation is complete, you are given the choice of restarting Windows now or later.
7. Select Yes, I want to restart my computer now, and then click OK.

   After your system reboots, you can check that eTrust AC was installed properly (see page 164).

   Note: If you choose to restart your computer later, an additional warning cautions you that the installation is not complete until your computer is rebooted.

Installation Program Screens

The eTrust AC installation program prompts you for the information required to install the features and functionality you select. Depending on the choices you make, the following screens may appear during the installation process:

License Agreement

Lets you select whether you accept the terms of the License Agreement for using eTrust AC.

Note: You need to scroll all the way down to make a selection.

Important! You cannot continue with the installation if you select not to accept the terms of the License Agreement.

Customer Information

Lets you enter information that identifies you and the computer you are installing on, and who you want this product installation to be available for.

Installation Type

Lets you select the installation type that suits your requirements. You can choose a Typical or Custom installation (see page 143).

Note: Further installation screens, and the order which they appear in, are determined by the type of installation you choose.

Select Features

(Custom installation only) Lets you define the location where you want eTrust AC installed and the eTrust AC features you want to install on this computer. The following features are available:

Task Delegation

Lets you grant ordinary users the necessary privileges (sub-administration rights) to perform administrative tasks.

Policy Model

Sets up the Policy Model service and lets you create a PMDB and configure its parents and subscribers.

SDK

Creates a subdirectory called SDK under the eTrust AC installation directory. In addition to the libraries and files required for using the eTrust AC SDK, this directory also contains API samples.

Mainframe Password Synchronization

Lets you synchronize user passwords with your MainFrame computers.

Unicenter Integration

Lets you integrate Unicenter NSM with eTrust AC and migrate Unicenter NSM data.

eTrust AC sends audit data to the host specified by the configuration parameters of Unicenter TNG or a host you select. To integrate, specify that audit data should be sent to Unicenter TNG and then select the host to which eTrust AC should send the audit data. If you want to integrate users and access permissions with Unicenter TNG calendars, specify how often you want to retrieve updates from the Unicenter Calendar host server (by default, every 10 minutes).

Unicenter Migration

Lets you specify whether you want to migrate Unicenter Security data.

If you do not select this option, the Unicenter Security to eTrust AC migration is not performed and user names in eTrust AC appear fully qualified (as DOMAINNAME\USERNAME). With migration, user names are not qualified (as USERNAME).

Stack Overflow Protection (STOP)

Enables the eTrust AC stack overflow protection feature.

Advanced Policy Management

Configures the policy deviation calculator to send policy deviations to a central database. You can also select to install:

- **Deployment Map Server (DMS)**

  A central database that records all the information required for centrally managing policies and creating reports.

- **Deployment Map Agent (DMA)**

  A component required on each Policy Model computer.

Note: For more information on advanced policy management and reporting, see the *Administrator Guide*.

Note: Mainframe Password Synchronization and Unicenter Integration are not available unless you have Unicenter NSM or CA Common Services installed on your computer. For more information about compatible Unicenter NSM versions, see the *Readme*.

Destination Location

Lets you define the location where you want eTrust AC installed.

Administrator and Host Information

Lets you define information for administering the eTrust AC instance you are installing:

eTrust AC administrators

Users with administrative access to the eTrust AC database.

eTrust AC administration hosts

Computers from which administrators can administer the eTrust AC database you are installing.

Allow logon without domain name

Lets users log on to the eTrust AC database without specifying a domain name. Keep the default (not allowed) for stronger security.

DNS Information

Lets you enter the domain names of your networks for eTrust AC to add to host names. You must enter at least one domain name.

Import option

(Custom installation only) Lets you import Windows users and groups into the database. If you select Yes, select one or more of the following options:

- **Import Users** - import your Windows users to the database.
- **Import Groups** - import your Windows groups to the database.
- **Connect Users to Their Default Groups** - automatically add the imported users to the appropriate imported groups in the database.
- **Change Owner of Imported Data** - define someone other than you as an owner of the imported data.

