e*Index Global Identifier Product Suite

e*Index™ Security User's Guide

Release 5.0.5 for Schema Run-time Environment (SRE)

SEEBEYOND

The information contained in this document is subject to change and is updated periodically to reflect changes to the applicable software. Although every effort has been made to ensure the accuracy of this document, SeeBeyond Technology Corporation (SeeBeyond) assumes no responsibility for any errors that may appear herein. The software described in this document is furnished under a License Agreement and may be used or copied only in accordance with the terms of such License Agreement. Printing, copying, or reproducing this document in any fashion is prohibited except in accordance with the License Agreement. The contents of this document are designated as being confidential and proprietary; are considered to be trade secrets of SeeBeyond; and may be used only in accordance with the License Agreement, as protected and enforceable by law. SeeBeyond assumes no responsibility for the use or reliability of its software on platforms that are not supported by SeeBeyond.

This work is confidential and proprietary information of SeeBeyond and must be maintained in strict confidence.

Version 20050127113609

Table of Contents

Chapter 1

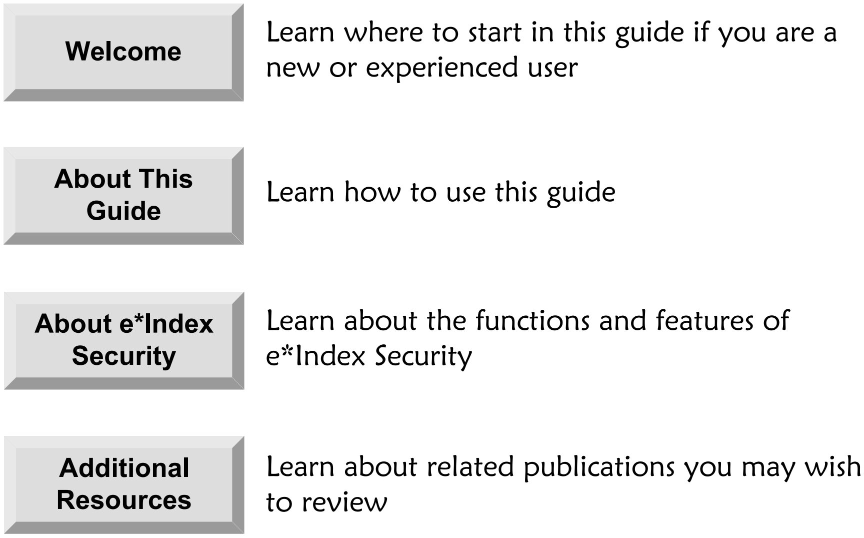
Introduction

About this Chapter

Overview

This Introduction welcomes new and experienced e*Index™ Security users and explains how to use this guide. e*Index Security provides security functions to the suite of e*Index products. This document describes the user interface for SeeBeyond’s e*Index Security.

The following diagram illustrates the contents of each major topic in this chapter.



Welcome Learn where to start in this guide if you are a new or experienced user

About This Guide Learn how to use this guide

About e*Index Security Learn about the functions and features of e*Index Security

Additional Resources Learn about related publications you may wish to review

Welcome

Welcome to e*Index Security, SeeBeyond's security module to e*Index™. Global Identifier. e*Index Security allows system administrators to control user and user group access and permissions to all program functions of e*Index. With e*Index Security, access is broken down into various levels of authority and can be limited to authorized operators and users. Access to applications can also be limited according to a set of defined authorization privileges set up by the system administrator.

To New Users

If you are new to e*Index Security, you should browse through this guide before you begin to use the software. Please pay particular attention to the overview sections provided at the beginning of each chapter and at the beginning of each section within a chapter. The overview sections provide background and explanatory information you may need to understand. After reading the overview information, you will be ready to perform specific tasks using the step-by-step instructions provided in each chapter.

To Established Users

If you are a more advanced e*Index Security user, you may prefer to use this guide as a quick reference to find information about forgotten or unfamiliar tasks. If you know what you need to do, but can’t remember exactly how to do it, you can easily find what you need in the Table of Contents. Or, you can browse through the guide and find the appropriate step-by-step procedure by scanning headings and instruction titles.

About this Guide

What is the Purpose of this Guide?

This guide provides the information you need to quickly get started with e*Index Security. It includes navigational instructions, functional instructions, and background information about the application's features. This guide also provides the information you need to maintain information about user profiles, user groups, and access permissions.

What is the Scope of this Guide?

This guide provides step-by-step instructions for all of the functions of e*Index Security, such as adding user and user group information, assigning and revoking security permissions, and maintaining security information. It also includes information on specifying system parameters.

This guide does not include information or instructions on using the e*Index or e*Index Administrator applications, working with Monk APIs for e*Index, or installing any e*Index applications. These topics are covered in the appropriate user's guide.

Who Should Use this Guide?

Any user who will add or maintain user profiles or user groups, or who will assign access privileges to the users of any e*Index application should read this guide. Intermediate or advanced users who need a refresher on using some of the basic functions of e*Index Security should also read this guide. A thorough knowledge of e*Index Security is not needed to understand this guide.

How Should this Guide be Used?

For best results, you should skim through the guide to familiarize yourself with the locations of essential procedures you need to perform. Each chapter begins with a simple graphic that identifies the information contained in the chapter. Each chapter contains instructions for performing e*Index Security procedures preceded by background information that will help you perform each procedure.

How is this Guide is Organized?

This guide is divided into four chapters and one appendix that cover the topics shown below.

Chapter	Topics
Chapter 1, Introduction	■ Welcome ■ About this Guide ■ About e*Index Security ■ Additional Resources
Chapter 2, Getting Started	■ Accessing e*Index Security ■ Learning About the e*Index Security Interface ■ Getting Help ■ Exiting e*Index Security
Chapter 3, Setting Up Security	■ Learning About Security Tasks ■ Establishing Security ■ Assigning Event Notification
Chapter 4, Maintaining Security Information	■ Learning About Security Maintenance ■ Maintaining User Profiles and User Groups ■ Maintaining User Access and Notification ■ Configuring Security Parameters
Appendix A, Access Permission Definitions	■ e*Index Global Identifier Access Permissions ■ e*Index Administrator Access Permissions ■ e*Index Security Access Permissions

What Conventions are Used in this Guide?

Before you start using e*Index Security, it is important to understand the typographic, icon, special notation, and other conventions used in this guide.

Typographic Conventions

The following typographic conventions are used in this and other e*Index publications.

Item	**Convention**	**Example**
Book titles	Title caps, italic	See the *e*Index Administrator User's Guide*
Button names, key names, and key combinations	Bold	**Save** button **F1** key **Alt+Shift+V** key combination
Chapter titles (and section titles within chapters)	Title caps, in quotation marks	See Chapter 2, “Getting Started” See “Modifying a User Profile” later in this chapter
Menu names and commands	Bold, capitalization is identical to the interface	**Functions** menu **Action** menu **Save** command
Messages	Bold	**Data has been saved.**
New terms	Italic	A *user profile* is a set of information that describes the characteristics of someone who accesses any e*Index application.
Window, page, and dialog titles	Title cap	User and Group Maintenance window Print dialog

Icon and Special Notation Conventions

The following conventions are used in this and other e*Index publications to identify special types of information.

Icon or Notation	Type of information
Note	Supplemental information that is helpful to know, but not essential to completing a particular task.
Tip	Information that helps you to apply techniques and procedures described in the text to your specific needs. May also suggest alternative methods.
Important!	Information that is essential to the completion of a task.
Caution!	Advises you to take specific action to avoid loss of data.
▶	Indicates the beginning of a step-by-step instruction.
✓	Specifies a task to perform before you begin a step-by-step instruction.
ℹ	Indicates a cross-reference to other sections of the guide or to other publications.

Mouse Conventions

You can use either a single-button mouse or a multiple-button mouse with e*Index Security. If you use a multiple-button mouse, the left mouse button is the primary button, unless the mouse is configured differently.

