

eTrust[®] Access Control for Windows

Getting Started

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.

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

Copyright © 2006 CA. All rights reserved.

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 1: Introducing All-Around Security for eBusiness 9

Purpose of This Guide	9
CA Technology Services: Delivering on the Vision of Enterprise IT Management	9
Education and Training: Maximizing the Business Value of CA Technology	10
eTrust Solutions	10
CA: The Software That Manages eBusiness	10
More Information	11
Is Your Open Distributed Network Environment Really Safe?	11
Windows and UNIX Superuser Privileges	11
Secure Your Environment	12
Prevent Host-based Intrusions	12
Protect Your Data and Applications	12
Manage User Accounts and Passwords	13
Secure Multiple Servers	13
Promote Consistent Cross-Platform Security	13
Distinctive Features	14
Active Directory Support	15
Policy Management System	16
Application Policy Generator	16

Chapter 2: Fortifying Operating System Security 17

Components, Features, and Installation Considerations	17
Components of eTrust AC	18
Features of eTrust AC	19
Managing eTrust AC Services	26
eTrust AC Documentation	27
What's Next	27

Chapter 3: Running the Administrator Interface 29

Implementing and Maintaining Your Security Policies	29
The Menu Bar and Toolbar	30
Program Bar	31
selang Commands	32
Setting Admin Defaults	33
Wizards	33
What's Next?	36

Chapter 4: Discovering the Power of Protection **37**

From Protecting Your Programs to Monitoring System Files	37
Creating Users and Groups	38
Protecting Files and Directories	40
File Groups	41
Protecting Programs	41
Monitoring Files	42
Protecting Processes from Being Killed	42
Program Patterns	43
Protecting Other Resources	44
Restricting Access with Predefined Groups	44
What's Next?	46

Chapter 5: Gaining More Control of Your User Accounts **47**

Limiting User Accesses and Privileges	47
Limiting the Use of Administrators	47
Restricting Access from Terminals	49
Limiting IMPERSONATION Requests	51
Setting Time-of-Day and Day-of-Week Rules	54
What's Next?	56

Chapter 6: Protecting Network Activity **57**

Controlling Network Level Accesses	57
Protecting the Network (TCP/IP)	57
Controlling Outgoing Connections	61
Service-Oriented TCP/IP Rules	62
What's Next?	63

Chapter 7: Setting Password and Audit Policies **65**

Passwords, Logins, and Auditing Rules	65
Setting Password Policies	66
Changing Passwords	67
Setting Audit Policies in the Native Environment	68
Cleaning Up	68
What's Next?	68

Chapter 8: Centralizing Administration **69**

Creating Users, Security Policies, and More	69
Creating a PMDB	69

Working with a PMDB	71
Transaction Manager-A Simpler Alternative	71
What's Next?	73
 Chapter 9: Integrating with Unicenter	 75
Integrating eTrust AC with Unicenter	75
Installing Unicenter Integration Tools	76
Installation Notes	77
What's Next?	77
 Chapter 10: Frequently Asked Questions	 79

Chapter 1: Introducing All-Around Security for eBusiness

This section contains the following topics:

[Purpose of This Guide](#) (see page 9)

[CA Technology Services: Delivering on the Vision of Enterprise IT Management](#) (see page 9)

[Education and Training: Maximizing the Business Value of CA Technology](#) (see page 10)

[eTrust Solutions](#) (see page 10)

[CA: The Software That Manages eBusiness](#) (see page 10)

[More Information](#) (see page 11)

[Is Your Open Distributed Network Environment Really Safe?](#) (see page 11)

Purpose of This Guide

This guide introduces you to eTrust AC. By the time you have finished reading this guide, you will have an overview of the wide scope of the product and its usability will be familiar to you. It is important to us that you feel comfortable with eTrust AC before you begin to use it.

CA Technology Services: Delivering on the Vision of Enterprise IT Management

CA Technology Services™ delivers enterprise IT management solutions to help our customers achieve more efficient operations and better manage the IT infrastructure, which drives meaningful business value and financial results. CA Technology Services leverages its global expertise and certified professionals in enterprise systems management, business service optimization, security management and storage management to maximize customers' IT investments.

We draw from our more than 27 years of management software experience, over 1,000 technology services professionals, most of whom are CISSP-, ITIL-, and SNIA-certified, and the complementary service delivery capabilities of industry-leading service partners, to offer you best practices and time-tested, proven methodologies.

Education and Training: Maximizing the Business Value of CA Technology

CA Technology Services education and training is focused on helping you realize streamlined implementations, reduced time-to-value, and improved productivity to maximize the business value of CA technology. We deliver instructor-led, self-paced, and extended learning solutions across CA's complete, integrated, and open solutions for enterprise IT management (EIM) and partner with leading value-added education providers to extend our course offerings in enterprise systems management, security management, storage management, and business service optimization. Our dynamic team of certified and experienced professionals transfers real-time expertise in optimizing CA software products and leveraging proven IT process models that educates your organization about how to make practical application of best practices in your IT environment.

For a complete list of education and training courses, visit <http://ca.com/education>.

eTrust Solutions

eTrust solutions enables eBusiness by delivering innovative technologies that make it easy for organizations to secure their environments. This comprehensive security suite enhances return opportunity for any eBusiness, with solutions that include risk assessment, attack detection, loss prevention and more. With eTrust, organizations have the flexibility to deploy a security solution as a standalone product, as a security suite, or fully-integrated with Unicenter NSM. Used with Unicenter NSM, eTrust solutions enable a consistent approach to building, deploying and managing security as part of the larger task of enterprise management.

CA: The Software That Manages eBusiness

The next generation of eBusiness promises unlimited opportunities by leveraging existing business infrastructures and adopting new technologies. At the same time, extremely complicated management presents challenges—from managing the computing devices to integrating and managing the applications, data, and business processes within and across organizational boundaries. Look to CA for the answers. CA has the solutions available to help eBusinesses address these important issues. Through industry-leading eBusiness Process Management, eBusiness Information Management, and eBusiness Infrastructure Management offerings, CA delivers the only comprehensive, state-of-the-art solutions, serving all stakeholders in this extended global economy.

More Information

After reading this Getting Started, you can refer to the numerous resources available to you for additional information. Your product CD contains instructional documents that showcase your software and provide detailed explanations about the product's comprehensive, feature-rich components.

For assistance, contact Technical Support at <http://ca.com/support>.

Is Your Open Distributed Network Environment Really Safe?

At most companies, critical information-such as financial transactions, customer information, and confidential personnel records-resides on distributed servers. Protecting and controlling access to this data is the key business requirement. Unfortunately, open system servers do not provide adequate data security. In fact, distributed servers are susceptible to unauthorized access due to "holes" in the underlying operating systems. Windows and UNIX operating systems are built around the *superuser* Administrator concept, which creates vulnerabilities through a single, privileged user account that has full access to applications, data, and audit logs.

Note: Unless specifically designated, the term "Windows" refers to any Microsoft Windows operating system supported by eTrust AC.

Windows and UNIX Superuser Privileges

One of the most serious problems in these systems is the single point of compromise through the system superuser or administrator. Administrator is a special privileged user who can perform any tasks and view or modify any files on the system. It is considered one of the greatest risks in these operating systems, because the account can terminate system services, remove critical files, access confidential information, and eliminate its audit trails. At the same time, superuser accounts are often given to other system administration operators for data backup, account creation and deletion, or password reset. Superuser is also the most targeted user account for hackers, because they know that once the account is compromised, they can virtually do anything that they want.

Secure Your Environment

With eTrust AC, companies can centrally manage user access privileges and quickly deploy pre-configured basic security policies. eTrust AC ensures that the right people have access to the right information. It proactively secures access to data and applications located on the Windows system servers throughout an organization.

eTrust AC provides reliable, non-intrusive protection through its Dynamic Security (DSX) technology. DSX dynamically intercepts security-sensitive requests in real time-without requiring any permanent changes to the operating system kernel. This provides a very high level of security without being intrusive to server processing. Advanced capabilities in eTrust AC-such as Generic File Protection-radically improve the security for Windows operating systems. With Generic File Protection, your organization can use wildcard options to protect groups of related files or programs. This capability makes it easy to develop powerful general access policies.

Prevent Host-based Intrusions

eTrust AC provides many key features for a Host-based Intrusion Prevention System (HIPS) which can reduce security risks of external worm attacks or malware damages. Through its Stack Overflow Protection (STOP) feature, Trojan Horse prevention function, pre-defined application security template samples, and the application behavior profiling program, eTrust AC offers administrators stronger protection of their critical servers, and more time to fix system vulnerabilities and distribute security patches.

Protect Your Data and Applications

Your organization's success depends on the integrity and privacy of its data and applications. With eTrust AC, people and programs have appropriate access to the information they need-and all unauthorized information requests are prevented and logged!

eTrust AC provides customized security policies for enhanced application security. CA is also partnering with leading software vendors, enabling eTrust AC to control access to specific applications. These "bullet-proof" solutions provide complete protection for business-critical applications.

Manage User Accounts and Passwords

As enterprises grow in the eBusiness market, managing users across different geographical or system domains and various departments causes a substantial amount of work for system administrators. Synchronization of user accounts, passwords, and security policies across various systems, or even platforms, can be a daunting task prone to error, complicated processes, increased reaction time, and cost.

Secure Multiple Servers

To solve the problem of securing multiple servers on a network, eTrust AC provides the Policy Model Database (PMDB) infrastructure. PMDB enables account, password, and security policy synchronization tasks to be executed securely and accurately to the subscribed hierarchical nodes. One critical design goal of eTrust AC is that security for a given server be enforced even if the network connectivity is not working properly. The result is that rules are decentralized and each server can exist securely on its own.

Promote Consistent Cross-Platform Security

With eTrust AC, the level of security on each system is raised to meet overall business requirements. A single eTrust AC security policy can be centrally created and automatically distributed and enforced on a variety of Windows and UNIX operating systems. The final result is a robust, consistent level of server security achieved with minimal time and effort.

Without eTrust AC, administrators must create and maintain a separate security policy for each computing system, and that requires an enormous amount of time and labor. In addition, company-wide security standards are often based on the system with the lowest level of security—an approach that fails to meet the security requirements of most organizations.

Policies can be created, managed, and distributed on an enterprise-wide basis, or customized to meet the security requirements of specific applications. This complete solution can be deployed in individual departments, such as accounting or development, the largest enterprises—and everything in between. Its hardened operating system security, complete auditing abilities, and cross-platform access control secures critical processes and sensitive information on the distributed systems.

Open and extensible, this powerful solution supports all industry-standard platforms, databases, and applications and includes published interfaces allowing it to secure any resource. eTrust AC can communicate with Unicenter TNG, providing a powerful, comprehensive solution for building, deploying and managing security as part of the larger task of enterprise management.

Distinctive Features

eTrust AC provides many features to manage your enterprise security:

Centralized Administration

eTrust AC lets you manage the administrator workstation and every other workstation on which eTrust AC is installed-from a single point.

Self-Protection

A self-defense mechanism prevents hackers or other users from bringing down eTrust AC services. This mechanism also safeguards eTrust AC files and audit data.

Profile Groups

eTrust AC lets you base security roles on group membership. For example, it can limit the rights granted to the Administrator's group and users who are members of that group.

Registry Protection

eTrust AC protects the registry to ensure that an unauthorized user does not change system parameters. Authorized users can update registry settings as necessary.

Process Protection

eTrust AC protects specified processes to make sure that they are not killed. eTrust AC process protection is also helpful for protecting Windows services and other non-interactive Windows applications.

Network Protection

eTrust AC controls access to network services and ports by regulating incoming and outgoing network connections.

SPECIALPGM Protection

eTrust AC protects specified programs, such as system services, that must typically be run as SYSTEM accounts so that only logical users can access them.

Logon Protection

eTrust AC lets you restrict user logons in several ways-from account expiration dates to day and time restrictions.

Program and File Signatures

eTrust AC protects programs and files by giving them signatures. If a signature has changed, the program or file becomes untrusted and cannot be accessed.

Task Delegation

eTrust AC lets you grant ordinary users the necessary rights and privileges so that these users can perform administrative tasks. This is called task delegation. The ability to delegate tasks-grant administrative privileges-in this granular way is one of the most significant advantages of eTrust AC.

Enhanced File Protection

eTrust AC protects all file systems currently used with Windows-Windows file system (NTFS) and file allocation tables (FAT). eTrust AC also supports CDFS and HPFS.

Stack Overflow Protection (STOP)

STOP prevents hackers from using stack overflow exploits, which can enable them to execute arbitrary commands in order to break into systems.

Cross-Platform Support

Administrators can create, implement, and maintain similar or identical security policies for Windows and UNIX machines.

Active Directory Support

Many organizations are moving to centralize their user data stores to Active Directory or LDAP based repositories. eTrust AC supports external users (users defined on external repositories) through eTrust Identity and Access Management. In other words, one can define users in an external directory and eTrust Identity and Access Management correlates these users to eTrust AC database. eTrust AC can also create, modify, or delete native users that reside in either the Active Directory or Security Account Manager (SAM), the Windows NT User Account database.

Policy Management System

eTrust AC provides a standalone policy management system that helps administrators easily manage departmental security policies with policy set-versioning, distribution and remote download abilities, to help ensure all subscription servers obtain the latest security policies, and easy version controls.

eTrust AC lets you manage several databases from a single central computer in two ways:

- Automatic rule-based policy updates
Regular rules you define in a central database (PMDB) are automatically propagated to databases in a configured hierarchy.
- Advanced policy-based management and reporting
Policies (group of rules) you store in a central location can be deploy and propagated to all databases in a configured hierarchy. You can also remove deployed policy versions (undeploy) and report on deployment status, deployment deviation, and deployment hierarchy. You need to install and configure additional components to use this functionality.

Application Policy Generator

An automated policy generator program is provided to profile application behaviors and generate security policies accordingly. It creates security envelope around the applications and greatly reduces the deployment efforts required to construct these rules.