  Note: By default, the owner of these records is set to the administrator doing the installation (you).

Note: If you choose not to import Windows data during installation, you can import it later using the ntimport utility or the NT import wizard in Policy Manager.

Unicenter Integration

(Custom installation only) If you selected Unicenter Integration, select whether to integrate eTrust AC with Unicenter TNG. Integration means:

- eTrust AC sends audit data to the host specified by the configuration parameters of Unicenter TNG or a host you select. To integrate, you specify that audit data should be sent to Unicenter TNG and then select the host to which eTrust AC should send the audit data.
- eTrust AC supports integration of Users and Access permissions with Unicenter TNG calendars. Configure eTrust AC to retrieve updates from the Unicenter TNG calendar host server more or less frequently than the default of 10 minutes.

If you have Unicenter Security data that you want to migrate to eTrust AC, select *Migrate Unicenter Security data*.

Encryption Settings

Lets you set the eTrust AC encryption method and the encryption key.

Hierarchy Context (Local computer settings)

Lets you define the position of the database in the hierarchy. You do this by defining one or more parent PMDBs to which this database subscribes to, and the parent password Policy Model from which password changes are propagated.

Leave this screen blank if you are not including this database in a PMDB hierarchy. You can also specify *_NO_MASTER_* as a parent PMDB to indicate that the local database accepts updates from any PMDB.

Note: You still need to define this database as a subscriber to the parent PMDB.

Hierarchy Context (Policy Model settings)

(Custom installation only) Lets you define the name of a PMDB to create, and its position in the hierarchy. You do this by defining one or subscriber databases to which this PMDB propagates changes to.

Note: You still need to define this PMDB as a parent on each of the subscriber databases.

Deployment Map Server (DMS)

(Custom installation only) Lets you configure the current computer as a DMS. You need to provide the DMS name, its administrative users and the computers from which it can be administered.

Advanced Policy Management and Reporting

(Custom installation only) Lets you define one or more DMS databases to send notifications to.

Note: For more information on advanced policy management and reporting, see the *Administrator Guide*.

Command Line Installations

You can use the command line to:

- Pass defaults to the graphical installation program.
- Silently install eTrust AC.

Set Custom Defaults for the Installation Program

To set the eTrust AC installation program with the defaults you want to use for your company, you can use the command line. The graphical installation program accepts input from the command line that determines which options are preselected.

To set custom defaults for the installation program

1. Log on to the Windows system as a user with Windows administrative privileges (that is, as the Windows administrator or a member of the Windows Administrators group.)
2. Close any applications that are running on your Windows system.
3. Insert the eTrust AC distribution CD in your CD-ROM drive.

   The eTrust AC Product Explorer appears.
4. Close the Product Explorer if it appears.
5. Open a command line and navigate to the following directory on the CD drive:

   ```
   \x86
   ```
6. Enter the following command:

   ```
   setup [/s] /v"<insert_params_here>"
   ```

   where <*insert_params_here*> specifies the installation settings you want to pass to the installation program.

   The installation program appears, and based on the options you chose to pass, lets you install eTrust AC using the graphical installation program (see page 148).

Install eTrust AC Using a Silent Installation

To install eTrust AC without interactive feedback, you can install eTrust AC silently using the command line.

To install eTrust AC using a silent installation

1. Log on to the Windows system as a user with Windows administrative privileges (that is, as the Windows administrator or a member of the Windows Administrators group.)
2. Open a command line and navigate to the following folder on the eTrust AC CD.

   ```
   \x86
   ```
3. Enter the following command:

   ```
   setup /s /v"/qn COMMAND=<keyword> <insert_params_here>"
   ```

   where <*insert_params_here*> specifies the installation settings (see page 155) you want to pass to the installation program.

   Note: To execute a silent installation you have to accept the license agreement. The keyword required for accepting the license agreement and silently installing eTrust AC can be found at the bottom of the license agreement available when running the installation wizard.