The instructions in this guide may require you to use the mouse in a variety of ways:

- **Point** means to position the mouse pointer until the tip of the pointer rests on whatever you want to point to on the screen.
- **Click** means to press and then immediately release the left mouse button without moving the mouse.
- **Double-click** means to click the left mouse button twice, in rapid succession.
- **Right-click** means to click the right mouse button once.
- **Drag** means to point and then hold down the mouse button as you move the mouse. **Drop** means to let go of the mouse button to place the dragged information where you want it to be moved.
- **Move** means to point to an object on the screen, such as an e*Index window, and drag the mouse to move the object to a screen location of your choice.
- **Highlight** means to select an area of text by dragging the mouse over the desired portion of text that appears on a window.
- **Select** means to point to a list of information on an e*Index window, and then click once to choose the data you want. The information becomes highlighted when selected.
- **Expand** means to double-click a row of information on an expandable list to display more details. The details appear on another row, below the row you double-click.
- **Collapse** means to double-click a row of information on an expandable list to hide the details that appear on the following row.

Field Description Conventions

This guide explains how to perform certain tasks and describes the fields that appear on the e*Index Security windows that you use to accomplish those tasks. Field descriptions appear at the end of most procedures, and are referenced by topic name from the step in which you are required to modify field values. For example:

> **3** On the Security Wizard toolbar, click **Edit**. The Edit Access Privileges window appears (for more information, see "About Edit Access Privilege Fields" following this procedure).

This step identifies the name of the topic that describes the fields you need to use

Each field description topic identifies and describes the fields you need to use first. If applicable, a description of display-only fields that appear on the window is also provided. For example:

Fields you need to use to complete the procedure

In this field …	type or select …
Name	The name of the user group. No default
Effective Date	The first date that a user profile assigned to this user group can access the components to which the group has been granted access. Default: today's date

Fields you need to use to complete the procedure

Select this check box …	to specify that …
User must change password at next login	The next time the user logs on to any e*Index applications, they must change their user password.

Display-only fields you may encounter while performing the procedure

This field or column …	displays this information …
Create Date	The date on which the selected user group was created.

About e*Index Security

Overview

This section of the chapter provides background information about the features of e*Index Security.

What is e*Index Security?

e*Index Security provides secure access to your e*Index database by restricting access through user login and password activities. You can restrict access by application functions, individual actions, windows within functions, user ID, and so on. e*Index Security also provides predefined categories that you can assign to users to grant them automatic access permissions. Assigning a category to a user can give them certain characteristics, such as the ability to be assigned access permissions that are not assigned to the user group to which they belong.

What are the Features of e*Index Security?

e*Index Security provides three primary functions to help you set up and manage security for e*Index:

- **Access Setup**
  The Access Setup function allows you to create and maintain user profiles and user groups, assign user profiles to user groups, expire user profiles from user groups, and grant access permissions to (or expire them from) user profiles and user groups.

- **Event Notification Setup**
  The Event Notification Setup function gives you the ability to specify that certain users receive an e-mail notification when certain transactions occur in the e*Index GUI. For example, an administrator may want to be notified via e-mail if two member profiles are merged from the e*Index GUI.

- **Control Key Maintenance**
  Control Key Maintenance allows the system administrator to configure a set of system parameters, known as *control keys*, for e*Index Security. System parameters include automatic password expiration, minimum password length, password histories, and a time-out feature.

What is Security Management?

Security management consists of several tasks that allow you to define secure access to the e*Index GUIs. The primary tasks of security management are creating user profiles, creating user groups, and assigning them access permissions.

You give e*Index users the ability to use certain functions of e*Index by granting *access permissions* to the user's profile. An access permission is the ability to perform a specific action in the e*Index GUIs. For example, if you assign a user the **Add Person** access permission, that user is able to create new member profiles using the e*Index GUI. You can also grant the same access permissions to a group of users by creating a user group, granting the group the appropriate access permissions, and then assigning user profiles to the user group.

Additional Resources

SeeBeyond has developed a suite of e*Index user's guides and related publications that are distributed in an electronic library.

- *e*Index Global Identifier User's Guide*
Helps e*Index quality workstation users to perform database maintenance tasks, such as merging and unmerging records, finding and resolving potential duplicates, adding and updating records, and viewing the audit trail.

- *e*Index Administrator User's Guide*
Helps system administrators configure system parameters, customize e*Index, work with Vality rule set files, and processing codes. This guide also describes how to maintain the information in the database that is used to populate the drop-down lists in the e*Index.

- *e*Index Global Identifier Technical Reference*
Describes message processing for e*Index, as well as database tables and e*Index Monk APIs. This guide also provides a complete listing of e*Index Monk APIs and functions, along with a description, parameters, syntax, return values, and examples for each.

- *e*Index Initial Load User's Guide*
Provides the background information and instructions that system and database administrators need in order to load legacy data into the e*Index database, including a description of the expected data format and the schema files included with the load program.

- *Working with Reports for e*Index Global Identifier*
Provides background information about the GUI and standard reports provided with e*Index, and explains how to modify and run the standard reports (for an Oracle installation only).

- *e*Index Global Identifier Installation Guide*
Helps system and database administrators install a new e*Index environment for the current release, including e*Index schema files, the e*Index GUI, and database installation.

- *e*Index Global Identifier Upgrade Guide*
Helps system and database administrators upgrade an existing e*Index environment to the most current release, including e*Index schema files, the e*Index GUI, and database upgrades.

- *Java Programmer's Guide for e*Index Active Integration*
Provides background and implementation information about the Java APIs for e*Index Active Integration. This guide also provides a complete listing of e*Index Java functions, along with a description, parameters, syntax, return values, and examples for each.

Getting Started

About this Chapter

Overview

This chapter helps you become familiar with the basics of e*Index Security and includes instructions and information that help you to put e*Index Security to work quickly.

The following diagram illustrates the contents of each major topic in this chapter.

Access e*Index Security	Learn how to log on to e*Index Security
About the GUI	Learn about the GUI front end of e*Index Security, including toolbars, menus, and windows
Help Features	Learn about the various help features of e*Index Security
Exit e*Index Security	Learn how to log off e*Index Security

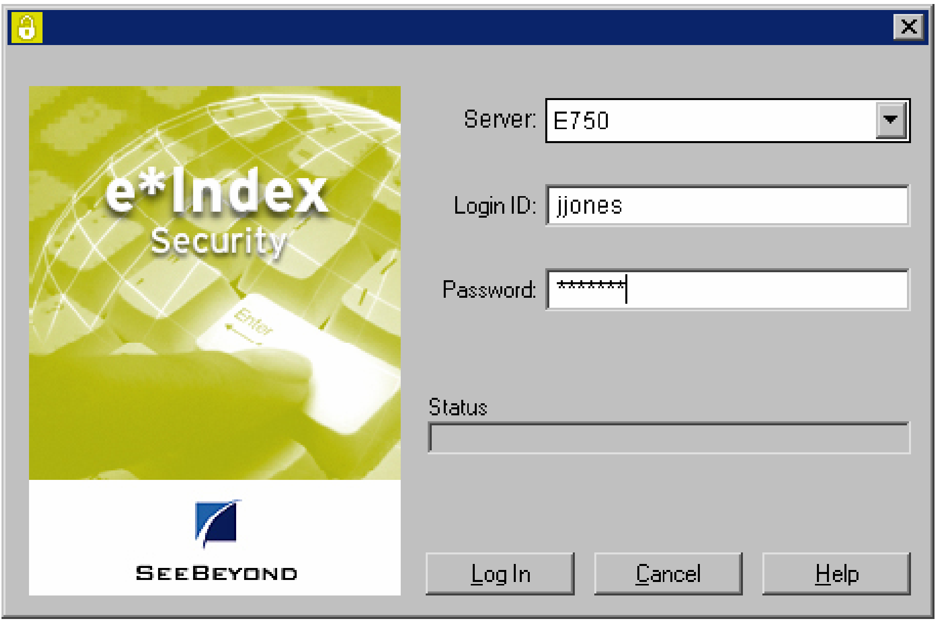
Accessing e*Index Security

Overview

This section of the chapter provides the instructions you need to get up and running with e*Index Security.

Logging on to e*Index Security

Before you can use e*Index Security, you must first specify your user ID, password, and perhaps other information such as the database you want to use.



Server: E750

Login ID: jjones

Password: *******

Specify your log-on information on the e*Index Security Login window

▶ To log on to e*Index Security

Before you begin:

✓ Make sure you have a user ID and password for e*Index Security

e*Index Security icon

1 To access e*Index Security, double-click the e*Index Security icon on the workstation desktop. This launches e*Index Security, and the e*Index Security log on window appears.