Chapter 2: Fortifying Operating System Security

This section contains the following topics:

[Components, Features, and Installation Considerations](#) (see page 17)

Components, Features, and Installation Considerations

The new open and distributed computing paradigm has created an increased demand on computer security. The integration task among divergent platforms becomes more complex. The need to have a security solution that can address disparate systems with consistent security coverage emerges as an important item on the security list. Also larger corporations conduct mergers and acquisitions more than ever. This has created a new level of security requirements, including burst expansion, distribution capacity, streamlined and centralized management, and cross-platform support.

eTrust AC has built-in basic policies to give organizations immediate results right out of the box. Open and extensible, this powerful solution supports all industry-standard platforms, databases and applications and includes published interfaces allowing it to secure any resource.

Ease of use, combined with centralized user and access administration enables organizations to confidently exploit today's eBusiness opportunities. As a part of the eTrust security solution, eTrust AC can inter-operate with Unicenter NSM, providing a powerful, comprehensive solution for building, deploying, and managing security as part of the larger task of enterprise management.

Components of eTrust AC

eTrust AC includes a database (seosdb), two drivers (seosdrv and drveng), a number of services (including the Watchdog, the Agent, the Engine, the Policy Model, and Task Delegation), and a graphical user interface.

The Database

The database contains definitions of users and groups in your organization, system resources that need protection, and rules governing user and group access to system resources.

The Drivers

The drivers intercept every request to open a file, open a registry key, terminate a process, or perform network activities. The drivers pass these requests to the Engine, receive the decision of the Engine whether the request should be granted or denied, and forward the decision to the original system call of the operating system, which then continues its processing based on the answer it receives from the drivers.

The Watchdog

The Watchdog constantly checks that the other eTrust AC services are running. On the rare occasion when the Watchdog discovers that another service has stopped, it immediately starts the service again.

The Agent

The Agent communicates with eTrust AC clients through a proprietary application protocol above TCP/IP and manages security for the eTrust AC user

The Engine

The Engine manages the database, including controlling all database updates, deciding whether to grant access requests that it has received from the Driver and the Agent, checking that the Watchdog service is running, and restarting the Watchdog if the Watchdog has stopped running.

The Engine handles both database access requests and the decision-making function, reducing interprocess communication to a minimum, and achieving maximum efficiency.

The Policy Model

Managing tens or hundreds of databases individually is not practical, so eTrust AC supplies the Policy Model service, a component that allows management of many computers from one computer. Using the Policy Model service is optional, but it greatly simplifies administration at large sites.

Task Delegation

eTrust AC lets you grant ordinary users the necessary rights and privileges so they can perform administrative tasks. This is called task delegation.

The Graphical User Interface

The Policy Manager is the graphical user interface (GUI) through which all eTrust AC functions are carried out.

Note: For more information about the Policy Manager, see the *Administrator Guide*.

Features of eTrust AC

eTrust AC lets you manage native Windows from one central location and significantly extends native Windows security. eTrust AC also can protect itself. The features are described in the following sections.

Windows Management

After eTrust AC is installed on the Windows stations in your organization, you can manage all of these stations, regardless of the domains they are in, from one central station. To do this, use the Policy Manager, or use the command-line language called selang.

Policy Manager

Policy Manager is the GUI for eTrust AC. Using Policy Manager, you can carry out all eTrust AC functions.

Note: For more information about Policy Manager, see the *Administrator Guide*.

selang

Selang is the command-line language of eTrust AC. You can also use selang to write scripts. You can run selang commands by invoking selang in the command prompt window, or from the Commands and Scripts tool in Policy Manager.

Note: For more information about selang and its commands, see the *Reference Guide*.

eTrust AC Self-Defense

It is virtually impossible for hackers or users to bring down eTrust AC services, intentionally or unintentionally. When eTrust AC is running, it is also virtually impossible for unauthorized users to change or erase eTrust AC files and data because eTrust AC uses special file signatures.

Administrator Account Limitations

Users who administer and manage Windows are usually members of predefined groups that are automatically created during system setup. Each predefined group exists to perform a certain set of system functions. Users who are members of a group can perform all the functions of the group.

The most powerful group in Windows is the Administrators group. Windows creates one account, Administrator, in the Administrators group. Every member of the Administrators group can perform a wide range of tasks, from creating, deleting, and modifying users to locking, reconfiguring, and shutting down servers.

One of the major security risks in Windows is that an unauthorized user can gain control of a user account in the Administrators group. If this happens, the unauthorized user can cause enormous damage to the system.

eTrust AC lets you limit the rights granted to the Administrator account and to limit the rights of users who are members of the Administrators group. This reduces the vulnerability of your Windows system.

Native Windows Security Administration

The following elements of Windows security can be administered with eTrust AC.

Registry Protection

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.

eTrust AC protects the registry to ensure that an unauthorized user does not change system parameters. Authorized users can update registry settings as necessary.

File Protection

Windows uses one of several different types of file systems. The most common are FAT and NTFS. If you use the NTFS file system, Windows protects the files in your system by creating and updating Access Control Lists (ACLs) for each file. eTrust AC supports file ACLs.

Password Protection

eTrust AC can protect passwords and enforce password quality just as native Windows security does, but through its own mechanism. eTrust AC can do the following:

- Enforce a maximum password age
- Enforce a minimum password length
- Save up to 20 generations of a user's passwords
- Lock accounts after repeated login failures
- Force users to log in to Windows before changing their passwords

Server Manager Functionality

eTrust AC can manage other native Windows resources through Server Manager on the Windows NT program bar. Protected Windows resources include:

COM

Records in the COM class define devices with a serial port (COM) or a parallel port (LPT) as listed in the Control Panel under Ports.

Device

Records in the DEVICE class define Windows hardware devices (as listed in the Control Panel under Devices).

Disk

Records in the DISK class define system volumes.

Domain Management

Records in the DOMAIN class define collections of computers that share a common database and security policy (domain).

Printer

Records in the PRINTER class define devices connected to a Windows computer system capable of reproducing visual images on a medium (as listed in the PRINTERS folder).

Process

Records in the PROCESS class define objects consisting of an executable program, a set of virtual memory addresses, and a thread (as listed in the Windows Task Manager).

Service

Records in the SERVICE class define Windows services (as listed in the Control Panel under Services).

Share

Records in the SHARE class define shared resources that include devices, data, or programs used by network users, such as directories, files, printers, and named pipes.

Windows Session

Records in the SESSION class define user sessions on the local host. The record includes the user name, computer name, elapsed time of the connection, and the resources being used.

Native Windows Security Expansion

The following eTrust AC features expand native Windows security.

Administrator Rights for Regular Users

eTrust AC lets you grant ordinary users the necessary rights and privileges so that these users can perform administrative tasks without being members of the Administrators group. This is called task delegation. The ability to delegate tasks-grant administrative privileges-in this granular way is one of the most significant advantages of eTrust AC.

Enhanced File Protection

eTrust AC protects all file systems currently used with Windows. The two most commonly used are the Windows file system (NTFS) and the file allocation table (FAT). eTrust AC also supports CDFS (a file system especially for CDs) and HPFS (an OS/2 file system).

eTrust AC supplies a total security solution to the file allocation table (FAT) and an extra layer of security to other file systems including NTFS and CDFS.

Generic File Protection

Generic file protection is the ability to protect all the files that fit a specified wildcard pattern (regular expression). Any resource with a name matching the specified wildcard pattern is protected by the specified generic access rule. eTrust AC can protect files generically.

If a resource matches more than one generic access rule, eTrust AC chooses the rule that most closely matches the file.

With generic file protection, no more than a handful of security rules must be defined to protect many of the files requiring protection.

Enhanced Password Protection

Native Windows security provides significant protection for user passwords (see page 21). However, eTrust AC significantly extends password protection so that the likelihood of a hacker succeeding in stealing a password is greatly reduced.

When using eTrust AC, you can create additional rules that force users to choose safer, more secure passwords. For instance, you can demand that users select a minimum number of alphabetic, numeric, special, lowercase, or uppercase characters. You can also ensure that the new password selected by a user does not contain, and is not contained by, the password being replaced.

Process Protection

eTrust AC protects specified processes to make sure that they are not killed. eTrust AC process protection is also helpful for protecting Windows services and other non-interactive Windows applications.

SPECIALPGM Protection

eTrust AC protects specified programs, such as system services, that must typically be run as System accounts so that only logical users can access them.

Program and Secured File Protection

eTrust AC protects programs and files by giving them signatures. If a signature has changed, the program or file becomes untrusted and cannot be accessed.

Stack Overflow Protection (STOP)

STOP prevents hackers from exploiting stack overflow, which lets them execute arbitrary commands in order to break into systems.

Program Pathing

Program pathing is the ability to demand that a specific file be accessed only through a specific program. Program pathing greatly increases the security of sensitive files. eTrust AC lets you use program pathing to provide additional protection for the files in your system.

B1 Security Level Certification

eTrust AC includes the following B1 “Orange Book” features: security levels, security categories, and security labels.

Active Directory Management

The following eTrust AC features expand Windows Active Directory Services.

User and Group Properties

Newer versions of Windows use several properties that uniquely identify a user (such as Full Name and Logon Name), but the Microsoft Net API, which managed user properties in older versions of Windows, does not support these properties.

eTrust AC supports these properties, so you can manage the values of user-defined properties in the Active Directory records of users and groups. Support of these properties also enhances Organizational Unit management as well.

Container Management

eTrust AC supports the creation and editing of Active Directory Organizational Units (OUs). An OU is a logical container into which users, groups, computers, and other object types are placed. eTrust AC supports three common object types: **User**, **Group**, and **Computer**, and it also supports OU nesting by supporting the object type OU. This gives you the following abilities:

- Create new users and groups in OUs or containers other than the default containers USERS
- Create or delete a container or OU from the Active Directory
- Move a user or group from one container or OU to another
- See the hierarchic Active Directory structure (parent and child relationships) from within eTrust AC.

Objects in the OU class can be created on the primary domain controller.

Note: The OU class is available only for Windows 2000 Advanced Server stations with Active Directory installed. If eTrust AC is running on computer with other configurations, this class is not applicable.

Security Management for Windows and UNIX

Often large organizations have both Windows and UNIX systems. This complicates the task of maintaining good security. Ideally, you would develop one security policy that can be implemented on both types of systems.

With eTrust AC, you can do the following:

- Develop one common security policy for UNIX and Windows
- Implement the policy by using eTrust AC
- Use one Windows workstation to manage the security for both the Windows and UNIX environments

The ability to make a change and have eTrust AC propagate it to many workstations in different environments greatly reduces administrative overhead.

Some elements that are particularly important in a common security policy are mentioned in the following sections.

Maintaining One Set of Users

After eTrust AC is installed at your site, you can maintain one eTrust AC database that contains all the users. This means that user maintenance must be done only once. eTrust AC can propagate the additions, changes, and deletions to all the workstations—both UNIX and Windows—that should receive the updates.

Maintaining One Set of Groups

It is often convenient to group users together who work on specific projects or in specific departments or divisions in the organization. Windows, UNIX, and eTrust AC all let you define groups of users. You can assign authorities to groups just as you would assign authorities to users. Using groups can ease your workload because you assign authorities once to the group rather than repetitively assigning the same authorities to individual users. Each user then receives the authorities of the group.

Working with eTrust AC makes it possible to create and maintain one set of groups that can be used in both the UNIX and Windows environments.

Maintaining One Set of Access Rules

The Policy Model service lets you develop and maintain one set of access rules for both Windows and UNIX. The Policy Model database (PMDB) lets you propagate a security database, and any changes made to it, to all its subscribers. Both Windows and UNIX workstations can be subscribed to the same PMDB.

Communication between the PMDB and its subscribers usually goes in one direction: the PMDB sends changes from its database to its subscribers. A subscriber communicates with the PMDB only when it informs the PMDB that it is online and requests all the changes that were sent by the PMDB while it was down. This design minimizes network traffic, and guarantees subscriber integrity.

Synchronizing Passwords

One of the main components of any good security policy is forcing users to select good passwords. It is easier if users must remember only one password that can be used throughout the system. By implementing eTrust AC, it is possible to enforce one set of password rules and to enable password synchronization between the two systems.

A PMDB can propagate rules defining acceptable passwords. The PMDB can also propagate new and changed passwords to all the subscriber stations, including mainframe computers.

Note: For more information, see the *Implementation Guide*.

Managing eTrust AC Services

By default, all eTrust AC services start automatically. You can change the way any eTrust AC service starts from automatic to manual or you can disable the service. To access the services:

1. Close eTrust AC.
2. From the Windows Control Panel, open Services.
3. Right-click the service you want to change or disable.
4. Select Automatic, Manual, or Disable for Startup Type to indicate how you want the service to start and click OK.

eTrust AC Documentation

The documentation for eTrust AC is provided as PDF files. To view PDF files, you must download and install the Adobe Reader from the Adobe website if it is not already installed on your computer.

Updated guides will be available at <http://ca.com/support>.

Note: A suitable version of Adobe Reader is also available on your product CD.

A full list of the eTrust AC documentation is available in the readme file.

What's Next

Now that you have a better idea of eTrust AC features and capabilities, you can learn to protect your enterprise's system integrity and your data's confidentiality. The following chapter guides you through protecting programs and files from users and groups.