Uninstall eTrust AC Using a Silent Installation

To uninstall eTrust AC without interactive feedback, you can uninstall eTrust AC silently using the command line.

To uninstall eTrust AC using a silent installation

1. Log on to the Windows system as a user with Windows administrative privileges (that is, as the Windows administrator or a member of the Windows Administrators group.)
2. Open a command line and navigate to the following folder on the eTrust AC CD.

   ```
   \x86
   ```
3. Enter the following command:

   ```
   setup /s /x /v"/qn <insert_params_here>"
   ```

   where <*insert_params_here*> specifies the installation settings (see page 155) you want to pass to the installation program.

   Note: To execute a silent installation you have to accept the license agreement. The keyword required for accepting the license agreement and silently installing eTrust AC can be found at the bottom of the license agreement available when running the installation wizard.

setup Command—Install eTrust AC for Windows

Use the setup command to install eTrust AC for Windows with preset custom defaults (see page 153) or when performing a silent installation (see page 154).

```
setup [/s] [/L] [/v"<insert_params_here>"]
```

/s

Hides the setup initialization dialog.

/x

Specifies that the installation program perform an uninstall.

/L

Defines the eTrust AC installation language. The following are the supported language IDs you can specify and their respective languages:

- 1033 - English
- 1041 - Japanese
- 1042 - Korean
- 2052 - Chinese (simplified)

/v "<insert_params_here>"

Defines the parameters to pass to the installation program.

Note: All parameters should be placed within the quotes ("").

The following parameters are passed to the installation program through the /v parameter:

/L[*<mask>*] *<log_file>*

Defines the full path and name of the installation log file. Use the mask *v to log all available information.

/qn

Specifies a silent installation, in conjunction with the */s* parameter.

Note: You need to use the <*license_accept*> property to execute a silent installation.

COMMAND=*<keyword>*

Defines the command required for accepting the license agreement and silently installing the eTrust AC. The actual keyword you need to use can be found at the bottom of the license agreement that is available when running the graphical installation program.

INSTALLDIR="<*location*>"

Defines the location where eTrust AC will be installed. By default, this is:

`<Local_Drive>\Program Files\CA\eTrustAccessControl`

SETUP_TYPE={"Typical" | "Custom"}

Defines the installation type (Typical by default).

ADMIN_USERS_LIST="<*users*>"

Defines a space-separated list of users with administrative access to the eTrust AC database.

HOSTS_LIST="<*hosts*>"

Defines a space-separated list of computers from which administrators can administer the eTrust AC database.

DOMAIN_LIST="<*domains*>"

Defines a space-separated list of your networks' domain names for eTrust AC to add to host names.

ENABLE_STOP={Y | N}

Specifies whether the stack overflow protection feature is enabled (disabled by default).

ENCRYPTION_METHOD={"Default" | "DES" | "3DES" | "256bit AES" | "192bit AES" | "128bit AES"}

Specifies the encryption method to use for communications.

LOGON_WITHOUT_DOMAIN={Y | N}

Specifies whether users can log on to the eTrust AC database without specifying a domain name.

CREATE_PMDB={Y | N}

Specifies whether a Policy Model should be created. If you specify this option and set it to Y, you also need to specify:

– **PMDB_NAME="**<*name*>**"**

  Defines the name of the PMDB.

– **PMDB_SUBSCRIBERS_LIST="**<*subs*>**"**

  Defines a space-separated list of subscriber databases to which the PMDB specified with the CREATE_PMDB option propagates changes to.

DMS_NAME="<*name*>"

Defines the current computer as a DMS and sets the name of the DMS database. If you specify this option, you also need to specify:

- DMS_ADMIN_LIST="<*users*>"

  Defines a space-separated list of users with administrative access to the DMS.

- DMS_HOSTS_LIST="<*hosts*>"

  Defines a space-separated list of computers from which administrators can administer the DMS.

- DMS_NODES_LIST="<*hosts*>"

  Defines a space-separated list of one or more DMS databases to send notifications to.

Note: For more information on advanced policy management and reporting and the DMS, see the *Administrator Guide*.