2 In the Server field, select the name of the e*Index database you want to access.

> ***Note:*** *Only databases that are defined in the e*Index initialization file, **stc_ua.ini**, appear in the drop-down list for this field. See your System Administrator if you need a database added to the list.*

3 Enter your login ID and password in the appropriate fields.

Log In

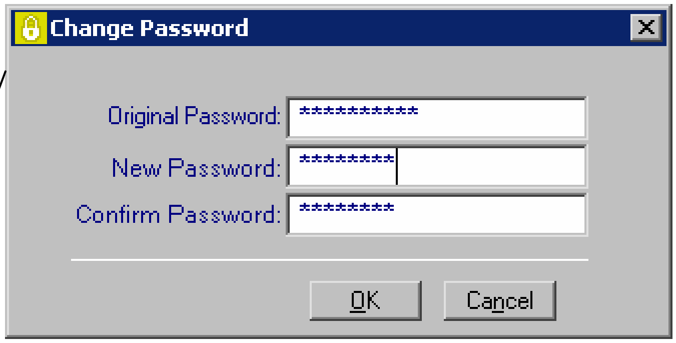
Log In button

4 In the lower portion of the login window, click **Log In** or press the **Enter** key. The e*Index Security Main window appears.

Changing Your Password

Once you log on to e*Index Security, you may need to change your password for various reasons. For example, your System Administrator may configure a specific period of time after which you must change your password. The administrator may also configure the application to require that you change your password the first time you log on to the system.

> ***Tip:*** *You should change your password periodically. The recommended frequency for your organization is based on internal security procedures. You can change your password at any time.*



Original Password: **********

New Password: ********

Confirm Password: ********

Change Password dialog

▶ To change your password

Before you begin:

✓ Determine the new password you want to use

Change Password tool

1 On the Primary Toolbar, click **Change Password**. The Change Password dialog appears.

2 On the Change Password dialog, fill in the password fields (for more information, see "About Password Fields" following this procedure).

OK button

3 On the Change Password dialog, click **OK**. A confirmation dialog appears.

OK button

4 On the confirmation dialog, click **OK**. The new password is saved to the database.

About Password Fields

The password fields, located on the Change Password dialog, allow you to change your existing password to a new password.

In this field ...	type or select ...
Original Password	The password you currently use to log on to the e*Index applications. No default ***Important:*** *The password you enter here must match the case of the password you used to log on. For example, if you logged on with a password of* ***c5RT3p****, you cannot enter* ***c5rt3p*** *in this field; you must enter* ***c5RT3p****.*
New Password	The new password you want to use to log on to e*Index. No default ***Tip:*** *Passwords may not be common words or names.*
Confirm Password	The same password you typed in the **New Password** field. No default

Learning About the e*Index Security Interface

Overview

This section of the chapter provides background information about the user interface of e*Index Security, the windows you will use, and common menu options.

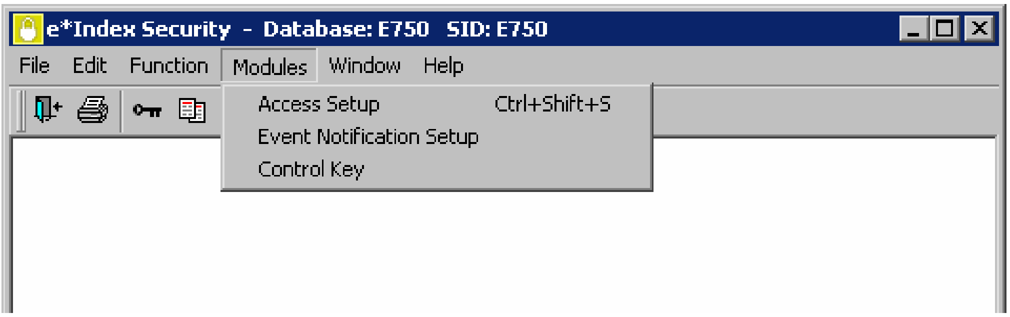
About the Basic Design

e*Index Security was designed specifically to restrict access to the e*Index applications. e*Index Security allows system administrators to control user access, user group access, and permissions to all program functions of the e*Index applications. With e*Index Security, access can be restricted using various levels of authority. Access can also be restricted according to the authorization privileges set up by the system administrator.

About the Graphical User Interface (GUI)

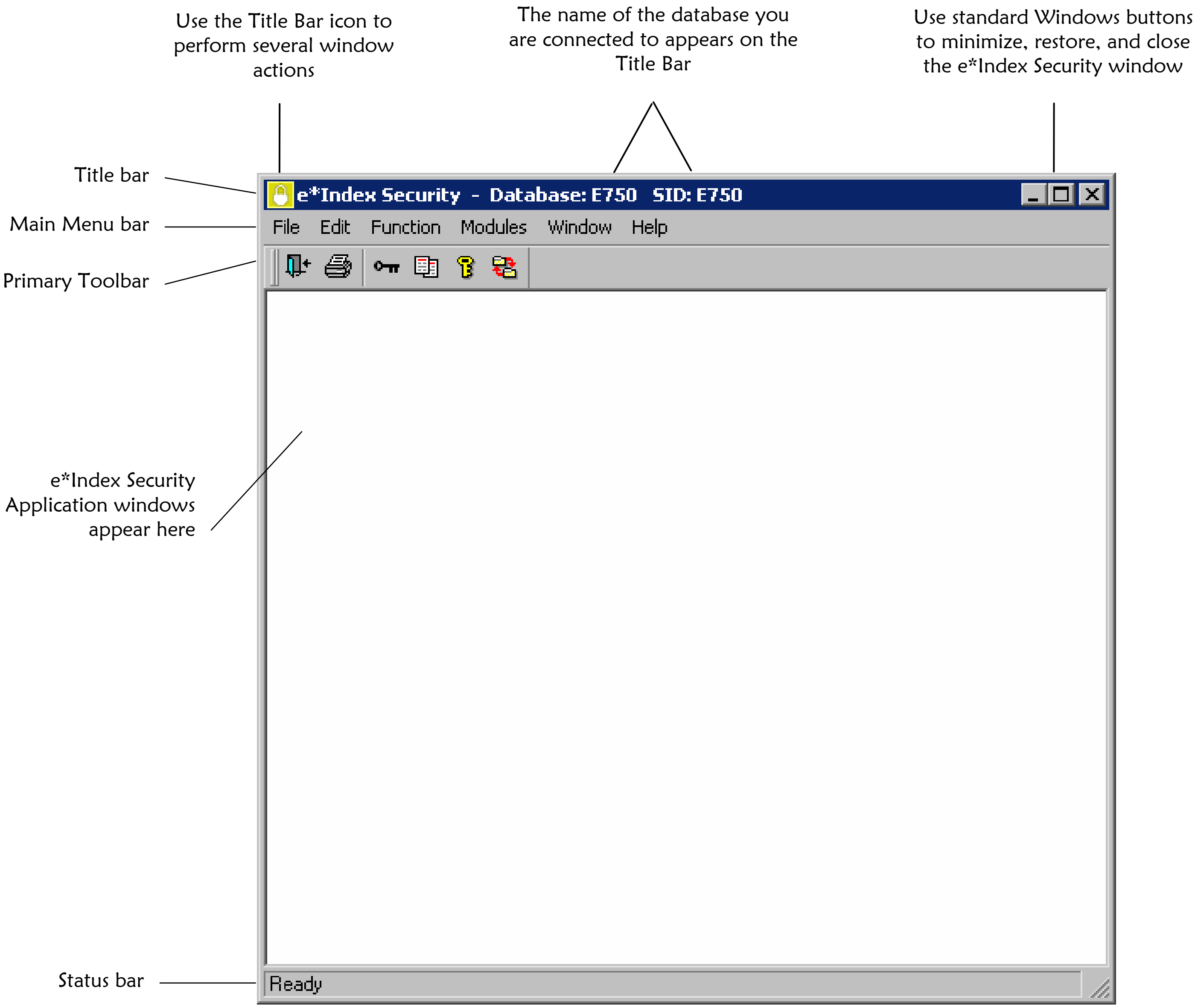
The design of the user window follows a standard Microsoft Windows progression based on user functionality. The application includes standard graphical elements, such as windows, dialog boxes, drop-down menus, action buttons, and icon tools. Several windows in e*Index Security display entities in a tree-view, similar to Microsoft Explorer. Click any word on the Main Menu to display a drop-down menu with a list of commands from which you can choose.