Chapter 3: Running the Administrator Interface

This section contains the following topics:

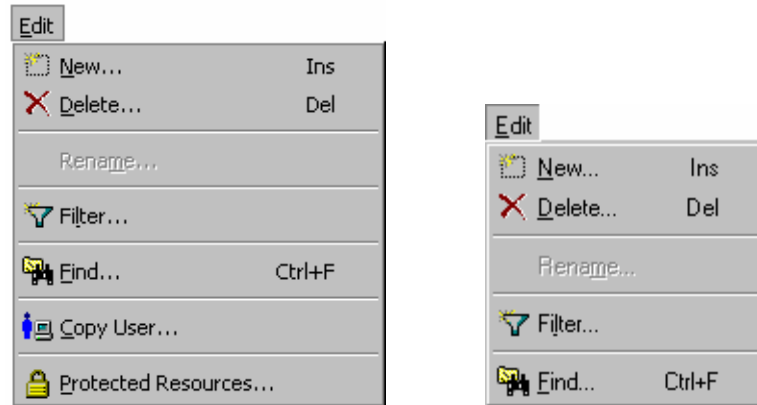
[Implementing and Maintaining Your Security Policies](#) (see page 29)

Implementing and Maintaining Your Security Policies

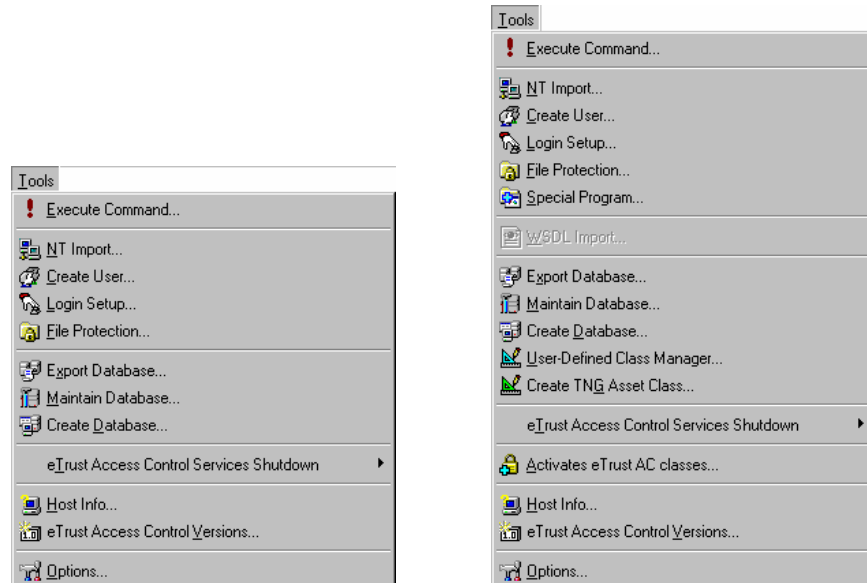
In this chapter, we will walk you through parts of the Policy Manager-the eTrust AC graphical user interface-where you can administer databases on Windows and UNIX platforms.

The Menu Bar and Toolbar

Menus display relevant information, depending on which window is open. Compare the Edit menu for the User window and the Resources window, for example:



As another example, look at the Tools menu. Displayed here are the Tools menus for the User window and the Resources window.



The View menu gives you control over the toolbars and window display.

Program Bar

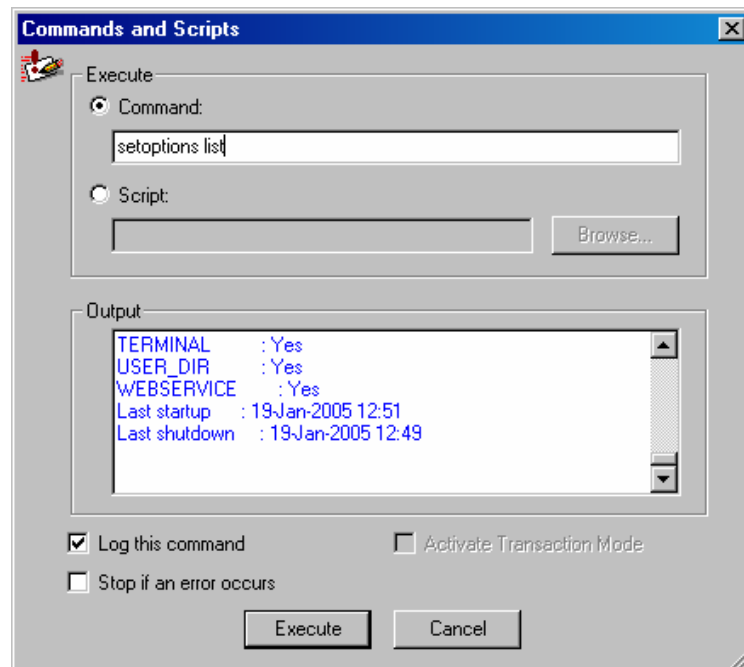
Functions are grouped into three program bars-eTrust accessors and resources, NT resources, and Tools. The same functionality is available using File, Open.

Note: If you have eTrust Web AC installed, you see a fourth bar to administer eTrust Web AC functions. These are described in the documentation for eTrust Web AC.



selang Commands

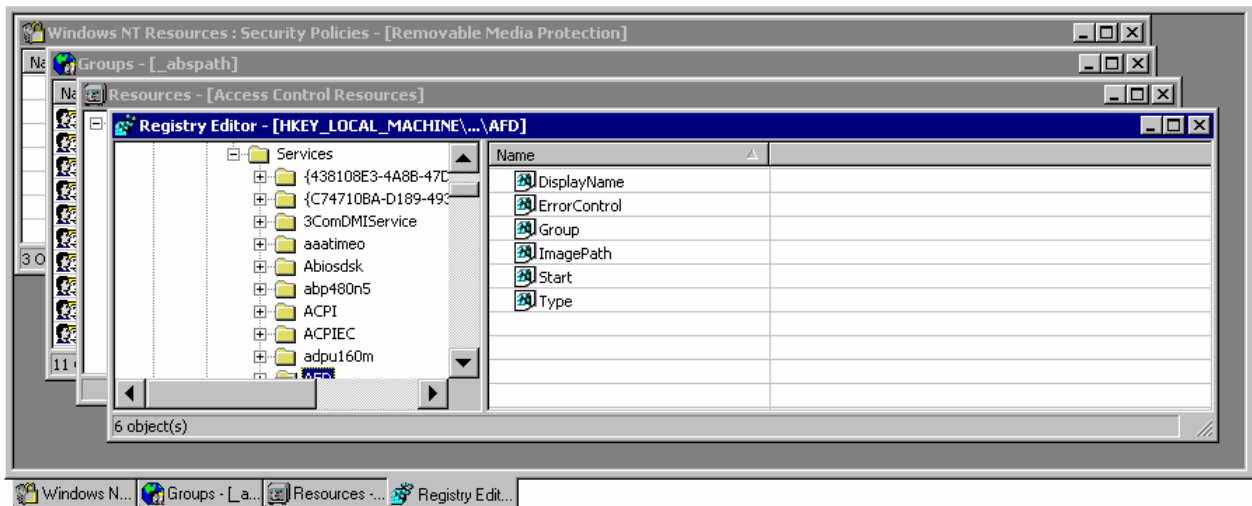
You can issue selang commands from Policy Manager by selecting Execute Command from the Tools menu. On the Commands and Scripts dialog that appears, enter the command in the Execute Command field.



Setting Admin Defaults

To set GUI defaults, select Options from the Tools menu.

You can change any option. *Appearance* and *Format* customize the interface. Make yourself comfortable. For example, Workbook mode puts tabs on the windows. If you work with lots of windows open, you may find it convenient.



Startup sets the startup defaults and activates the custom splash screen. *Create* defines the default environment for creating new users and groups. You may want to change the default to eTrust only for working through the tours. (This minimizes cleanup).

Note: Settings take effect immediately after you click OK.

Wizards

eTrust AC provides many helpful wizards to guide you through common procedures.

Using the Login Protection Setup Wizard

eTrust AC security prevents users from logging in from unauthorized terminals. Specifically, every terminal must be defined in a TERMINAL class record, and every user must have access permissions defined in the Access Control List (ACL) of each terminal they use. The Login Protection Setup wizard takes care of this, and more:

1. Start the Login Protection Setup wizard by clicking the Wizard Manager toolbar button. Select Login Protection
2. Select users and groups to protect:
Note: You can define multiple users and groups on the Protected Users and Groups page.
3. On the Login Terminals page, specify the terminals that the users and groups can (and cannot) log in from.
4. On the Restricting a User Account page, specify the days and times when the specified users and groups can log in.
Note: Use the Weekdays button to deselect Saturday and Sunday with a single click.
5. On the following page, specify login authorization for holidays, and click Finish.

Note: To allow or prevent logins on a specific holiday, you must have previously defined the holiday in the calendar before you use this dialog.

Using the Create User Wizard

Use the Create User Wizard to identify users. Follow the wizard to specify user attributes (such as operator or administrator), passwords and group memberships.

Using the File Protection Wizard

Use the File Protection Wizard to protect specified files and directories. Follow the wizard to select files to protect, users and groups who can access the file, and the level of access they have.

Using the NT Import Wizard

If you did not import Windows users and groups during installation, use the NT Import wizard to:

- Import users from the Windows database to the local host database or to a PMDB
- Import groups from the Windows database to the local host database or to a PMDB

You cannot import to a remote host. You can import the Windows database directly, or save it as a script file (.lng).

Using the Special Program Wizard

Use the Special Program Wizard to protect special programs.

You can set up authorization protection for programs like system services, which usually need to be run as a SYSTEM account. You can restrict access to the specified program by using a logical user or a bypass.

The wizard creates the SPECIALPGM resource and displays the results in the Output Bar of the Policy Manager window.

Using the Copy User Wizard

Use the Copy User Wizard to:

- Copy a user record from one host to another or to a PMDB on the same host
- Attach users to groups as you copy them
- Copy multiple user records from one host to another or to a PMDB on the same host
- Use one user record as a template to create another record on the same host
- Create a script to copy a user record

Note: To access the Copy User wizard, on the Access Control program bar click Users, then from the Edit Menu choose Copy User.

Using the Copy Group Wizard

Use the Copy Group Wizard to:

- Copy a group record from one host to another or to a PMDB on the same host
- Copy member user records with the group from one host to another or to a PMDB on the same host
- Copy multiple group records from one host to another or to a PMDB on the same host
- Use one group record as a template to create another record on the same host
- Create a script to copy a group record

Note: To access the Copy Group wizard, choose Copy Group from the Edit Menu after you have clicked the Groups icon on the Access Control program bar.

What's Next?

Now that you have a better idea about the Policy Manager, the following chapter guides you through setting access and account restrictions and more, giving you suggestions on how to use your new software.

Chapter 4: Discovering the Power of Protection

This section contains the following topics:

[From Protecting Your Programs to Monitoring System Files](#) (see page 37)

From Protecting Your Programs to Monitoring System Files

In this chapter, you will learn how to register new users and groups, protect files and directories, protect files from unauthorized users, protect files with program pathing and file name patterns and much more-the next steps to putting eTrust AC to work for you.

Creating Users and Groups

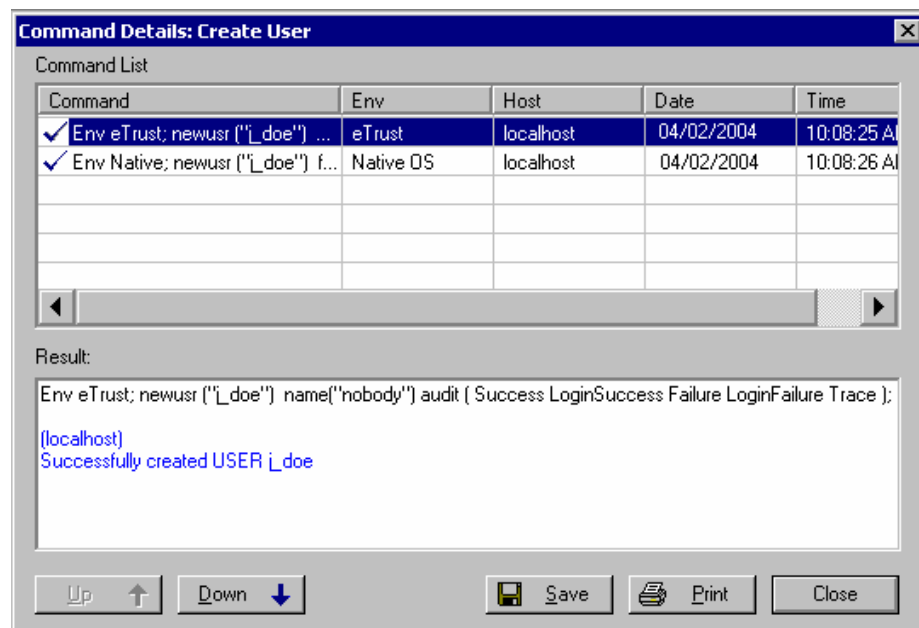
To create a user:

1. Click the Users icon in the program bar on the left side of the GUI.
2. Click the New icon on the toolbar. Enter "j_doe" in the User Name text box. Skip the password options for now.
3. Click User Attributes. Enter **nobody** in the Owner field. Do not check any of the User Type boxes because j_doe is a regular user.
4. Click the Miscellaneous icon and select Audit Information.

Note: The title tells you which panel you are working in.

5. Click All, and then click OK on each of the windows to close them.

If you look at the lower part of the interface, you see that the output bar shows that you successfully created a new user. Double-click the entry line to see the Details window.



The upper part of the window displays the selang commands generated by Policy Manager; the lower part displays the results. Select each command to see the result for that command.

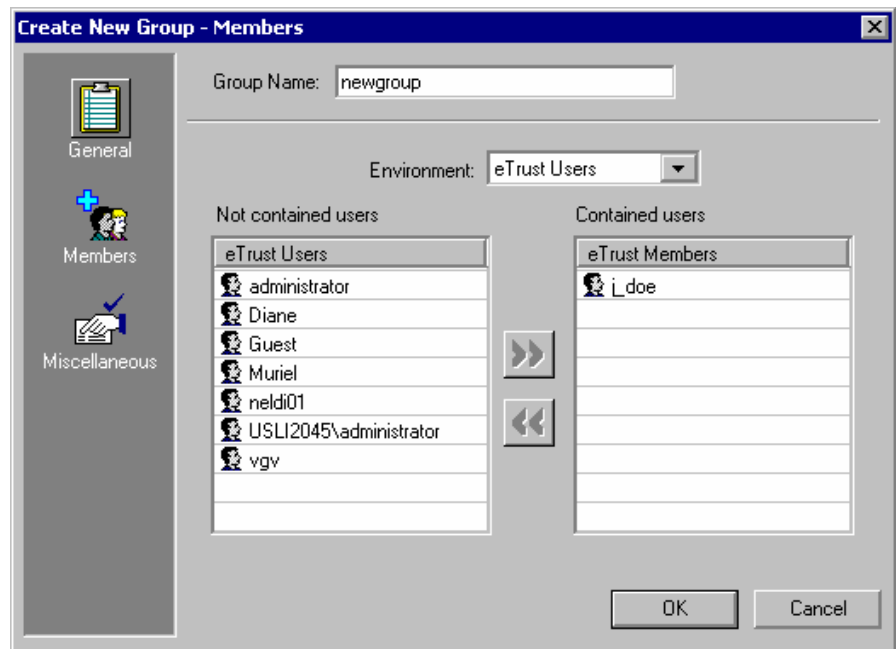
As you probably noticed, this example was very simple. You could have added many more parameters to the user record in the eTrust AC database with very little extra effort.