IMPORT_NT={Y | N}

Specifies whether to import Windows users and groups into the database. If you select Y, specify one or more of the following options:

- **IMPORT_USERS={1 | 0}**

  Specifies whether to import Windows users to the database.

- **IMPORT_GROUPS={1 | 0}**

  Specifies whether to import Windows groups to the database.

- **IMPORT_CONNECT_USERS={1 | 0}**

  Specifies whether to automatically add the imported users to the appropriate imported groups in the database.

- **IMPORT_CHANGE_OWNER={1 | 0}**
  NEW_OWNER_NAME=<*name*>

  Specifies someone other than you as an owner of the imported data.

Note: By default, all of these options are not specified (equivalent to a value of 0).

Example: Use the setup command to set installation defaults

The following example sets the installation directory, specifies a Custom installation, and defines installation log file defaults for the eTrust AC installation, then opens the graphical installation program.

```
setup.exe /s /v"INSTALLDIR="C:\CA\eAC" SETUP_TYPE="Custom" /L*v
%SystemRoot%\eACInstall.log"
```

To Install eTrust AC from Unicenter Software Delivery

To install eTrust AC from Unicenter Software Delivery, follow these steps:

Note: The eTrust AC installation CD contains a directory named reginfo. This directory contains several files needed to install eTrust AC using Unicenter Software Delivery.

1. To export the eTrust AC Unicenter Software Delivery package, insert the eTrust AC installation CD into your drive.
2. Launch the Unicenter Software Delivery explorer.
3. Register the Unicenter Software Delivery package for eTrust AC by choosing the root directory of the eTrust AC installation.
4. Unseal the eTrust AC package.
5. In the procedures for Start Services, Stop Services, Uninstall, and Upgrade replace the parameters <admin> and <password> with the credentials of the eTrust AC ADMIN user.

   Note: These credentials are used to shut down eTrust AC during these processes. The user you enter should be able to log on to client computers with these credentials.
6. Seal the package.

Managing Access Control Services

By default, all eTrust AC services start automatically. You can change any service from automatic to manual or you can disable the service. Use Policy Manager or the Windows Control Panel.

From Policy Manager:

1. From the Windows program bar, select Server Manager.
2. Select Service from the tree.
3. Select the SeOS service you want to change or disable and double-click it.
4. Make the changes you want in the View or Set Service Information window and click OK.

From the Windows Control Panel:

1. Shut down eTrust AC. (See Starting and Stopping eTrust AC.)
2. Choose Start, Settings, Control Panel, and double-click the Services icon.
3. Select the service you want to change or disable, and click Startup.
4. In the Services window, select Automatic, Manual**,** or Disable to indicate how you want the service to start and click OK.

Maintenance Mode Protection (Silent Mode)

eTrust AC has a maintenance mode, also known as silent mode, for protection when the eTrust AC services are down for maintenance. In this mode, eTrust AC denies events while these services are down.

When eTrust AC is running, it intercepts security sensitive events and checks whether the event is allowed. Without activating maintenance mode, all events are permitted when eTrust AC services are down. With active maintenance mode, events are denied when eTrust AC services are down, stopping user activity while the system is maintained.

Maintenance mode can be tuned, and it is disabled by default.

When the eTrust AC security services are down:

- If maintenance mode is active, all security sensitive events are denied, except for special cases and for events executed by the maintenance user.
- If maintenance mode is disabled, eTrust AC does not intervene and execution is passed to the operating system.

When maintenance mode is activated and security is down, the prevented events are not logged in the audit log file.

In order to enable maintenance mode, follow these steps:

1. Make sure the eTrust AC services are down.
2. Using a registry editor, navigate to registry key

   ```
   \HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrustAccessControl\FsiDrv
   ```

   and change the following values:

   - SilentModeEnabled = 1
   - SilentModeAdmins = a list of user names that are allowed to access the computer while eTrust AC services are down.

     Use a new line for each user. Whether specified or not, *SYSTEM* is always a maintenance mode user.