The Main Menu, with the Modules drop-down menu displayed


e*Index Security - Database: E750 SID: E750
File
Edit
Function
Modules
Window
Help
Access Setup Ctrl+Shift+S
Event Notification Setup
Control Key

What is the e*Index Security Main Window?

The e*Index Security Main window is the first window that appears when you log on to e*Index Security. This window consists of the e*Index Security Main Menu bar, the Primary Toolbar, and several standard Windows graphic elements.



Use the Title Bar icon to perform several window actions

The name of the database you are connected to appears on the Title Bar

Use standard Windows buttons to minimize, restore, and close the e*Index Security window

Title bar

Main Menu bar

Primary Toolbar

e*Index Security Application windows appear here

Status bar

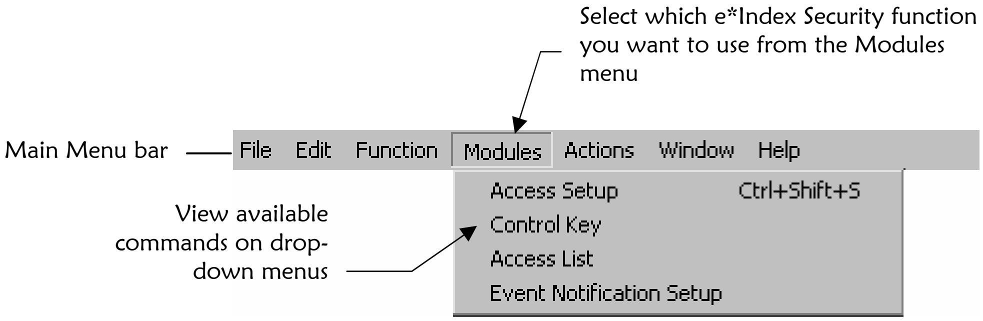
The e*Index Security window is the first window that appears when you log on.

About the Main Menu

The Main Menu bar lists the names of six drop-down menus (File, Edit, Function, Modules, Window, and Help) from which you can perform a variety of functions. When you select a menu from the Main Menu bar, the available commands appear on drop-down menus. The most frequently used menu is the Modules menu, where you can choose which security function to perform.

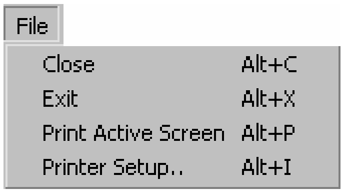
When you access a function from the modules menu, the Main Menu bar lists an additional drop-down menu, named **Actions**, with commands specific to the active window.

Once you display a drop-down menu, you can select an option from the menu by clicking it with your mouse or by pressing the underlined letter of the command on your keyboard.


Select which e*Index Security function you want to use from the Modules menu
Main Menu bar
File
Edit
Function
Modules
Actions
Window
Help
View available commands on drop-down menus
Access Setup Ctrl+Shift+S
Control Key
Access List
Event Notification Setup

About the File Menu

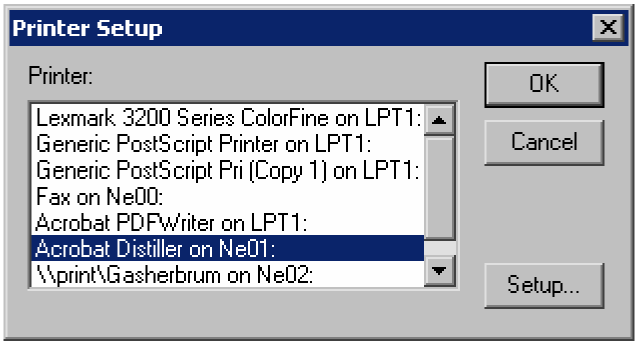
The *File Menu* on the Main Menu contains standard Windows options, such as Close, Print Active Screen, Print Setup, and Exit.



- **Close**
  The *Close* option closes the current open window, and returns to the previous open window or the e*Index Security main window.

- **Print Active Screen**
  The *Print Active Screen* option allows you to print the current active window. This option becomes very useful when referencing a particular window.

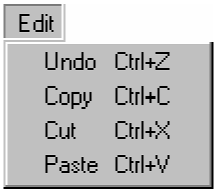
- **Print Setup**
  The *Print Setup* option allows you to select or set up a printer for the current active session.


Printer Setup
Printer:
Lexmark 3200 Series ColorFine on LPT1:
Generic PostScript Printer on LPT1:
Generic PostScript Pri (Copy 1) on LPT1:
Fax on Ne00:
Acrobat PDFWriter on LPT1:
Acrobat Distiller on Ne01:
\\print\Gasherbrum on Ne02:
OK
Cancel
Setup...

- **Exit**
  The *Exit* option terminates the application and returns to the Windows Desktop.

About the Edit Menu

The options available in the *Edit Menu* allow you to undo the most recent action and to copy, cut, and paste information.



- **Undo**
  Use this command to undo the most recent action (cut, copy or paste) and return to the previous status.

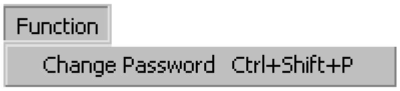
- **Copy**
  This command copies the contents of the highlighted field to the clipboard.

- **Cut**
  This command removes the contents of the highlighted field and places them on the clipboard.

- **Paste**
  This command places the contents of the clipboard into the field that is currently highlighted.

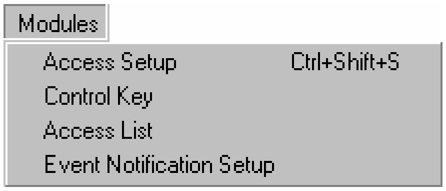
About the Function Menu

The option available on the *Function Menu*, Change Password, allows you to change your log on password for all e*Index applications. You can change your password at any time.



About the Modules Menu

The options available on the *Modules Menu* allow you to access the primary functions of e*Index Security.



- **Access Setup**
  This command opens the User and Group Maintenance window, where you can create and maintain user profiles and user groups, and assign user profiles to user groups or expire user profiles from user groups.

- **Control Key**
  This command opens the Control Key Maintenance window, where you can configure e*Index Security using a set of parameters known as *control keys*. These keys control the length of time a session of e*Index Security can be inactive before automatically shutting down, the minimum password length, password histories, and whether passwords must be changed after a specified period of time.

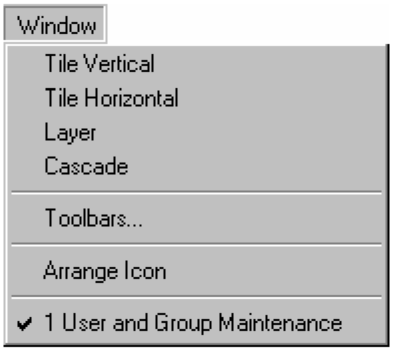
- **Access List**
  Use this command to grant access permissions to users and user groups. Once you assign access permissions to a user group, you can assign user profiles to that user group to grant those users the same access permissions. This menu option only appears on the Modules Menu when the User and Group Maintenance window is active.

- **Event Notification Setup**
  Use this command to specify that certain users are notified by e-mail when specific transactions occur in the e*Index GUI. For example, you

can specify that a user receive an e-mail notification whenever two user profiles are merged from the e*Index GUI.

About the Window Menu

The *Window Menu* contains standard commands available with most Windows applications. These commands allow you to customize the appearance of your e*Index Security windows and toolbars for the current session.



- **Tile Vertical**
  The *Tile Vertical* option arranges open windows vertically.

- **Tile Horizontal**
  The *Tile Horizontal* option tiles all open windows horizontally.

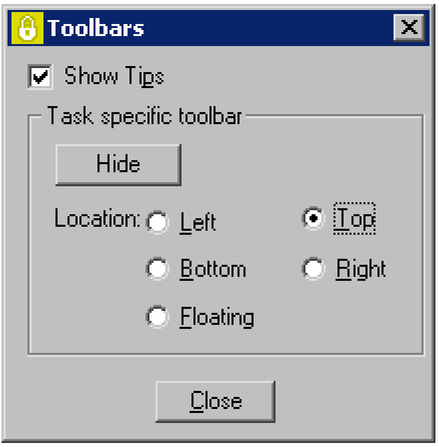
- **Layer**
  The *Layer* option returns the current active window to its original size.