Here is another example. This time, create a group.

1. Click the Groups icon on the program bar, then the New icon on the toolbar. The Create New Group window is similar to the same as the New User Window.

Note: You can also point your mouse anywhere in the Groups window and right-click. New Group is one of the options on the shortcut menu that appears when you right-click.

2. Give the group a name and assign owner **nobody**. You can also assign a super group. Your new group is then a subgroup; inheriting all of the properties of the super group except those you change or add as you create it.
3. Click Members icon and add some members to the new group.

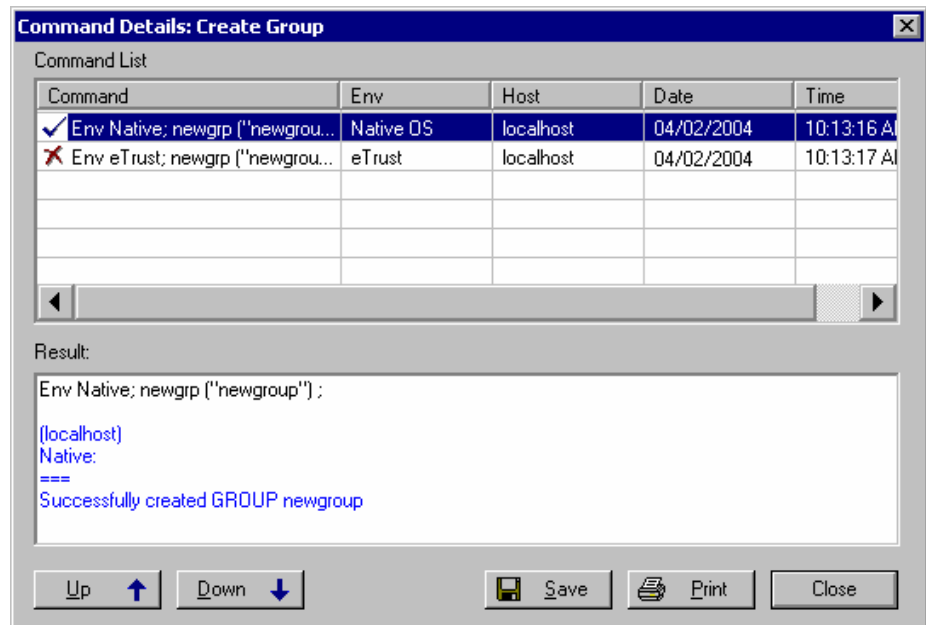


In this example, we have added only one user. You can add more. Hold the Shift or Ctrl key when selecting groups to add several users at once.

4. When you have finished adding users to the group, click the Miscellaneous icon. Add day and time restrictions and click OK to create the new group.

Note: Restrictions assigned to a user take precedence over those assigned to a group.

- Now, look at the command details to see what has happened.



Protecting Files and Directories

Any computer system has at least two kinds of 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. Among the major benefits of eTrust AC is that it can protect files and directories from unwanted access, even from system administrators; and that protection can be extended to non-NTFS file systems.

Let's create a dummy file for this exercise.

- Click on the Resources icon on the Programs bar to open the Resources window. Under System Resources, click File.
- Click the New icon on the toolbar, and use the Browse button to find the file, and then define owner **nobody**.
- Authorize some users or groups to access the file. To do this, click Authorize and then the Add button by the Add Accessors list box. Select the user or group and click OK. The names you add appear in the Add Accessors list box.

4. Select each user or group in turn to select permissions for them.

For the administrator, adm1, we selected Delete only. This is an extreme example of limiting an administrator's access permissions.

We gave user p_jones full permission. (The permissions for p_jones are shown in the previous illustration). But Jones is also a member of Newgroup, which has only read permission. The rule is that permissions are additive, so Jones is not limited by his membership in Newgroup.

Note that we selected a program (Word) for the group. This is known as program pathing, and means that these users are only able to access the file using that specific program. Program pathing greatly increases the security of sensitive files. In this case, for example, no one in the group could open this file with an application that reads the metadata.

5. Finish by specifying the audit mode and clicking OK to create the file resource.
6. Check the command details to see which selang commands were issued.

Note: For more information about file protection, see the FILE class in the *Reference Guide*.

File Groups

Once you have defined files in the database, you can group them and assign permissions to the group. For example, you can put all of the finance department's files in a group called Finance, and allow access only to top management and finance department employees.

The individual files or patterns in the group would have a different set of accessor permissions, based on the need of individuals or groups within the department to access the files. You can also nest file groups within file groups for granular control of the file permissions hierarchy.

Protecting Programs

eTrust AC defines programs that are considered part of the *trusted* computing base. Programs in this class are trusted not to have security breaches because the Watchdog monitors them to make sure they are not modified. If a trusted program is altered, eTrust AC automatically marks the program as untrusted, and the program is prevented from executing.

Note: When defining a program in the PROCESS class, you must also create a FILE class record for it. The order in which you create these records is not important.

To protect a program, look at the System Resources section of the Resources window.

1. Click Program.

Notice that your database already contains a record for Microsoft Word. eTrust AC created it automatically when you implemented program pathing for NewGroup in the previous exercise.

2. Right click the entry for Microsoft Word and select Properties.

You can assign accessors Execute permission only. Denying permission blocks access the program.

3. Click the General icon.

The General panel has a check box labeled Trust. eTrust AC sets this property when you create the Program record. If the program is modified, eTrust AC resets this property to "untrusted" and prevents the program from executing. When the problem is fixed, you can reset the trust property in this window.

Monitoring Files

eTrust AC can monitor important system files. By creating records in the SECFILE class (a class with object representing secured files), you can verify that an unauthorized user does not alter sensitive system files that are not frequently modified. The watchdog scans these files and ensures that the information known about these files is not modified.

The following are some examples of the type of files to include:

- \Winnt\system32\drivers\etc\hosts
- *etc\services
- *etc\protocol
- *etc\networks

Protecting Processes from Being Killed

Executable files that run in their own address space may need to be protected from being terminate or "killed". Major utilities and database servers are good candidates for eTrust AC process protection, since these processes are the main targets for denial-of-service attacks. eTrust AC process protection is also helpful for protecting Windows services and other non-interactive Windows applications.

eTrust AC can protect against three kill signals: the regular terminate signal (TERM) and the two signals that an application cannot mask (Terminate Process and STOP).

As an example, we will protect Task Manager (Taskmgr.exe).

1. Select Process and click New.
2. Create a new record for Taskmgr.exe (in the \system32 subdirectory).

Note: Taskmgr.exe must be active (that is, displayed on the Windows Taskbar) in order to appear as a selection with the Browse button.

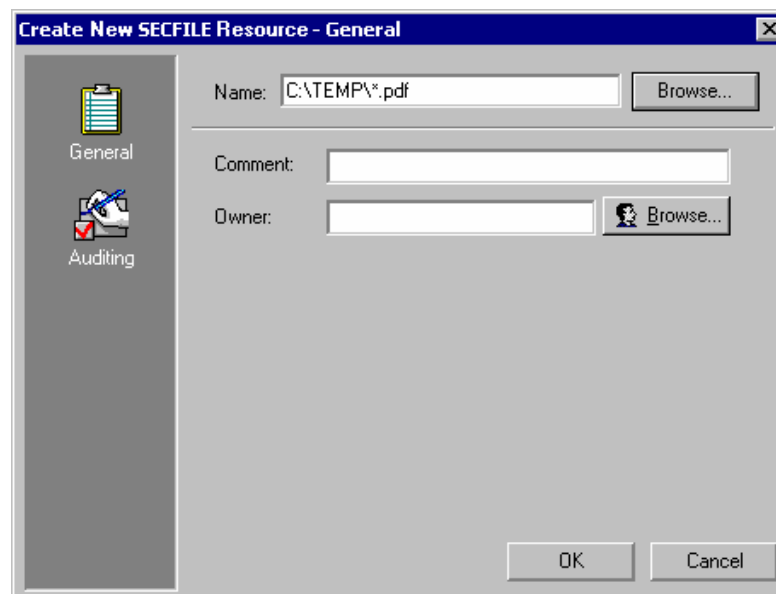
3. Authorize users to kill the process. Read permission means the user can kill the process; Deny means the user cannot kill the process.

Program Patterns

Defining file resources for each file in your system can be tiring. eTrust AC gives you tools to speed up the process.

The following example shows you a quick way to protect groups of files. By specifying a pattern, rather than a specific name, you can enforce the same access restrictions on all files that fit the pattern.

Select Monitored Files on the Resources window and click New.



You can also protect a directory.



Note the check box that lets you protect files and subdirectories. Try creating a file resource with and without checking the box. You see a difference in the resource list. Check the command details to see the different commands issued.

Protecting Other Resources

Notice the other types of resources that eTrust AC can protect. Expand the tree in the Resources window to see that eTrust AC can monitor vital system components such as your network and the Windows registry.

Restricting Access with Predefined Groups

eTrust AC contains four predefined groups that you can use to restrict access to files:

- `_abspath`
- `_interactive`
- `_network`
- `_restricted`

Using the _restricted Group

Adding users to the _restricted group blocks them from accessing any file that they are not specifically given access to. This includes files that are not listed in the database. These files are controlled by the default access value of the FILE class. On installation, this default is automatically set to none.

Note: If a user is added to the _restricted group and the database contains few FILE access rules, then a _restricted user may not be able to do anything. If you plan to add users to the _restricted group with NONE as the default access for the FILE class, consider using WARNING mode. Then the audit events show what files your _restricted users need for their work. After awhile, you can grant the appropriate authorizations and turn WARNING mode off.

You already know how to add a user to a group. Adding a user to the _restricted group is no different.

To promote security, reset the audit mode for the FILE class.

1. In the Resources window, open the Administration folder and click Access by Class. Double-click FILE.

Note: If you hold the cursor over the Set Default Access button, the tool tip displays the current default access.

2. Open the Auditing panel. Clear Failure and select Warning Mode.
3. Now you can test the results of adding a user to _restricted.

Note: eTrust AC reads the list of _restricted users only when starting. If a user has joined or left the _restricted group, the change is effected only when you restart eTrust AC.

Using the _network and _interactive Groups

The _network group defines access from the network to a particular resource. The _interactive group defines the access permitted to a particular resource from the computer on which the resource resides. These groups apply to all resources, not just files. They also apply to all users; no user has to be explicitly added to the group.

Let's look at an example.



Here, we have added _network with no permissions to the Access Control List (ACL) of the file Company Secrets.doc. This means the file cannot be accessed from the network. _interactive works the same way on the local host. Remember, you do not add users to these groups.

Note: There is no connection between the _network and _interactive groups in eTrust AC. You can add them both to the same resource.

What's Next?

You now have a better idea about creating users and groups and protecting files, directories, and programs. The following chapter guides you through the administrator interface.

Chapter 5: Gaining More Control of Your User Accounts

This section contains the following topics:

[Limiting User Accesses and Privileges](#) (see page 47)

Limiting User Accesses and Privileges

In this chapter, you set administrator rights, restrict access from terminals, set time-of-day and day-of-week rules, set conditional access, and more- the next steps to putting eTrust AC to work for you.

Limiting the Use of Administrators

One of the major security risks in computer networks is that an unauthorized user could gain control of a user account in the Administrators group. If this happens, the unauthorized user can cause enormous damage to the system.

eTrust AC lets you limit the rights granted to the Administrator account and limit the rights of users who are members of the Administrators group. You can then distribute the Administrator-type rights and privileges to regular users, allowing them to perform administrative tasks without being members of the Administrators group. This feature-called *task delegation*-is one of the most significant advantages of eTrust AC.

User Types

eTrust AC provides a number of user types that have partial administrator privileges. Assigning users these attributes is usually the first step in distributing administrator privileges.

Among the eTrust AC user types are the following:

Group administrators

Users who can perform most administrative functions within one particular group.

Sub administrators

Users who can manage administrator-specified classes and resources.

Password managers

Users who have the authority to modify the password settings of other users.

Group password managers

Users who have the authority to modify the password settings of other users in one particular group.

Auditors

Users who have the authority to read audit logs. They also determine the kind of auditing to be done on each login and each attempt to access a resource.

Group auditors

Users who can read audit logs for a particular group. They also have the authority to determine the kind of auditing to be done within that group.

Operators

User who can display (read) all the information in the databases.

Group operators

Users who can display all the information in the databases for the group in which they are defined.

Note: Do not confuse the Administrators Group (which *is* part of native Windows) with a group administrator (which is not).

You can define these special user types in the native environment and in the eTrust environment. Their special permissions, however, are part of eTrust, not part of Windows.

You can assign user attributes when creating a new user or modifying an existing user record. Policy Manager supports assigning attributes in the eTrust database.

To assign user attributes to an existing user, click the Users icon. Select the user name in the resulting list, and click User Attributes.

To assign attributes for a user that apply only within groups, click the Groups icon. Select the group name under the "Member of" column, and click Group Attributes.

This attribute gives user j_doe the right to audit accessors and resources owned by group Administrators.

Note: When you make a group the owner of an accessor or resource, the administrators, auditors, and other members in the group have their respective administrative privileges for that accessor or group.