     Note: On Windows 2000 and Windows NT you cannot use regedit to edit the SilentModeAdmins key; use Regedt32.exe instead.
3. Start eTrust AC services with “seosd -start” command from the command shell, or using an option from Windows Start menu.

Now, if eTrust AC services are down, only users that are listed under SilentModeAdmins registry key will have access to the computer, and all other users will receive a deny to any attempt of activity.

Stack Overflow Protection

Stack Overflow Protection (STOP) is a feature that prevents hackers from creating and exploiting stack overflow to break into systems. Stack overflow enables hackers to execute arbitrary commands on remote or local systems, many times as the administrator. They do this by exploiting bugs in the operating system or other programs. These special types of bugs permit users to overwrite the program stack, changing the next command to be executed.

STOP works by intercepting crucial operating system calls to each application on the computer. Each call is then given an initial analysis before being sent for further analysis if it is seems suspicious. Further analysis is performed using data from the STOP configuration and signature files.

Enable STOP

STOP lets you prevent hackers from creating and exploiting stack overflow to break into your systems. You can enable STOP when installing eTrust AC by using a Custom installation. Alternatively, you can enable STOP manually.

To enable STOP

1. Enter the following command:

   ```
   secons -s
   ```

   eTrust AC shuts down.

2. Set the *STOPOperationMode* registry entry to 1.

   The registry entry can be found in the following key:

   ```
   HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\STOP
   ```

   When eTrust AC is started, STOP modules will load and STOP will be enabled on the computer.

3. (Optional) Adjust STOP configuration using registry entries in the following key:

   ```
   HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\STOP
   ```

   Note: For more information about STOP registry settings, see the *Reference Guide*.

4. the following command:

   ```
   seosd -start
   ```

   eTrust AC starts up.

Configure STOP for Receiving Signature File Updates

You can make sure that all computers in your environment have the latest STOP information required for preventing stack overflow. You can do this by updating the STOP signature file on a central computer and setting up your computers to regularly retrieve the file.

To configure STOP for receiving signature file updates

1. Enter the following command:

   ```
   secons -s
   ```

   eTrust AC shuts down.

2. Set the *STOPSignatureBrokerName* registry entry to the host name the computer you want to eTrust AC to retrieve the signature file from.

   The registry entry can be found in the following key:

   ```
   HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\STOP
   ```

   When eTrust AC is started (and then at a defined interval), it retrieves the STOP signature file from the specified computer.

   Note: If you leave this registry entry empty but you have a parent Policy Model (parent_pmd registry entry) defined, the signature file will be retrieved from that parent Policy Model.

3. Set the *STOPUpdateInterval* registry entry to the interval at which you want the signature file updated.

   eTrust AC retrieves the signature file from the specified computer at the specified interval.

4. (Optional) Adjust STOP configuration using registry entries in the following key:

   ```
   HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\STOP
   ```

   Note: For more information about STOP registry settings, see the *Reference Guide*.

5. the following command:

   ```
   seosd -start
   ```

   eTrust AC starts up.

Note: You can retrieve the signature file from any host using the eACSigUpdate utility. For more information about this utility, see the *Reference Guide*.

Starting and Stopping eTrust AC

eTrust AC is started whenever you start Windows **if** the startup of the eTrust AC services is automatic.

Stopping eTrust AC

The eTrust AC utilities let you start or stop eTrust AC from the taskbar Start button.

To stop eTrust AC:

1. Choose Start, Programs, CA, eTrust Access Control.
2. Choose Stop eTrust AC. Click OK.

You can also stop eTrust AC from the command prompt:

1. Be sure you are logged in to the Windows system as a user with Windows administrative privileges (that is, as the Windows administrator or a member of the Windows Administrators group).
2. Choose Start, Programs, Accessories, Command Prompt.
3. In the Command Prompt window, change to the directory containing the eTrust AC binaries (by default, \Program Files\CA\eTrustAccessControl\ bin on your system directory).
4. Stop eTrust AC on the local machine by entering:

   ```
   secons -s
   ```

   Stop eTrust AC on one or more remote machines by entering:

   ```
   secons -s stationNames
   ```

   where *stationNames* is a list of names of the remote computers separated by spaces.