- **Cascade**
  The *Cascade* option displays all open windows in a descending cascade.

- **Arrange Icons**
  The *Arrange Icons* option arranges the icons at a set interval across the window.

- **Toolbars**
  The *Toolbars* option allows you to customize your display options for the e*Index Security toolbars and icons. You can define where to place your toolbars and whether to display balloon help or descriptive text along with each toolbar button.

▶ To customize your toolbar options



Use the Toolbars dialog to modify the appearance and location of your toolbar

1 From the Main Menu, select **Window**, and then select **Toolbars**. The Toolbars dialog appears.

2 Do one of the following:

*To display the toolbar on the left side of the e*Index Security window*, click the **Left** option.

*To display the toolbar at the top of the e*Index Security window*, click the **Top** option.

*To display the toolbar on the right side of the e*Index Security window*, click the **Right** option.

*To display the toolbar at the bottom of the e*Index Security window*, click the **Bottom** option.

To display the toolbar such that you can move it around the window, click the **Floating** option.

3 To display descriptive text for an icon only when you pass the mouse pointer over it, select the **Show Tips** checkbox.

Hide button

4 To remove the toolbar from view, click the **Hide** button.

Show button

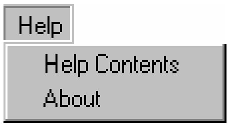
5 To make the toolbar visible when it is hidden, click the **Show** button.

Close button

6 When you complete your changes, click **Close**.

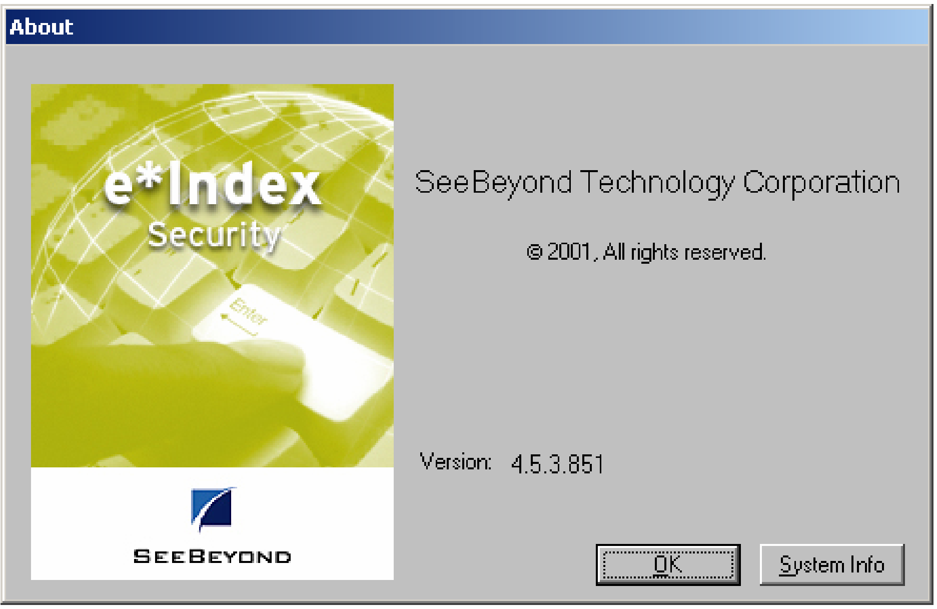
About the Help Menu

The *Help Menu* allows you to access e*Index Security online help and system information, including version number and copyright information.



- **Help Contents**
  The *Help Contents* option displays the e*Index Security online help system to assist you in performing security functions.

- **About**
  The *About* option displays the About information dialog. Click **System Info** on this dialog to display the operating system, CPU type, resolution, database, database server, e*Index Security version and build numbers, and the PowerBuilder version. Click **OK** to close the information dialogs and return to the Main Menu.

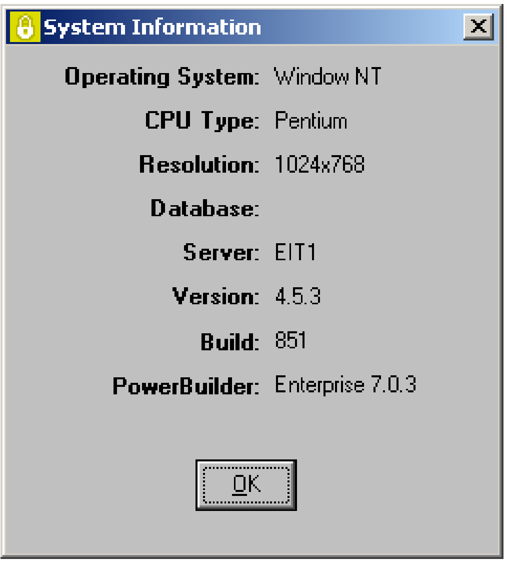

About information dialog

About

SeeBeyond Technology Corporation

© 2001, All rights reserved.

Version: 4.5.3.851



Operating System: Window NT

CPU Type: Pentium

Resolution: 1024x768

Database:

Server: EIT1

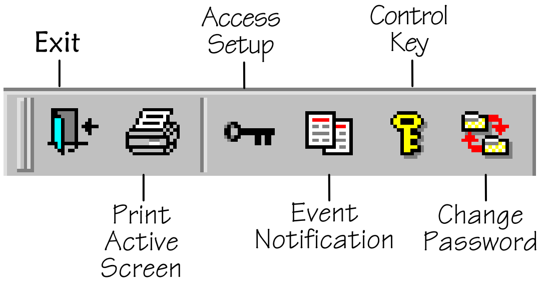
Version: 4.5.3

Build: 851

PowerBuilder: Enterprise 7.0.3

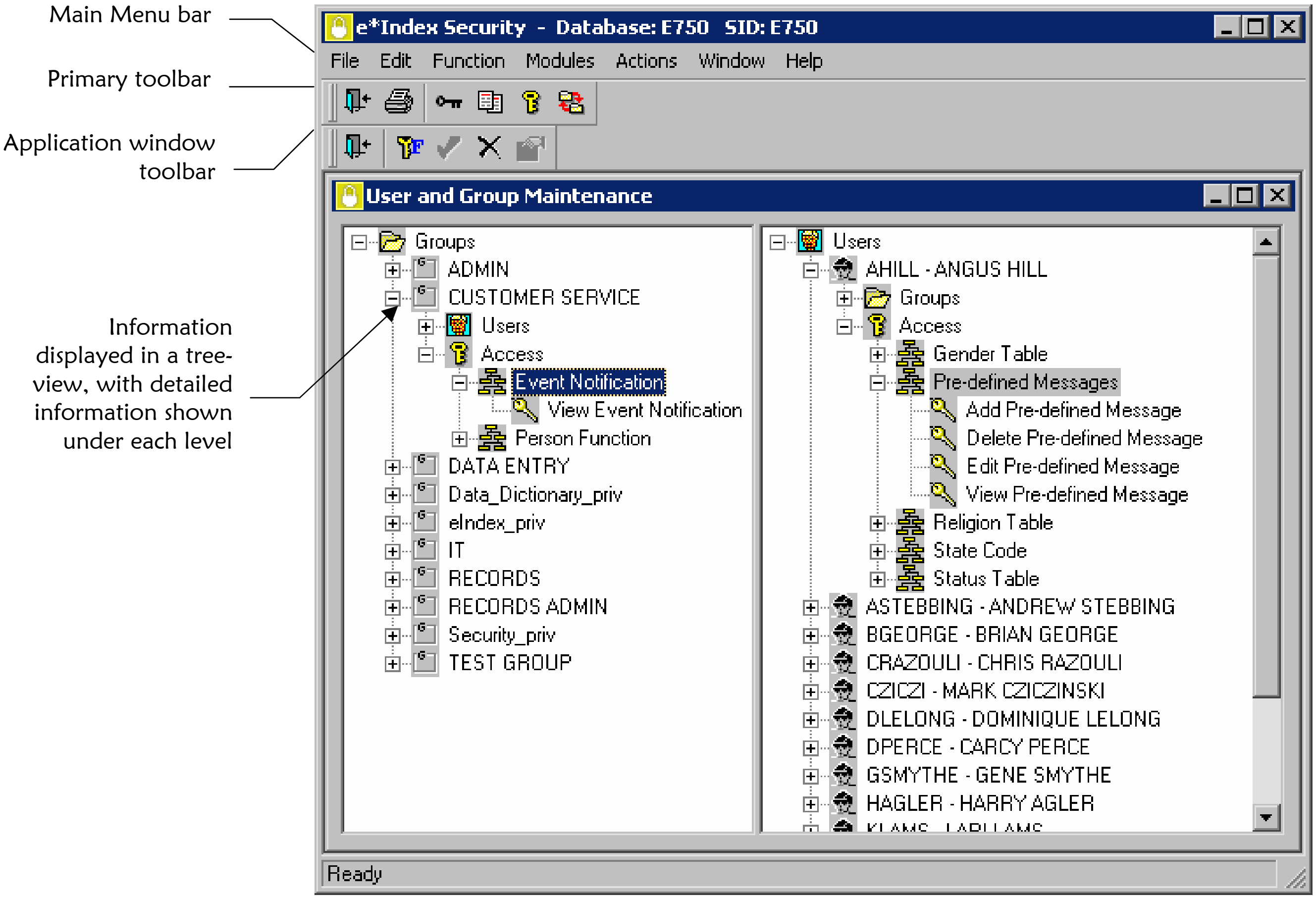
About the Primary Toolbar

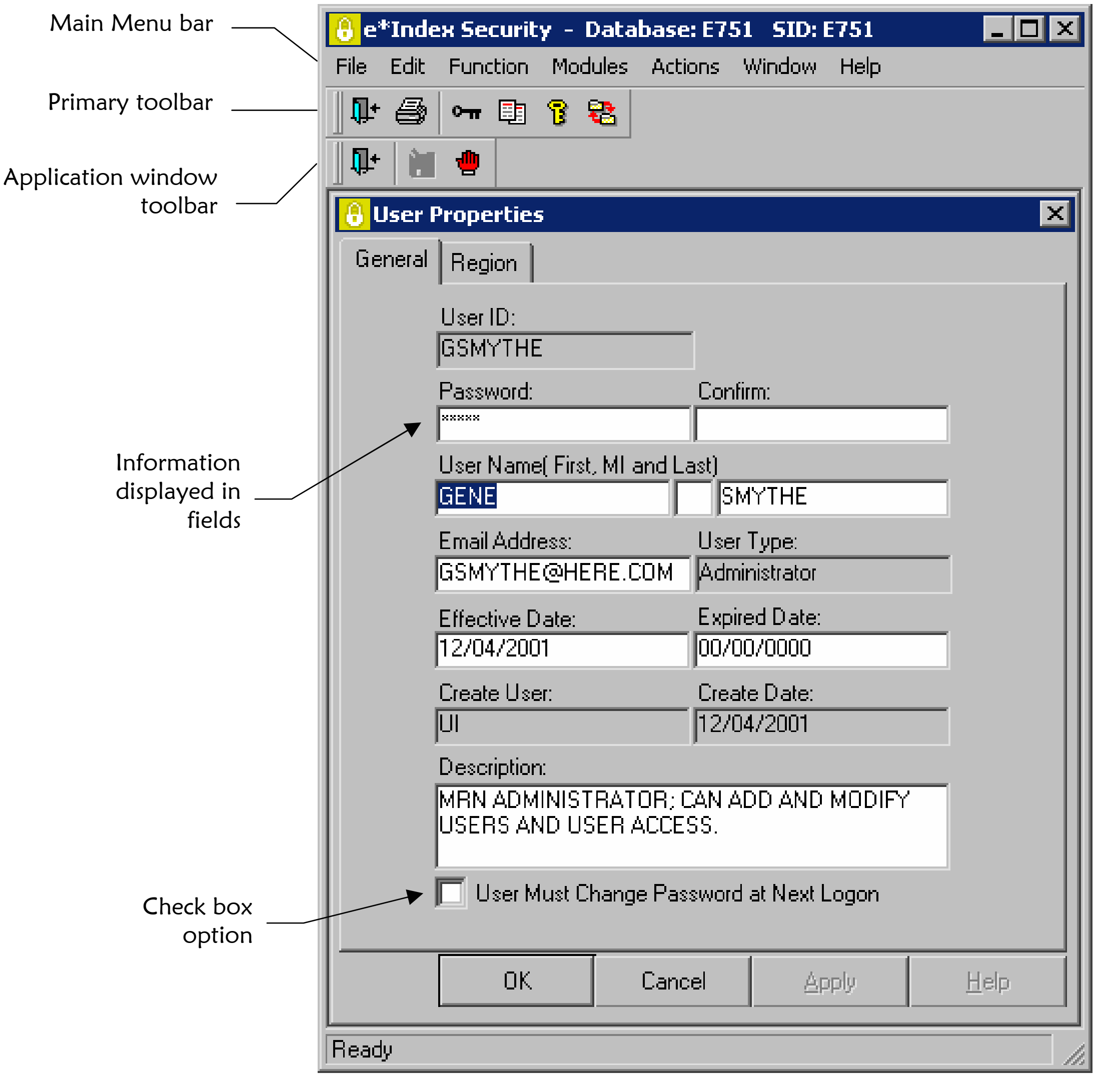
The *Primary Toolbar* gives you quick access to the most frequently used e*Index Security functions. This toolbar is located just below the Main Menu, and includes a set of buttons, or *tools*, to help you quickly access frequently used functions and modules. Since this toolbar is visible at all times, you can access these tools at any time. Depending on which function you access, another toolbar specific to that function appears under the Primary Toolbar. A description of each icon tool on the Primary Toolbar appears below.



What are Application Windows?

There are numerous *application windows* in e*Index Security that you use to perform specific functions. For example, you display the User and Group Maintenance window to view a list of current users and groups, but you display the User Properties window to modify information about a user. There are two different types of application windows. One type displays information in a tree-view; the second type displays information in fields.





User ID: GSMYTHE

Password: ***** Confirm:

User Name(First, MI and Last) GENE SMYTHE

Email Address: GSMYTHE@HERE.COM User Type: Administrator

Effective Date: 12/04/2001 Expired Date: 00/00/0000

Create User: UI Create Date: 12/04/2001

Description: MRN ADMINISTRATOR; CAN ADD AND MODIFY USERS AND USER ACCESS.

☐ User Must Change Password at Next Logon

Several components may appear on an application window.

- **Main Menu**
  The *Main Menu* is located at the top of the application window, and is visible in all application windows. This menu displays the functions available to e*Index Security.

- **Primary toolbar**
  The *Primary toolbar* is located just below the Main Menu, and is visible in all application windows. Use the tools on the Primary toolbar to access the primary functions of e*Index Security.

- **Application window toolbar**
  The *application window toolbar* is unique to each application window, and contains tools for various functions that you can perform from the active application window.

- **Tree list**
  Some application windows contain a *tree list*. This list is similar to Windows Explorer in that you can expand displayed levels to view information contained within each level.

- **Fields**
  Some application windows contain *fields* instead of a tree list. Fields allow you to add, modify, and delete information about specific entities in e*Index Security.

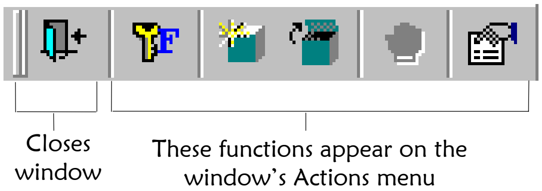
About Application Window Menus

Whenever an application window appears, the Main Menu changes slightly to accommodate the functions available on the application window. When you access an e*Index Security function, the following menu is added to the Main Menu:

- **Actions Menu**
  The *Actions menu* contains a set of action commands that are unique to each application window. There are three categories of commands on the Actions menu: User, Group, and Access. Commands are only enabled when they apply to the active application window. The Actions menu appears on all windows accessed by the Modules menu, such as the User and Group Maintenance window, the Access List window, and the Event Notify window.

About Application Window Toolbars

Every application window has a unique toolbar, which is located directly below the primary toolbar. Application window toolbars contain tools for various functions you can perform from the active application window. The tools generally include functions from the Actions menu.