Restricting Access from Terminals

eTrust AC provides several ways to restrict user access. These include setting an expiration date for an account, setting grace logins, limiting login to specific days and times, and controlling the terminals from which users log in. We look at terminals here, and time restrictions in the following section.

When we created a new user with the wizard, we used the Login Setup wizard to define a terminal for the user. Remember, not matching the user with a terminal can prevent the user from logging in or from accessing protected resources. Let's take a closer look at the Terminal resource.

First of all, you need a pair of users defined in the native environment. If you have not defined them, do so now. To save time, add an existing eTrust user to the native environment:

1. Select a user, click the Properties icon on the toolbar, and add the native environment using the Advanced button.

Note: You can also right-click a user, and choose Properties from the shortcut menu.

2. Assign terminal permission to the user:
 - a. Click the Resources icon on the program bar, and click the plus sign next to Login Protection to open the tree.
 - b. Select Terminal, and then double-click your local host.
 - c. Open the Authorize panel and click the Insert icon for Add Accessors.
 - d. Use the browse button to add the user, then click OK.
 - e. Check the Deny box for Read and Write permissions.

User j_doe is now blocked from using the terminal named workstation1.

3. Now repeat the authorization with another user, and this time assign Read permission.

Note: To let a user administer the terminal, assign Read and Write permissions.

4. Log off your computer, and try logging in as each of the users. User j_doe should receive a login error message, but user b_raines can access the terminal.

Important! When cleaning up from this exercise, **do not** delete the terminal resource for your computer. (You can delete terminal resources for remote computers.) **Do not** delete or change your own read and write authorization for your computer. Doing either of these blocks your ability to administer eTrust AC. You may not be able to recover except by reinstalling the software.

Terminal Groups

If you want to assign similar restrictions to several computers, you can put them in a terminal group and authorize all of them at once.

1. Select Terminal Groups in the Resource window, and click the New icon on the toolbar.
2. Give the group a name and owner.
3. Open the Membership panel. Click the New icon for Add/Delete Members and select the terminals.

Note: Hold down the Ctrl key or the Shift key to select multiple terminals.

4. Complete the authorization and auditing as before.
5. Check the command details to see which selang commands were generated.

Limiting IMPERSONATION Requests

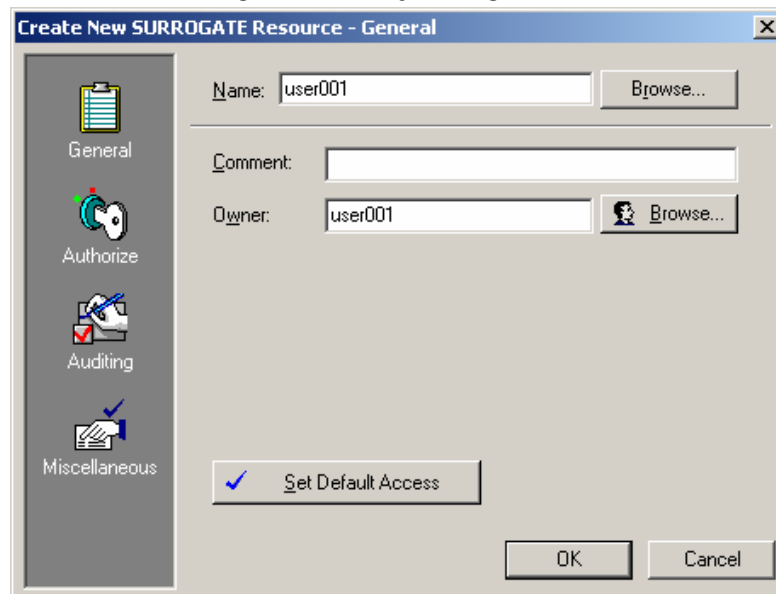
An *impersonation request* is generated when a user tries to switch from his or her username to another username. Impersonation requests can come directly from a RunAs command, or they can come from any program that uses the proper Win32 API.

eTrust AC protects Administrator and other users by enforcing limits on impersonation requests. For a demonstration, follow these steps:

1. Select a username whose password you know. In the following commands, *user001* represents the user name that you have selected.

On the Resources window, select User Identity Control, User ID Substitution and then click New on the toolbar.

2. Define the following rule in Policy Manager:



This rule tells eTrust AC to protect against impersonation requests for user *user001* and not to allow anyone to impersonate user001 unless explicitly authorized.

You can test the surrogate rule as follows.

- From a windows shell, enter the following command:

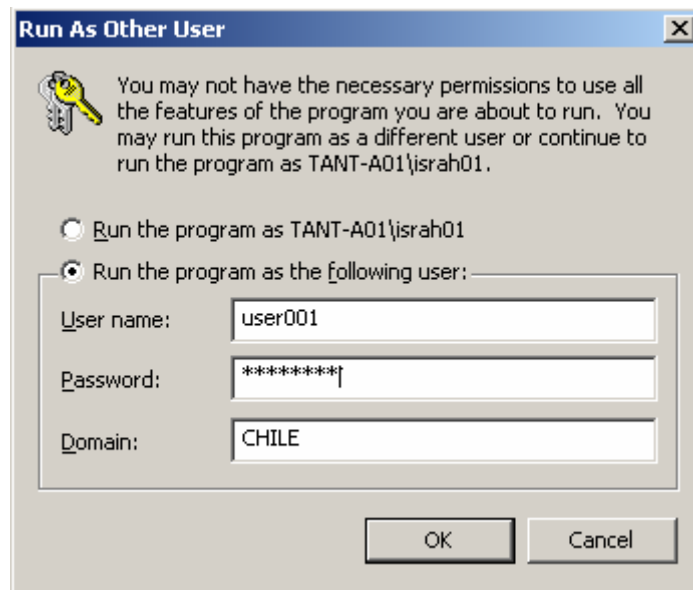
```
cmd> RunAs /profile /USER:CHILE\user001 cmd.exe
```

- Enter password for CHILE\user001

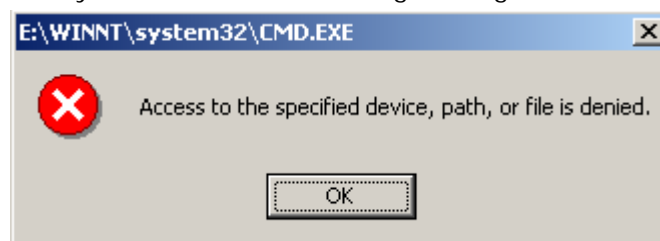
The system returns the following messages:

```
Attempting to start "cmd.exe" as user "CHILE\user001"...  
RUNAS ERROR: Unable to run - cmd.exe  
5: Access is denied.
```

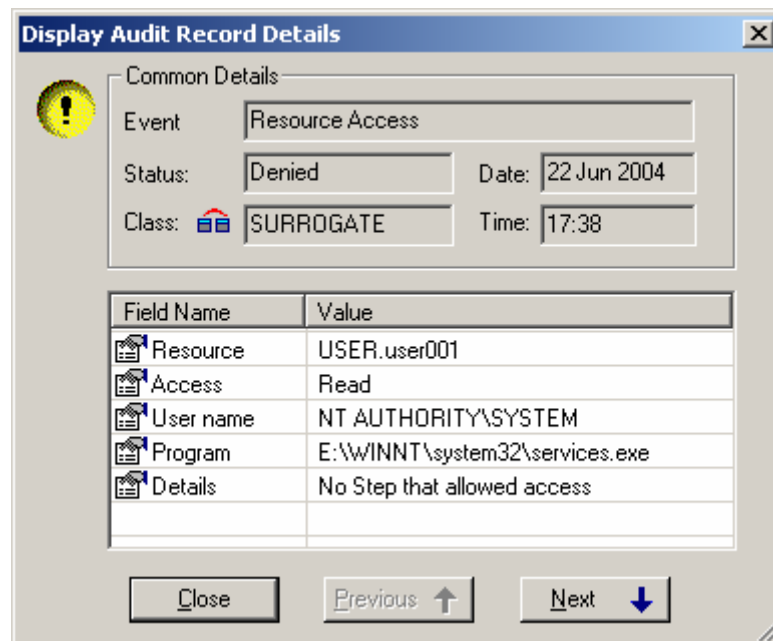
- From a Windows Run As Another User dialog, enter:



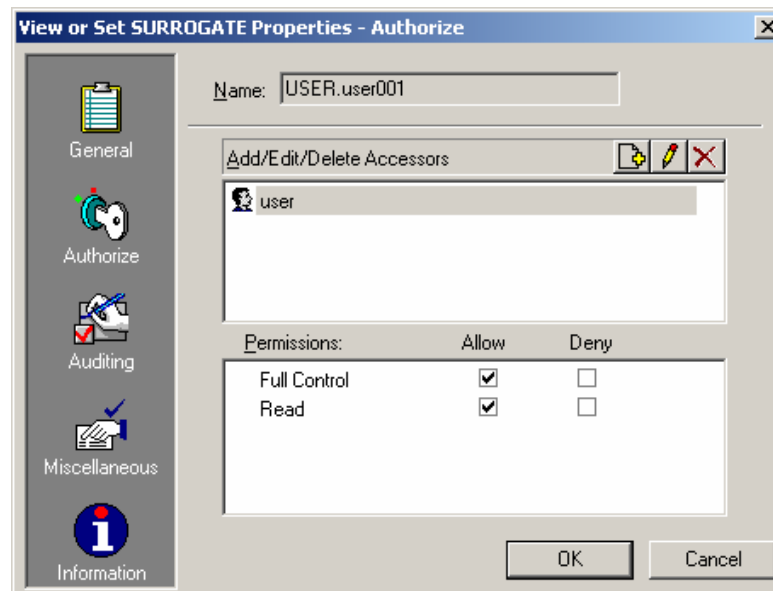
The system returns the following message:



In the audit window, you find that the impersonation event was denied because there was no rule to grant you access.



If you want to instruct eTrust AC to allow you to impersonate to user001, specify the following rule in the eTrust Policy Manager window. You can specify your own username if you want to be the only user allowed to impersonate to user001. If you want to permit all eTrust AC defined users to impersonate to user001, you can use an asterisk (*) as user.



Note: Even the super-user cannot impersonate to *user001* unless the authorize command is used to explicitly authorize such an impersonation request.

Setting Time-of-Day and Day-of-Week Rules

The most vulnerable time for a system is usually late at night and on weekends, when few auditors or other personnel are present. With eTrust AC, you can restrict user logins to specific times of the day and to specific days of the week, giving you a greater level of security.

Start by adding time restrictions to a user.

1. Select a user and open the User Properties window. Set time restrictions by clicking the Day/Time Restrictions button on the Miscellaneous panel. The default is 24 hours a day for 7 days a week. You can deselect any days you wish. The times apply to all of the selected days; you cannot set different times for each day.

You can also select a Unicenter TNG calendar to use the Calendar feature.

2. Click OK when you are finished setting restrictions.
3. Check your results by trying to log in as the user during authorized and unauthorized times.

Account Lockout

In the previous example, we gave Peter Jones extra login access around the standard 9 to 5 day. These times relate to login only. Once logged in, he can stay on the network as long as he wants. If we want to prevent Peter from being on the network at 6 pm, we must set that up as follows:

From the Policies menu, choose Account. The Account Lockout tab has a check box at the bottom to force logoff.

Setting Holiday Information

Another way to restrict times when users have access to the system is to define Holidays. Holidays block access to the system for all users not given special permissions.

Note: The best way to make sure you do not lock yourself out of the system is to change your user attributes to include Ignore Holiday before you start this exercise. This gives you permission to log in during all holidays. See the following illustration.



To set a holiday:

1. Open the Resources window again.
2. Under Login Protection, select Holidays.
3. Click the New icon on the toolbar to create a new Holiday resource.
Selecting the Holiday icon lets you add dates. You can put as many holidays as you want in a single Holiday resource, or you can define separate holidays if you want more control over permissions.
4. Enter the start and end dates, or click the arrow next to the date field to drop down the calendar for point-and-click selection. The default sets the holiday for all day every year, but you can change that by clearing the appropriate check boxes.
5. Next, assign authorization permissions. Each user or group granted Read permission can log in during the specified holiday.

6. Create a holiday resource for today. Give some users Read permission, give some users None permission, and leave other users off the list entirely.
7. Now, try to log in as each user.

Resources

Resources can also have time restrictions applied to them. You can restrict access to terminals, files, network protection objects, container objects, registry objects-in fact any resource-to specific days and times.

The procedure is identical to restricting times for users. Select a resource, open the Properties window and enter restrictions on the Miscellaneous panel.

What's Next?

Now that you have a better idea of how to limit user access and privileges, helping you control your network's security, read the following chapter, which guides you through protecting networks, controlling outgoing connections, and more.

Chapter 6: Protecting Network Activity

This section contains the following topics:

[Controlling Network Level Accesses](#) (see page 57)

Controlling Network Level Accesses

In this chapter, you walk through protecting the network's TCP/IP connection-the next steps to putting eTrust AC to work for you.

Protecting the Network (TCP/IP)

The openness of a TCP/IP network is both its most appealing feature and, in terms of security, a major deficiency. As a network protector, eTrust AC provides the functionality of firewalls without requiring a computer specifically dedicated for that purpose. Using eTrust AC, you can permit specific clients to send specific TCP/IP services to specific hosts and permit only certain hosts to send specific TCP/IP services to the local host.

Controlling Inbound Connections

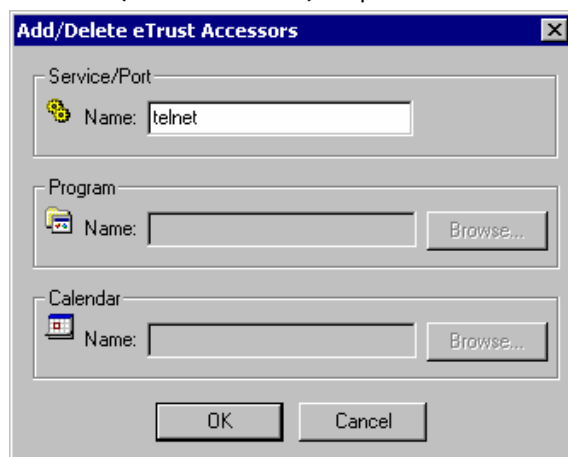
To see how eTrust AC protects a computer from unauthorized access from the network, perform these steps:

1. Check to see if the HOST class is activated.
 - a. Choose **Activates eTrust AC Classes** from the Tools menu.
The **Activate eTrust Classes** dialog appears.
 - b. Scroll until you find **HOST**. If the **HOST** box is not checked, check it and click **OK**.
2. Select another computer-attached to the computer you are running eTrust AC on-to define as a host. In the following example, *workstation2* represents the computer that you have selected.