When eTrust AC stops on the local machine, the following message appears:

```
seosd is now DOWN
```

When you stop eTrust AC on remote machines, eTrust AC reports whether the remote machine shutdown was successful. An attempt is made to shut down each machine on the list, even if the remote machine preceding it was not shut down successfully.

Starting eTrust AC Manually

Typically, you start eTrust AC by starting Windows.

If you stopped eTrust AC, you can also restart it manually by issuing selang commands from the command prompt or with the Start utility from the taskbar Start button.

To start eTrust AC manually:

1. Choose Start, Programs, CA, eTrust Access Control.
2. Choose Start eTrust AC. Click OK.

   A window appears showing you the progress of the utility. If eTrust AC does not start successfully or is only partly successful, use the Stop utility to shut down eTrust AC, and then restart.

To start eTrust AC using selang:

1. Be sure you are logged in to the Windows system as a user with Windows administrative privileges (that is, as the Windows administrator or a member of the Windows Administrators group).
2. Choose Start, Programs, Command Prompt.
3. In the Command Prompt window, change to the directory containing the eTrust AC binaries (by default, \Program Files\CA\eTrustAccessControl\ bin on your system directory).
4. Start eTrust AC by entering:

   ```
   seosd -start
   ```

Checking Your Installation

If you have installed eTrust AC successfully, you will notice the following changes:

- A new key is added to the Windows registry:

  `HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl`

  These keys are protected so that they can be changed only when eTrust AC is running and by using the selang commands newres or chres or Policy Manager. (For more information about selang commands, see the chapter “The selang Command Language” in the *Reference Guide*; for more information about Policy Manager, see chapter “Using the Administrator Interface” in the *Administrator Guide*.)

- When you restart your computer, several new eTrust AC services start automatically. These services include the Watchdog, Engine, Agent, and TD. If you installed a PMDB, the Policy Model service is also running. You can verify that these services are running by choosing Start, Settings, Control Panel, Administrative Tools, Services.

Displaying Login Protection Screen

By default, after you install eTrust AC, every time a user logs in interactively (GINA) and eTrust AC services are running, a protection screen appears, telling the user that this computer is protected by eTrust AC.

The splash screen displays for four seconds and closes automatically:

To disable this protection message, you must change the HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrustAccessControl\eTrustAccessControl\SplashEnable registry key value from 1 to 0.

Uninstalling eTrust AC

To remove eTrust AC from your computer:

Be sure you are logged in to the Windows system as a user with Windows administrative privileges (that is, as the Windows administrator or a member of the Windows Administrators group). You must also be defined in the database as an administrator (that is, with the ADMIN attribute).

1. Shut down eTrust AC. See Starting and Stopping eTrust AC.
2. Choose Start, Settings, Control Panel.
3. Double-click Add/Remove Programs.
4. Select eTrust AC from the installed programs list and click Add/Remove.
5. In the message box confirming that you want to remove eTrust AC, click Yes.
6. When uninstall is complete, click OK.
7. Reboot the computer to remove all eTrust AC components.

Customizing eTrust AC for Cluster Environments

To use eTrust AC in a cluster environment, you must install eTrust AC on each node of the cluster. Define the same set of rules (quorum disk or network if you use network interception) for common resources on each node as well.

eTrust AC can detect that it is running in a cluster environment. If eTrust AC detects that the cluster has its own network with separate network adapters used for cluster internal communications only, network interception is disabled for these network adapters. For network interfaces that connect the cluster to the rest of the enterprise, network interception works as usual.

Note: This feature is not enabled if the cluster uses the same network interface for cluster internal communications **and** communication to the rest of the network.