This section does not include a description of each application toolbar, but you can easily determine the function of each toolbar button by passing the mouse pointer over a button to view balloon help. Balloon help specifies the function of each button (see "Using Balloon Help" later in this chapter).

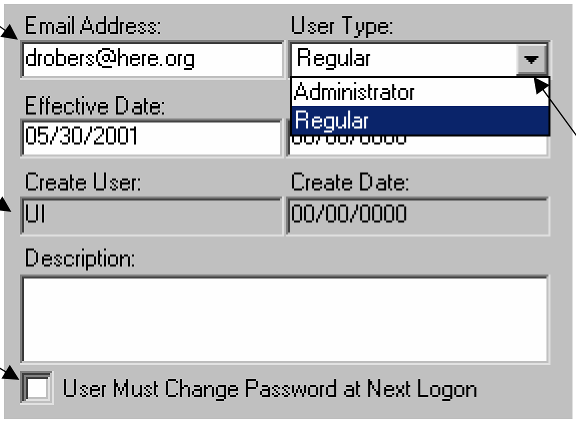
About Fields

Information that you work with in e*Index Security is contained in *fields.* There are several different types of fields on the e*Index Security windows. The field types are entry, display-only, drop-down list, and check box. You cannot change or enter information into display fields, which are indicated by gray shading. You can type information into entry fields and select values from a list in fields with drop-down lists, but you can only view information in display-only fields. You can also select check-box options.

You can type into entry fields, ...

... you can only view information in display-only fields...

... you can select check box options...



Email Address: drobers@here.org

User Type: Regular

Effective Date: 05/30/2001

Create User: UI

Create Date: 00/00/0000

Description:

□ User Must Change Password at Next Logon

... and, you can select an item from a drop-down list of options

Getting Help

Overview

e*Index Security provides several user assistance tools to help you look up the information you may need to help you perform your tasks. The available user assistance tools include online help, balloon help, and online documentation.

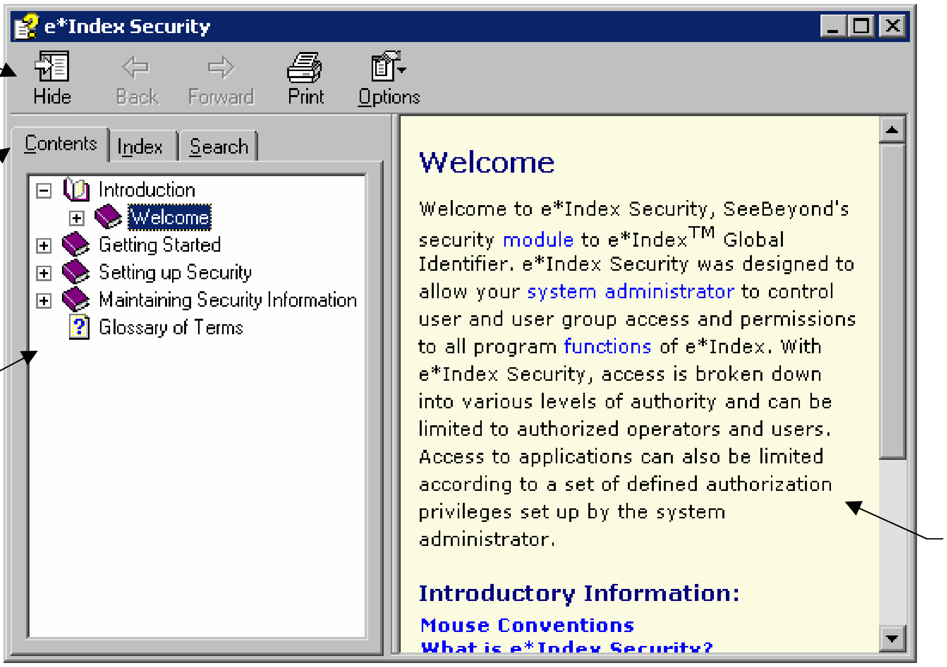
Using Online Help

The online help system provides background information and step-by-step instructions on performing the necessary functions of e*Index Security. The help system is provided in HTML format.

Note: *Internet Explorer 3.02 or higher is required in order to view online help.*

▶ To view online help

1 On the Main Menu, click **Help**, and then click **Help Contents**. The help window appears with the first page displayed.



Welcome

Welcome to e*Index Security, SeeBeyond's security module to e*Index^{TM} Global Identifier. e*Index Security was designed to allow your system administrator to control user and user group access and permissions to all program functions of e*Index. With e*Index Security, access is broken down into various levels of authority and can be limited to authorized operators and users. Access to applications can also be limited according to a set of defined authorization privileges set up by the system administrator.

Introductory Information:

Mouse Conventions

What is e*Index Security?

Online help commands

Navigation pane tabbed headings

Navigation pane

Help window

2 Do any of the following:

On the **Contents** tab, expand the topic list until you see the topic you want to view. Click once on that topic, and the related text appears in the Help window.

Click the **Index** tab to view an alphabetized list of subjects from which you can select.

Click the **Search** tab to perform a search for a specific word or phrase.

3 Once you display a topic, you can click on the links to view additional information.

Tips on using the help system:

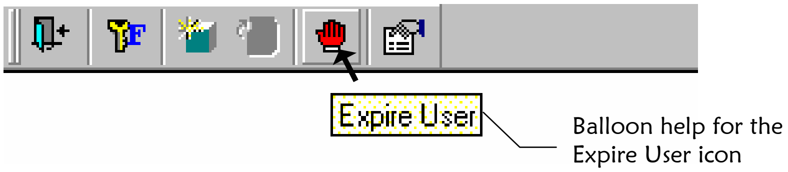
- *Use the **Hide/Show** button at the upper-left corner of this window to hide or show the navigation pane.*
- *You can also view the information contained in the online help system from the documents included in your electronic library (included on your installation CD). For more information, see "Displaying Online Documentation" later in this chapter.*

Using Balloon Help

You can view short descriptions of toolbar button functions by using the balloon help function.

▶ To view balloon help

- Place the mouse pointer over a toolbar button, and hold it there for a second or two without clicking the button. A description of the toolbar button appears below the button you selected.



Balloon help for the Expire User icon

Displaying Online Documentation

SeeBeyond provides online documentation for all e*Index products in an electronic library. The documents are in PDF format, and can be viewed using Adobe® Acrobat® Reader. The e*Index Electronic Library Welcome Document describes all the documents provided in electronic format, provides links to each document, and includes tips on how to use the electronic library.

▶ To display the electronic library welcome document

Before you begin:

- ✓ Make sure that you have Acrobat Reader installed on your workstation
- ✓ Make sure that the e*Index documentation is installed on your workstation

1. In Windows Explorer, navigate to your e*Index home directory, open the **docs** directory, and then double-click the file named **Welcome.pdf**.
2. You can page through the welcome document using the left and right arrows at the bottom of each page.

▶ To view online documentation

Before you begin:

- ✓ Open the welcome document from your Windows desktop

1. In the welcome document, scroll to the page that lists the document you wish to view, and click on the name of the document. The specified document appears in the Acrobat Reader window.
2. You can return to the welcome document at any time by clicking on the House icon in the upper left corner of the first page in the document.

Exiting e*Index Security

Overview

This section of the chapter provides the instructions you will need to log off e*Index Security.

Logging off e*Index Security

To exit e*Index Security, first close each open window, and then exit the application. There are several methods you can use to log off e*Index Security.

▶ To exit e*Index Security

Before you begin:

- ✓ Make sure all application windows are closed

1 Do one of the following:

To exit using the Main menu, click **File**, and then click **Exit.**

Exit tool

To exit using a toolbar button, click the **Exit** tool on the Primary Toolbar.

To exit using a short-cut key, press **Alt+F4**.

Close button

*To exit by closing the e*Index Security Main window*, click the **Close** button in the upper right corner of the window.