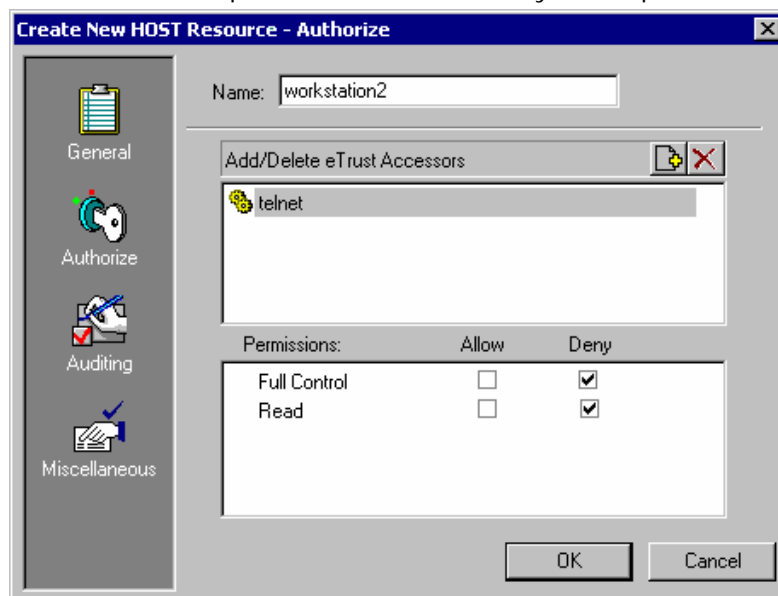
3. Define workstation2 as a host.

From the Access Control program bar, click the Resources icon, expand Network Protection, and select Host. Then click the New icon on the toolbar. The Create New HOST Resource-General dialog appears:

Using the icons on the left, enter information for the new HOST record. Use the Authorize icon to enter authorization information, including services (such as TCP/IP) or ports:



4. Give the local host permission to receive all TCP/IP services from workstation2 except Telnet. To do this, deny Telnet permissions:



5. Try to Telnet from workstation2. Your attempt should be denied.

6. Try to FTP from workstation2. Because FTP is a non-Telnet TCP service, the FTP request should be granted.

Note: You can also specify TCP/IP access rules at the host-group level, the network level, and the name-pattern level.

Protection at the Host-Group Level

To define a host group, create a database record in the class GHOST. The host group receives authorizations the same way as a single host.

Note: Just as for individual users, any one particular rule for individual hosts overrides the rules of the group.

To set TCP/IP access rules on a resource from the Access Control program bar click the Resources icon, expand Network Protection, and select Host Groups. Then click the New icon on the toolbar.

Protection at the Network Level

You can also specify eTrust AC access rules at the network level. To define a network, create a database record in the class HOSTNET. Then the network receives authorization the same way as a single HOST record does.

Note: Any rules at the host-group level override the rules of the network level.

To set TCP/IP access rules on a resource from the Access Control program bar click the Resources icon, expand Network Protection, and select Host Network. Then click the New icon on the toolbar:

Create New HOSTNET Resource - General

Name:

Comment:

Owner: Browse...

Network

Mask:

Match:

OK Cancel

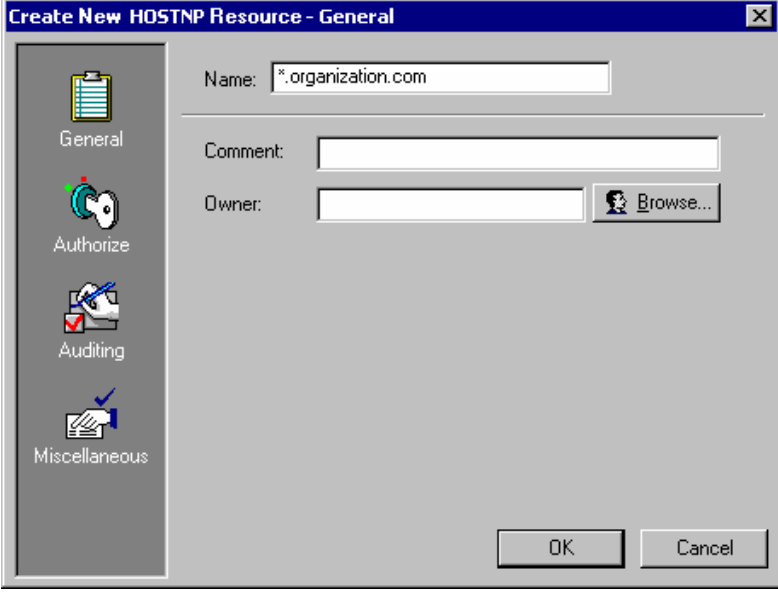
Protection with Name Patterns

Another way to define TCP/IP access rules is through the name-pattern service using the HOSTNP (host name pattern) class. The network receives authorization in the same way as a single HOST record does.

Note: Any rules at the network level override the rules at the name-pattern level.

To set TCP/IP access rules on a resource, click the Resources icon on the Access Control program bar, expand Network Protection, and select Host Protection by Name Pattern. Then click the New icon on the toolbar.

The Create New HOSTNP Resource dialog appears:



The image shows a Windows-style dialog box titled "Create New HOSTNP Resource - General". On the left is a vertical sidebar with four icons and labels: "General" (a clipboard icon), "Authorize" (a hand with a red arrow), "Auditing" (a hand with a red checkmark), and "Miscellaneous" (a hand with a blue checkmark). The "General" tab is selected. The main area of the dialog contains three fields: "Name:" with the text "*.organization.com", "Comment:" with an empty text box, and "Owner:" with an empty text box and a "Browse..." button to its right. At the bottom right are "OK" and "Cancel" buttons.

Controlling Outgoing Connections

The outgoing connections of each computer can be managed as another type of resource.

By limiting outgoing connections within your network, you can minimize damage from any perpetrators who manage to break in through a firewall. Legitimate Internet visitors, too, can be confined to a specific set of services and systems within your network. You might, for example, allow only email and certain necessary forms of database access.

To see how eTrust AC limits outgoing connections, perform these steps:

1. Check to see if the CONNECT class is activated.
 - a. Choose Activates eTrust AC Classes from the Tools menu.
The Activate eTrust Classes dialog appears.
 - b. Scroll until you find CONNECT. If the CONNECT box is not checked, check it and click OK.
2. Select another computer-attached to the computer you are running eTrust AC on-to define as a connect resource. In the following example, *workstation2* represents the computer that you have selected.
3. Define workstation2 as a connect resource. To do this, on the Access Control program bar click the Resources icon, expand the Common and Network Protection folders, and select Outgoing Connection by Host. Then click the New button.
4. On your machine try to telnet or FTP to workstation2. Your attempt should be denied.
5. Assign connection permission to the user j_doe:
 - a. Click the Resources icon on the program bar, and click the plus sign next to Network Protection to open the tree.
 - b. Select Outgoing Connection by Host, and then double-click workstation2.
 - c. Click the Authorize icon to open the Authorize page and click the Insert icon for Add Accessors.
 - d. Use the browse button to add the user j_doe, then click OK.
 - e. Check the Allow box for Read permissions.

User j_doe is now permitted to telnet or FTP to workstation2, despite the deny rule for all users.

Service-Oriented TCP/IP Rules

eTrust AC also accommodates service-oriented TCP/IP access rules (in addition to the host-oriented like the rules mentioned earlier in this chapter).

These kinds of access rules can govern inbound and outbound connections through a specific TCP service (port). To define such rules, you use the TCP class.

To see how eTrust AC protects a computer using service-oriented TCP/IP rules, perform these steps:

1. Deactivate the HOST and CONNECT classes.

- a. Choose Activates eTrust AC Classes from the Tools menu.

The Activate eTrust Classes dialog appears.

- b. Scroll until you find HOST. Make sure the Host box is not checked.
- c. Scroll until you find CONNECT. Make sure the CONNECT box is not checked.
- d. Click OK.

2. Define Telnet as a TCP service:

On the Resources window, select Network Protection, TCP Protection and then click New on the toolbar.

Give the local host permission for Telnet activity with all computers except receiving Telnet communication from workstation2. To do this, click the Set Default Access button on the Create New TCP Resource-General dialog and select All. Click OK.

3. Click the Authorize icon to enter authorization information. On the Create New TCP Resource-Authorize dialog, click the Insert icon, and then on the Add/Edit eTrust Accessor dialog, click the Browse button, choose Host and then choose workstation2.

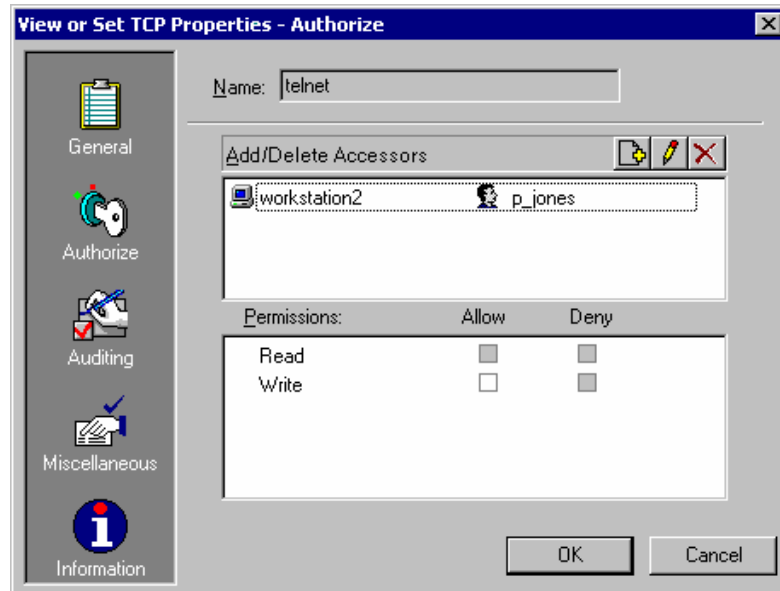
Make sure Read and Write permissions are not checked for workstation2.

4. Try to Telnet from workstation2. Your attempt should be denied.
5. Give all computers permission for Telnet activity with the local host except for user p_jones sending Telnet communications to workstation2.

Note: You have already set the default access for the Telnet resource to All.

- a. Click the Authorize icon on the View or Set TCP Resource dialog.
- b. Click the Insert icon, then on the Add/Edit eTrust Accessor dialog, click the Browse button, choose Host and then choose workstation2.
- c. Check the Outgoing Connection box and enter p_jones in the Name field.

- d. Click OK. Your dialog should look like the following:



6. Log in as user p_jones and try to Telnet to workstation2. Your attempt should be denied.

What's Next?

Now that you have learned more about protecting network, the following chapter guides you through setting password policies.

Chapter 7: Setting Password and Audit Policies

This section contains the following topics:

[Passwords, Logins, and Auditing Rules](#) (see page 65)

Passwords, Logins, and Auditing Rules

In this chapter, you define password policies, change passwords, activate policy checking, audit policies, and much more. The Policy Manager makes it easy to set a default security policy.

A security policy consists of password rules, login rules, and audit rules. You can set one general policy for users and different policies for groups, on a group-by-group basis. Some settings are global, but others (minimum and maximum age and grace, for example) can be overridden by the individual user settings.

Setting Password Policies

Before you define a password policy, check to see if password policy checking is activated. (This is the default setting for new installations.)

1. Choose **Activates eTrust AC Classes** from the **Tools** menu.

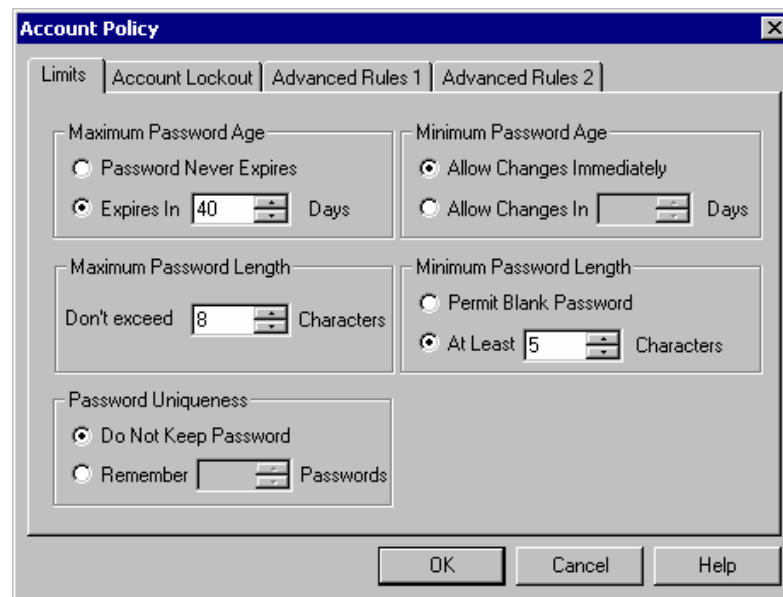
The **Activate eTrust Classes** dialog appears.

2. Scroll until you find **PASSWORD**. If the **PASSWORD** box is not checked, check it and click **OK**.

Before you make this-or any other-change, check the password rule defaults. Make a note of the settings so that you can restore them when you complete the exercises in this section.

3. After inspecting the current values in eTrust AC, you can change the values to suit the needs of your site. For more information, see the *Administrator Guide*.
4. To set general user account policy, activate the **User** window. Select the **Users** icon on the program bar. Then select **Policies** on the menu bar. You can set **Account** or **Audit** policies from this menu.