Example

Suppose you have two nodes:

- NODE1 that has two IP addresses:
- 10.0.0.1 is an internal cluster network IP address.
  - 192.168.0.1 is an outside network connection.
- NODE2 has also two IP addresses
  - 10.0.0.2 is an internal cluster network IP address.
  - 192.168.0.2 is an outside network connection.

  The cluster itself has an additional IP address of 192.168.0.3.

Network interception does not prevent NODE1 from connecting to NODE2 and vice versa as long as they do their communications using the internal cluster network IP addresses.

Network interception acts as defined by eTrust AC rules if NODE1 or NODE2 are contacted using outside network IP addresses.

In addition, network interception acts as defined by eTrust AC rules if the cluster is contacted at its 192.168.0.3 IP address.

Chapter 6: Installing the Policy Manager

This chapter explains how to install the Policy Manager.

Policy Manager is a graphical user interface that lets you manage eTrust AC and Policy Model databases. It is usually installed on an administrator's workstation with TCP/IP communication to the database.

It lets 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 eTrust AC for UNIX and eTrust AC for Windows databases.

The Policy Manager is an administrative tool and is designed for administrators of the eTrust AC 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.

This section contains the following topics:

About Policy Manager Installations

This section designed to guide you through what you need to know before you install 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

Note: For more information about installation considerations, known issues, and supported operating systems, see the *readme* file.

Installation Location

Policy Manager needs to be installed on the workstation of every eTrust AC administrator. The computer running Policy Manager must have administrative (TERMINAL) access to the eTrust AC database. You can assign Policy Manager terminals with administrative access to the computer during the eTrust AC installation or, after installation using the Policy Manager.

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

Installation Methods

Policy Manager can be installed by one of two methods:

Graphical installation

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

Command line

The command line interface to the installation program lets you:

- Set custom defaults for running the graphical installation program

  You can pass defaults to the graphical installation program from the command line. Use this method to create a batch file that opens the installation program with the preset defaults you want to use, but lets you customize options for each installation.

– Perform a silent installation

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

Installing Policy Manager

Depending on the installation method you choose, you need to follow the appropriate instructions for that method.

The easiest way to install Policy Manager is to use the Product Explorer. The Product Explorer lets you easily access the Policy Manager installation and lets you browse through other eTrust AC features you can install from the product CD.

Install Policy Manager Using the Graphical Installation Program

To view the installation options and choose which ones meet your needs, you can use the graphical installation program to install Policy Manager. This lets you learn the installation options as you install Policy Manager.

To install Policy Manager using the graphical installation program

1. Log on to the Windows system as a user with Windows administrative privileges (that is, as the Windows administrator or a member of the Windows Administrators group.)
2. Close any applications that are running on your Windows system.
3. Insert the eTrust AC distribution CD in your CD-ROM drive.

   If you have Autorun enabled, the Product Explorer automatically appears. Otherwise, navigate to the CD-ROM drive and double-click the ProductExplorerx86.EXE file.
4. From the Product Explorer main menu, expand the Components folder, select eTrust Policy Manager, and click Install.

   The Choose Setup Language window appears.
5. Select the language you want to install Policy Manager with and click OK.

   The Policy Manager installation program starts loading and after a short while the Introduction screen appears.
6. Follow the instructions on the installation screens.

   Depending on the choices you make, you may need to provide answers in various installation screens.

   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 AC is selected.

   Encryption Method

   Specifies the type of encryption used to encrypt Policy Manager communication.

   Destination Folder

   Specifies where you want to install the Policy Manager files.

   The installation program installs Policy Manager. Be sure to view the readme file to find out the latest information that is not included in the documentation.

Command Line Installations

You can use the command line to:

- Pass defaults to the graphical installation program.
- Silently install or uninstall Policy Manager.

Set Custom Defaults for the Installation Program

To set the Policy Manager installation program with the defaults you want to use for your company, you can use the command line. The graphical installation program accepts input from the command line that determines which options are preselected.

To set custom defaults for the installation program

1. Log on to the Windows system as a user with Windows administrative privileges (that is, as the Windows administrator or a member of the Windows Administrators group.)
2. Insert the eTrust AC distribution CD in your CD-ROM drive.