The **Account Policies** window has four tabs. The first two tabs set rules that apply to both the native operating system and the eTrust database. The **Advanced Rules** tabs set eTrust policies only.



5. Change some of the parameters. You can check the results by testing the restrictions on the system.

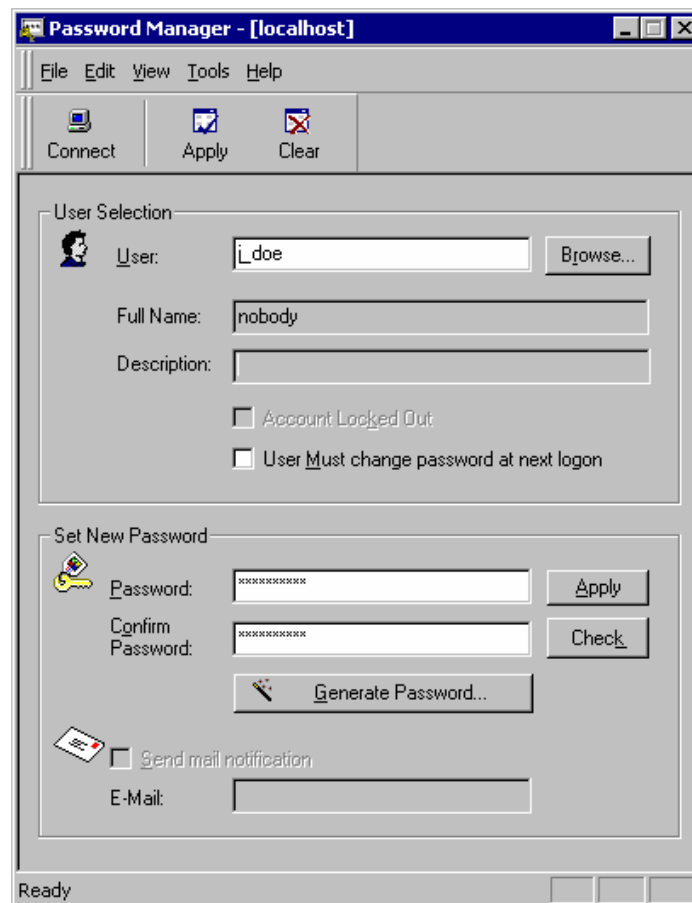
Advanced rules set the eTrust password policy. The Number of Logons field represents the grace login parameter.

Note: For more information about grace logins, see the *Administrator Guide*.

Changing Passwords

You do not need Policy Manager to change user passwords. Users designated as Password Managers in the database can have just the Password Utility (SetPwd.exe) installed on their workstations, accessible from the Start button on the taskbar.

Choose Start, Programs, CA, eTrust Access Control, Password Manager. The Password Manager utility can change passwords for any user defined in the native environment.



Setting Audit Policies in the Native Environment

Set the audit policy by choosing Audit from the Policies menu.

Try changing some of the parameters. Check the results by inspecting the command line details.

You can see the results of your changes by opening the Windows Event Viewer.

Cleaning Up

Be sure to reset password and audit policies to original defaults.

What's Next?

Now that you have a better idea about password and audit policies in eTrust AC, the following chapter guides you through managing multiple hosts. You will create Policy Model Databases, point workstations to a PMDB, work with the Policy Model, and more.

Chapter 8: Centralizing Administration

This section contains the following topics:

[Creating Users, Security Policies, and More](#) (see page 69)

Creating Users, Security Policies, and More

In this chapter, you create a Policy Model database (PMDB) and register users, permissions, and passwords. The Transaction Manager sends eTrust AC transactions to multiple hosts automatically, as they are performed on the local host.

Creating a PMDB

In the example that follows, we create a PMDB, named policy1, and register the PMDBs workstat1 and workstat2 as its subscribers. To keep this example simple, we create the subscribers on the same host.

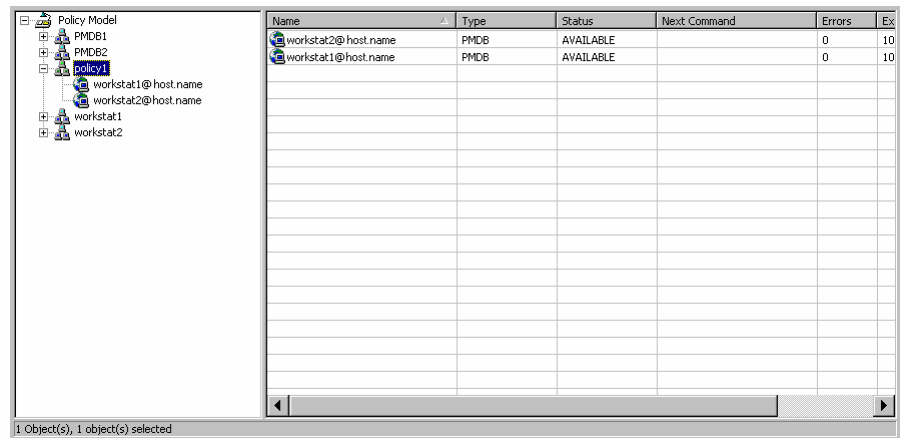
To register two users-adm1 and adm2-as authorized to administer the PMDB, complete the following steps:

1. Connect to bighost. Create the user accounts for the administrators.
 - The administrators of a PMDB are users authorized to change the properties of the PMDB.
 - The auditors of a PMDB are users authorized to view the PMDB's audit log files.
 - The password managers of a PMDB are users authorized to change passwords in the PMDB.
2. Create the user with all three attributes.
3. Give the administrators terminal permissions to administer from the workstation.
4. Now log off and log back in as one of your administrators.
5. Click Tools on the program bar and select Policy Model.
6. Select the New icon on the toolbar to create a new PMDB. Enter the name of the PMDB, and then select the Administrators icon.
7. Select New, then enter the name or use the Browse button. Repeat for the second administrator.
8. Now select Terminal. Click New, and then enter the name of the host or use the Browse button.

9. Now that you have created the PMDB, you can add subscribers. A subscriber can be any existing PMDB or eTrust database. In this example, we have already created the subscriber PMDBs on bighost, but they could be anywhere in the enterprise.

Right-click the PMDB policy1.

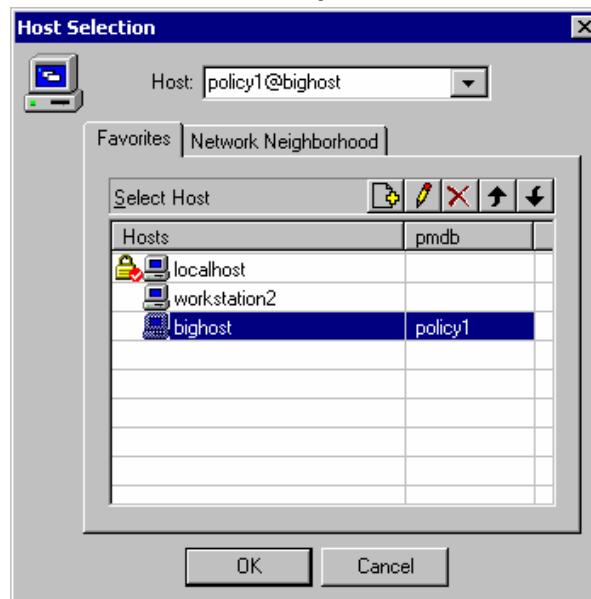
10. Choose Add Subscriber. Enter the name in the form subscriber@host.
11. Repeat for the second subscriber. The tree displays the Policy Model hierarchy.



Working with a PMDB

Now, we will create a new user and watch the changes propagate through the model.

1. First, connect to the Policy Model.



2. Create a user jsmith (Jennifer Smith).
3. Connect to one of the subscribers.

Note: Remember, if a host is not on your favorites list, you can enter its name at the top of the connect dialog.

4. Open the Users window.

New user jsmith appears in the list.

Transaction Manager-A Simpler Alternative

The Transaction Manager sends eTrust AC transactions to multiple hosts automatically, as they are performed on the local host. This transaction mode is intended as a quick and efficient substitute for the Policy Model. It does not offer guaranteed propagation to the security database of every subscriber, but it is simpler to use, and is especially useful when you want to make changes to multiple databases that are not defined as part of your Policy Model hierarchy.

Setting Up the Transaction Manager

Before using the Transaction Manager, verify the following:

- You have ADMIN authority on each remote host you will be accessing, as well as on the local host.
- You created a TERMINAL record for the administering computer on each host you will be accessing.

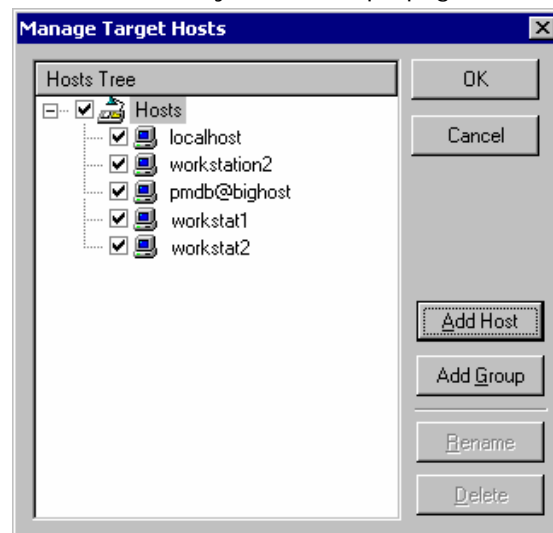
These requirements are the same as for administering a remote host. You must enable the Transaction Manager before you can use it.

1. From Policy Manager, choose Tools, Options and click the Transaction Mgr tab.
2. Select the Enable multi-host transactions box above the list.

You can also select other Transaction Manager options you want to activate.

3. Click File, Target Hosts to create the Target Host file.
4. Add the hosts-workstat1 and workstat2-to the target host list.

Select the hosts you want to propagate commands to.



Hosts can be local databases or PMDBs. You can create groups of hosts to speed selection. Clicking a group name activates all members of the group. You can also select or deselect any individual host. The selections go into effect immediately on clicking OK and remain in effect until changed. You must manually reset the Target Host File each time you want to send transactions to a different group of hosts.

Note: When Transaction Mode is enabled, the Host Selection settings apply to the Copy User and Copy Group Wizards as well as the Transaction Manager.

5. Before you continue, connect to bighost again. Now, click the Transaction Mode icon on the toolbar.

Any transaction you perform is propagated to the selected hosts as well. When you click the Transaction Mode icon again, commands are not propagated.

Now, delete the user we just created.

1. Select user jsmith and click Delete on the toolbar.

To see what happened internally, right-click the Transaction Manager icon in the Windows Taskbar tray, and choose Open Transaction Manager. The following dialog displays the results for workstat1.

2. Select workstat2 to see results on that host.

In this example, the log appears in red, indicating that the command was not successfully propagated.

3. Double-click the selection to see the command details for more information.

Note: After correcting a problem, you can run the propagation again by selecting the transaction and clicking the Run Again icon. (The Run Again icon looks like a set of gears.)

What's Next?

You now have a better idea about the Policy Model, PMDBs, and the Transaction Manager. The following chapter guides you through integrating eTrust AC with Unicenter TNG.

Chapter 9: Integrating with Unicenter

This section contains the following topics:

[Integrating eTrust AC with Unicenter](#) (see page 75)

Integrating eTrust AC with Unicenter

eTrust AC is fully integrated with the Unicenter TNG enterprise management environment. This chapter describes how eTrust AC handles the integration.

Note: For integration to occur, Unicenter TNG must be installed on the same machine as eTrust AC, and Unicenter TNG Security should be activated with the following command:

```
SETOPT CA_ROUTER_CAUSECU 1  
SETLOCAL CAIACTSECSV YES
```

Installing Unicenter Integration Tools

Complete the following steps to set up Unicenter Integration in the Windows environment. Do the following to **each** node during the eTrust AC installation:

1. On the Select Components dialog of the Installation Wizard, select Unicenter Integration and click Next.
2. 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.
3. 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 and click Next. (The default is every 10 minutes.)
4. If you want to migrate Unicenter Security data, on the Unicenter Migration dialog of the Installation Wizard, select Migrate Unicenter Security data to eTrust Access Control and click Next.

Note: If you do not want to migrate Unicenter Security data, do **not** select Migrate Unicenter Security data to eTrust Access Control.

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).

5. Continue with the rest of the installation.
6. If the Database Import dialog appears, choose Yes or No to indicate whether to import Windows NT data into the database.

Note: If you did **not** select the Migrate Unicenter Security data to eTrust Access Control option, the Database Import dialog does not appear.

Installation Notes

- We do not recommend running Unicenter TNG login intercepts after running the Unicenter Integration and Migration Installation process. Once you run the Unicenter Integration and Migration Installation process successfully, you should verify that Unicenter TNG login intercepts are disabled.
- Unicenter Data Scoping rules (rules that target Unicenter TNG asset types with a -DT 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 for 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 that the CAUSECR.DLL file in the %CAIGLBL000%\BIN directory has not been replaced and is the same as the CAUSECR.DLL.EAC file in the *eTrustACDi*\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.

Note: For a complete list of Unicenter Integration features and how they work, see the *Administrator Guide*.

What's Next?

The chapter that follows presents answers to common questions about eTrust AC. Take a moment to read through the material, because it provides-at a glance-valuable information to further your knowledge about your new software.

Chapter 10: Frequently Asked Questions

In this chapter, we highlight some of the common security policy concerns and how eTrust AC simplifies UNIX, Linux, and Windows security management and enforcement. A graphical user interface centralizes control over security policies as well as the administration of users, groups, and system resources.

Q: What is eTrust AC?

A: eTrust AC is a software package that provides protection for UNIX, Linux, and Windows servers, and access management for system administrators.

Most traditional methods of protecting UNIX and Linux systems have focused on reacting to threats, assessing vulnerabilities, or trying to limit the ways to become root. Measures taken include running frequent audit reports, using shareware tools to reveal system vulnerabilities, and installing CERT-advisory patches, as supplied by the vendors.

eTrust AC was designed in recognition of the fact that stronger UNIX or Linux security requires a fundamental change in the way UNIX or Linux grants access to system resources. eTrust AC enables you to control access to different operating OS resource based on simple and easy configurable access rules. The result is an added layer of security, which resides right next to the protected data. The solution does not change the way UNIX or Linux operates or the way administrators do their jobs.

Q: Is eTrust AC the same on each supported platform?

A: Yes. The functionality of eTrust AC is equivalent on all supported platforms. All eTrust AC interfaces provide cross-platform administration, transparent to underlying OS differences (except during the initial configuration). Naturally, when the OS has different names for resources, eTrust AC maintains consistency with the native OS.

Q: What is the eTrust AC Dynamic Security Extension (DSX) technology?

A: The DSX technology is a dynamic interception of security related syscalls. The system call (or system vector) table stores memory address pointers to system call kernel code. eTrust AC stores these address pointers and then changes them to point to the corresponding eTrust AC code.

If the access is approved the request continues on to the original syscall code, if the access is denied then the request is terminated.

Q: Does eTrust AC intercept every event on the system?

A: No. Certain syscalls are intercepted by eTrust AC. Once a syscall is intercepted, the eTrust AC engine determines whether to allow or disallow access to the intercepted resource based on the eTrust AC rules that were defined in the database.

eTrust AC intercepts the initial access to a file or device but not the subsequent I/O events performed on the file (like read and write).

The same is true for network connections. eTrust AC intercepts the establishment of a network socket (that is, port-IP address pairing) but not the subsequent transfer of data.

eTrust AC does not intercept the routines that allocate memory to processes.

Q: What is the CPU overhead incurred in running eTrust AC?

A: This varies depending on the function of the host itself. A mail server typically has a lower performance penalty than a system hosting a database server.

Our customer experience, including high performance demand systems, has shown a typical performance range of 1-5% additional overhead on the CPU.

Q: Where are the access rules stored?

A: The eTrust AC access rules are stored in a protected database on the localhost.

Q: Does eTrust AC include an API?

A: Yes. In fact, eTrust AC includes a number of APIs that contribute to the eTrust AC open architecture. APIs can be used for everything from access control to administration to alert notification. The eTrust AC documentation explains in detail the usage of each API, and sample programs, written in C, are included with the software. eTrust AC APIs include:

- The **Authorization API** is used by applications to check user access to arbitrary resources. This set of API calls enables sites to centrally manage security with eTrust AC even for homegrown applications.
- The **Administration API** is used by applications that manage aspects of Windows, UNIX, or Linux security as handled by eTrust AC.
- The **Auditing API** allows customization of the eTrust AC audit.
- The **Password API** enables customization of password quality checks in addition to those provided in the product.

Q: Does eTrust AC provide encryption for network process communication?

A: Yes, eTrust AC encrypts all networked communication related to eTrust AC.

Q: What does eTrust AC protect?

A: eTrust AC protects the operating system and application resources that reside on the protected host. This is achieved by controlling access to system resources. The following is a brief listing of the types of resources that can be protected by eTrust AC, and the type of access controlled:

Files (generic and discrete)

Enhanced file access control protects files beyond operating system limitations. For example, a user not authorized to access a file is not able to do so even with root access. eTrust AC can also control *how* users may access files (that is, using which program or application).

Network connections

eTrust AC controls access to network services and ports by regulating incoming and outgoing network connections.

Processes

eTrust AC protects process from being killed by unauthorized users. Windows services are good candidates for this protection.

Userids and groupids (su)

UNIX only. eTrust AC can control surrogate userids and groupids. Knowing the password of another user is not sufficient to surrogate to a different uid.

Privileged programs

Programs that run with privileged authority are the primary source of backdoor and unauthorized access to system resources. eTrust AC protects the trusted base of privileged programs from modification and prevents the execution of new, unrecognized privileged programs.

SPECIALPGM

Some applications, such as programs or system services, require special eTrust AC authorization protection. SPECIALPGM protects specified programs by associating a logical user name (defined as a USER record in the eTrust AC database) with the user name required to run the program, authorizing only that logical user to run the programs.

Stack Overflow Protection (STOP)

STOP prevents hackers from using stack overflow exploits, which can enable them to execute arbitrary commands in order to break into systems.

Terminals

eTrust AC controls entry-points to system access by defining who can login from which terminals and under what conditions.

User-defined resources

Using the eTrust AC Authorization API and database tools, administrators can define site-specific rules for protecting access to data from applications that hook into the eTrust AC server.

Users and groups impersonation

Windows only. eTrust AC controls impersonation of users and groups. Knowing the password of another user is not sufficient to impersonate that user.

Windows Registry

Windows only. eTrust AC restricts a user's ability to access registry keys. You can give a user one or more types of access, such as READ, WRITE, and DELETE. The access can be specified with regard to an individual registry key or to a set of similarly named registry keys.

Q: Can eTrust AC protect resources from an attacker who gets root access?

A: Yes. In fact, this is one of the primary ways in which eTrust AC enhances UNIX and Linux security. In native UNIX, users with an id of zero (0) can effectively access all system resources. User passwords and file permissions are not only ineffective at protecting against users who successfully attack root, but the rules can be modified without leaving an audit trail.

Q: How does eTrust AC manage root capabilities?

A: The greatest security threat to UNIX and Linux lies in the existence of its superuser-root-as an all-powerful user-id accessible to various individuals in an organization. eTrust AC:

- Supervises access to root.
- Defines and limits what root can do.
- Corrects the exposure of root's unlimited powers.
- Shifts privileges to accountable individuals.
- Limits the damage that attackers can do through root access.
- No other security solution in the market provides this revolutionary capability.

Q: How are Root Responsibilities delegated on a need-to-use basis?

A: Administrators and operators need privileged root access in order to perform their job functions. Without eTrust AC, this is achieved on “all or nothing” basis by giving them the root Password. eTrust AC provides easy to apply rules to define “roles.” These roles delegate root capabilities to accountable users.

Q: Does eTrust AC file access control replace UNIX or Linux file permissions?

A: No, it enhances them. Native UNIX provides no file security against an attacker with root access and does not provide for securing files with a generic wildcard definition to determine and maintain access to groups of files.

eTrust AC provides complete file protection by intercepting every file access request and deciding if the user is authorized to access the file in the requested manner, according to its ACLs.

eTrust AC can protect the contents of entire directories, for example, `/etc/*` or `$DIR/webserver/ht-docs/*`. eTrust AC rules can also protect files such as `$HOME/*/.rhosts` thus protect all users' `.rhosts` files. You can also set a rule to protect a set of files with the same name: `/app/config*`. This would protect `/app/config.dat` and `/app/config.tar`, for example.

If the need arises to protect files that do not map into a directory or common naming convention, you can use the GFILE class. This class allows you to define specific files and apply a common set of access control rules to all of the files.

Additionally, with Program ACLs (PACLs), you can ensure that sensitive resources are only being accessed using approved programs. [For example, that personnel database files are only being written to using the database application.]. For operating systems that support native UNIX ACLs (Solaris and HP-UX), eTrust AC can synchronize eTrust AC ACLs with the operating system.

Q: How can I determine if a rule is too restrictive?

A: Simply enforcing the rule to watch for “hits” or denied access is impractical. For this reason, eTrust AC includes a Monitor-only mode called warning mode. Suppose that a user tries to access a resource that they do not have permission to access. If the resource is in warning mode, the access rule is not enforced (that is, the user can access the resource if the operating system allows it) but a special audit log entry is created which indicates that, under Enforcement Mode, the access would have been denied.

By examining the audit log entries for warned access to resources, it is possible to determine if the rule is too restrictive without actually enforcing it. This is particularly useful in developing new rules without the risk of breaking in an application that does surprising things within the OS.

Q: Is it possible to manage eTrust AC using both interface and batch processing?

A: Yes. The selang commandline interface can be used with both the Policy Manager (the administration interface) and with batch processing.

Q: What is the Policy Model?

A: The Policy Model is a simple, hierarchical mechanism for propagating access rules to multiple systems, and for creating models of access rule sets that have various hosts as subscribers. Each PMDB is a stand-alone eTrust AC database, which contains the same types of rules as an eTrust AC database associated with a specific host system. When rules are applied to the master PMDB, these rules are propagated to all of the subscribed databases that were defined for the master.

Q: Does eTrust AC allow for administration of both Windows and UNIX operating systems?

A: Yes. eTrust AC provides a powerful, intuitive GUI that enables the administrator to manage user accounts and resources in both Windows and UNIX from one central location.

Q: Do I need to add users twice: once to UNIX or Linux, and once to eTrust AC?

A: No. However, users who need to have explicit resource access control must appear in both environments. That is, they must be defined in native UNIX, and in the eTrust AC database. Using the Policy Manager interface, you can define or change definitions of both UNIX and eTrust AC users and groups.

Q: Does eTrust AC allow for administration of Windows operating systems as well as UNIX and Linux operating systems?

A: Yes. eTrust AC provides a powerful, intuitive GUI that enables the administrator to manage user accounts and resources in multiple operating systems from one central location.

Q: Does eTrust AC support Hardware-Based Authentication, such as SecureID?

A: eTrust AC is compatible with all authentication software, since it does not interrupt the authentication process.

Q: How does eTrust AC compare with firewalls?

A: Firewalls are used to limit network access to and from outside sources using networks, hosts, users, protocols, services, and applications. As businesses increase the level of network-based connectivity, more and more data needs to pass through the firewalls.

Once behind the firewall, servers and data are vulnerable. eTrust AC protects resources on a system behind a firewall, as well as those in the DMZ.

Q: If I have a firewall, why do I need eTrust AC?

A: A firewall is important to filter both incoming and outgoing network traffic. Well-configured firewalls can greatly reduce the number of curious users who might otherwise try to penetrate the system, and they can protect the information assets from being sent out over the Internet.

However, a firewall can do nothing to provide protection once a user is inside the network. In addition, firewalls can be, and have been, circumnavigated by clever crackers.

Q: What exactly does it mean that eTrust AC provides proactive security?

A: Most security solutions tend to provide methods that are reactive in nature. The history of computer security has proven these reactionary methods to be temporary fixes only, since the methods address the security symptoms at the application level. The design of eTrust AC is such that it addresses security events at the system and system call level.

This approach is taken because all resource access requests (application or other) are handled by the system and must go through the kernel. As a security sensitive request is made eTrust AC is able to intercept and disallow the request before it can become a threat.

Q: What advantages does eTrust AC have over the freeware security solutions in general?

A: Freeware solutions tend to be reactionary in nature. They address the symptoms and not the cause, supplying workarounds that are unprotected from root or system attacks.

A short list of the eTrust AC advantages over freeware:

- Self-protecting.
- Self-checking (rules database and services\daemons)
- Protects configuration files when it is running.
- Less administrative overhead for installation and maintenance.
- Vendor support.
- Provides a means for gradual implementation. eTrust AC has the concept of warning mode. Rules can be applied without enforcement so as not to impact business as usual.
- Provides a common solution as a super set of freeware solutions, and as a single point of administration for several machines and platforms.

Some of the more well-known host-based solutions are SUDO, auditing, Tripwire, and TCP wrappers. eTrust AC provides a functional superset of these solutions in a single package, addressing not the symptoms but the core issue by providing proactive security in the kernel.

Maybe the question to ask is, "If someone compromises the root account can the freeware solutions still provide protection?" The answer is no. These tools give a false sense of security. With eTrust AC the answer is yes, it can provide protection to key resources.

Q: How does eTrust AC compare with native file permissions?

A: Native file permissions only provide access for the owner, one group and the world as a whole with Read, Write, and Execute permissions. Native file access permissions can be over-ridden for any file by root access or the owner of that file.

eTrust AC extends the access modes beyond normal operating system access mode with access rights such as Update, Delete, Create, and more. eTrust AC access modes cannot be compromised by the file owner, or the root account. Where UNIX or Linux is limited to one group for access, eTrust AC can allow for several groups with different access rights.

eTrust AC also extends file access based on which programs are allowed to access files, something native UNIX or Linux does not provide.

Q: Can eTrust AC provide a 100% security solution?

A: No solution offering 100% security exists. However, eTrust AC can provide a comprehensive and more reasonable software solution that previously did not exist by addressing the causes of operating system security issues. Security aspects extend beyond software control and are addressed by establishing and following common sense policies concerning and including physical access and account sharing.

Q: I have heard about hackers using tools like "rootkit" to gain access to a machine. Can eTrust AC protect against these?

A: Rootkit has been around for a while and is one of many tools that have been used to gain unauthorized access to machines. It was not the first and most certainly will not be the last. To understand how eTrust AC addresses these issues, let's examine the goal and general profile of a hacker and his tools and how eTrust AC can address them.

The hacker's goal is to obtain full control of a system by seizing the root account. eTrust AC can respond to this by restricting who may become root, and how. In the event of unauthorized root access, eTrust AC can control what may be accessed.

The following helps illustrate how the hacker threat can be defended against:

Attack Profile	Hack Attack	eTrust AC Defense
A) Penetration	A1) Well known service flaws	A1a) Disable or limit access to valid remote sources
	A2) Accounts with bad passwords	A2a) Disable accounts with repeated attacks
		A2b) Limit sensitive accounts to local access
		A2c) Enforce Password Quality Control
B) Obtain root	B1) Flawed programs	B1a) Limit which programs allow root access
	B2) Guessing root password	B2a) Limit root to local access
		B2b) Limit who can become root, even if password is known
C) Retain root	C1) Alter existing priv programs	C1a) Protect privileged programs from tampering
	C2) Introduce new priv program	C2a) Protect system from the introduction of unauthorized privileged program.
	C3) Alter system log to hide penetration	C3a) Protect system logs from tampering
		C3b) Provide logging separate from system.

In addition, eTrust AC works with new eTrust technology called Stack Overflow Protection (STOP), which protects against stack overflow, or buffer overflow attacks, further strengthening the ability of eTrust AC to protect your system.