   The eTrust AC Product Explorer appears.
3. Close the Product Explorer if it appears.
4. Open a command line and navigate to the following directory on the CD drive:

   ```
   \x86\PolicyManager
   ```
5. Enter the following command:

   setup /s /v"<*insert_params_here*>"

   where <*insert_params_here*> specifies the installation settings (see page 172) you want to pass to the installation program.

   The installation program appears, and based on the options you chose to pass, lets you install Policy Manager using the graphical installation program.

Install Policy Manager Using a Silent Installation

To install Policy Manager without interactive feedback, you can install Policy Manager silently using the command line.

To install Policy Manager using a silent installation

1. Log on to the Windows system as a user with Windows administrative privileges (that is, as the Windows administrator or a member of the Windows Administrators group.)
2. Open a command line and navigate to the following folder on the eTrust AC CD.

   ```
   \x86\PolicyManager
   ```

3. Enter the following command:

   ```
   setup /s /v"/qn COMMAND=<keyword> <insert_params_here>"
   ```

   where <*insert_params_here*> specifies the installation settings (see page 172) you want to pass to the installation program.

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

Uninstall Policy Manager Using a Silent Installation

To uninstall Policy Manager without interactive feedback, you can uninstall Policy Manager silently using the command line.

To uninstall Policy Manager using a silent install

1. Log on to the Windows system as a user with Windows administrative privileges (that is, as the Windows administrator or a member of the Windows Administrators group.)
2. Open a command line and navigate to the following folder on the eTrust AC CD.

   ```
   \x86\PolicyManager
   ```

3. Enter the following command:

   ```
   setup /s /x /v"/qn COMMAND=<keyword> <insert_params_here>"
   ```

   where <*insert_params_here*> specifies the installation settings (see page 172) you want to pass to the installation program.

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

setup Command—Install Policy Manager

Use the setup command to install Policy Manager with preset custom defaults or when performing a silent installation.

```
setup [/s] [/L] [/v"<insert_params_here>"]
```

/s

Hides the setup initialization dialog.

/x

Specifies that the installation program perform an uninstall.

/L

Defines the Policy Manager installation language.

/v "*<insert_params_here>*"

Defines the parameters to pass to the installation program.

Note: All parameters should be placed within the quotes ("").

The following parameters are passed to the installation program through the /v parameter:

/L[*<mask>*] *<log_file>*

Defines the full path and name of the installation log file. Use the mask *v to log all available information.

/qn

Specifies a silent installation, in conjunction with the */s* parameter.

Note: You need to use the *<license_accept>* property to execute a silent installation.

COMMAND=*<keyword>*

Defines the command required for accepting the license agreement and silently installing the Policy Manager. The actual keyword you need to use can be found at the bottom of the license agreement that is available when running the graphical installation program.

INSTALLDIR=*<location>*

Specifies the location where Policy Manager will be installed.

ENCRYPTION_METHOD={aes128enc.dll | aes192enc.dll | aes256enc.dll | defenc.dll | desenc.dll | tripledesenc.dll}

Specifies the encryption method to use for communications, where aes128enc.dll, aes192enc.dll, and aes256enc.dll are the AES 128-bit, 192-bit, and 256-bit methods respectively, defenc.dll is the Default method, desenc.dll is the DES method, and tripledesenc.dll is the 3DES method.

Example: Use the setup command to set installation defaults

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

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

Verify a Successful Installation of Policy Manager

You can verify that the installation of Policy Manager was successful.

To verify that the installation of Policy Manager has been successful

1. Select Start, Programs, CA, eTrust Access Control, Policy Manager.

   The Policy Manager opens and logs you in to the local database using your WIndows credentials.

   Note: If no local database is available, you need to provide your credentials and the eTrust AC database you want to connect to.

2. Perform a quick scan of your resources and users (Users, and Resources icons on the program bar) to verify that the basic functionality is accessible through the Policy Manager.

Index