2 On the confirmation dialog that appears, click **Yes**.

Chapter 3

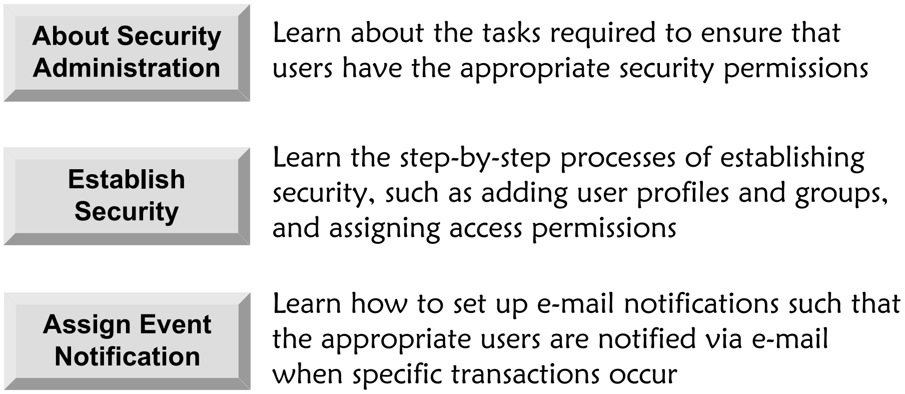
Setting up Security

About this Chapter

Overview

This chapter presents the background information and the step-by-step instructions you need to perform security tasks such as creating user profiles and user groups, and assigning access permissions.

The following diagram illustrates the contents of each major topic in this chapter.



About Security Administration

Learn about the tasks required to ensure that users have the appropriate security permissions

Establish Security

Learn the step-by-step processes of establishing security, such as adding user profiles and groups, and assigning access permissions

Assign Event Notification

Learn how to set up e-mail notifications such that the appropriate users are notified via e-mail when specific transactions occur

Learning About Security Tasks

Overview

This section provides the background information you need in order to manage security with e*Index Security.

What is Security Administration?

Security administration includes setting up and maintaining the e*Index security system. Setting up security for the e*Index system involves a variety of tasks, such as adding user profiles and user groups, assigning user profiles to groups, granting access permissions to user profiles and user groups, and assigning event notifications to user profiles. The tasks required for maintaining e*Index security once setup is complete are described in "What are Maintenance Tasks" in Chapter 4 of this guide.

When you initially install e*Index Security, you can only log on as the predefined user, the *e*Index Administrator*. The person who logs on as the e*Index Administrator is generally responsible for the overall security administration of e*Index.

What are User Profiles?

A user is anyone who views, adds, or modifies information in any of the e*Index applications. A *user profile* is the set of information you specify when you add a new user to e*Index Security. When you create a user profile, you identify a user by name and assign them a user ID and password. You can also specify a user type, email information, and effective and expiration dates. After you create a new user profile in e*Index Security, you can add the profile to a user group or grant that user specific permissions to access certain windows and perform certain functions within e*Index. One user profile, the e*Index Administrator, is defined when you install e*Index Security. By default, this user has access to all functions and actions of e*Index.

What Is the e*Index Administrator?

One user, the *e*Index Administrator*, is predefined when e*Index is installed. This user belongs to the three predefined user groups (see "What are User Groups?" later in this chapter), and can perform any task in any of the e*Index applications. The person who initially logs in as the e*Index Administrator is typically responsible for creating new user profiles and user groups, adding user profiles to the appropriate user groups, and assigning security permissions. The e*Index Administrator is usually the system administrator or the database administrator. You can add new administrator user profiles as needed.

What are User Types?

The user profiles you add must be one of two user types, regular user or administrator user. These categories determine the access permissions you can grant to a user profile. You assign the user type when you add a user to e*Index Security, and that type cannot be modified once the user profile is saved.

- **Administrator User**
  Administrator users, such as system or security administrators, are the only users who can perform all functions within the e*Index applications. Only administrator users can create user profiles.

- **Regular User**
  Regular users differ from administrator users in that they cannot create new user profiles, even if granted the access permission. Regular users can perform any other function for which they have access permissions.

What are User Groups?

User groups allow you to grant the same access permissions to a group of users with similar processing needs without having to define individual permissions for each user. For example, you can set up a group for users who need to view a particular function, such as Potential Duplicates, but who should not be able to merge or unmerge records. You can assign each user that meets these criteria to the new group, and all members of the group will be able to view Potential Duplicates, but will only be able to merge or unmerge any records if they are assigned those access permissions individually. Three user groups are predefined when you install e*Index.

- **e*Index Privileges Group**
  User profiles assigned to this group automatically receive access permissions to all functions of the e*Index GUI, including viewing, adding, merging, deactivating, and unmerging member profiles. Make

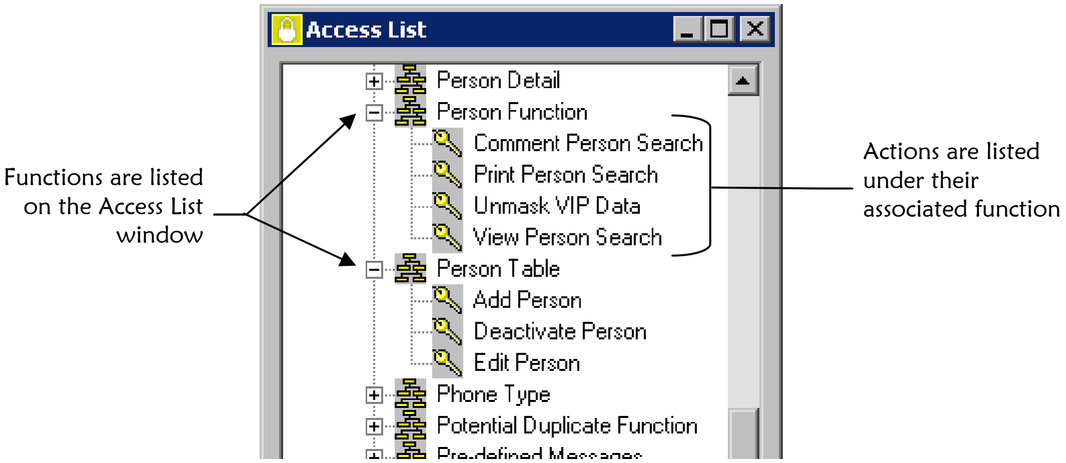
sure you only assign users to this group if they are fully trained on the e*Index GUI and are familiar with your record processing requirements.

- **Data Dictionary Privileges Group**
  User profiles assigned to this group automatically receive access permissions to all functions of the e*Index Administrator GUI, including adding and deleting common code table and custom code table entries, modifying control key values, and configuring e*Index. You should only assign users to this group if they are at an administrator level.

- **Security Privileges Group**
  User profiles assigned to this group automatically receive access permissions to all functions of the e*Index Security GUI, including adding and expiring user profiles and user groups, granting and revoking access privileges, and assigning e-mail notifications. Only administrator users can use their access permission for adding new user profiles; regular users cannot use this function.

What are Functions and Actions?

Access permissions are categorized by *functions* and by *actions*. In e*Index Security, a function represents a set of actions that perform related tasks. An *action* is a specific task that you can perform within a function. For example, the Audit Trail function includes three specific actions: View Audit Trail, Print Audit Trail, and Comment Audit Trail. Functions are also known as modules, and actions are also known as sub-modules. The Access List window provides a list of functions and actions, with each action listed under its associated function.



How are Access Permissions Granted?

After you create a user profile or user group, you can grant access permissions to that user profile or user group. You can grant access permissions to user profiles by two different methods. You can grant permissions directly to the user profile, or you can add a user profile to a user group, which automatically grants all of the permissions associated with the user group to the user profile. You can assign a user profile to more than one group, and you can assign additional access permissions to a user profile that belongs to a group.

What Kind of Access Permissions Can I Grant?

In e*Index Security, access is controlled by function. For example, you might grant a user or user group permission to access the Audit Trail and Comparison functions, but not the Potential Duplicate or Merge functions. You can further control access to actions within a function. For example, you can grant a user or user group permission to view member profiles on the Comparison window, but not to perform merges or add comments from the Comparison window. There are five primary categories of access permissions. Additional access permissions, such as Comment or Merge, may be available for certain modules depending on the commands available from that module. For a description of each access permission you can assign, see "e*Index Global Identifier Access Permissions", "e*Index Administrator Access Permissions", and "e*Index Security Access Permissions" in Appendix A.

Note: *You must assign View permission for a function in order for the user to be able to perform any other action within that function. For example, in order for a user to be able to merge member profiles from the Potential Duplicate function in e*Index, that user must be assigned both the View Potential Duplicate permission and the Merge Potential Duplicate permission.*

- **View**
  A user with *view* permissions can only look at, but not modify, information on the window for which the permission is granted.

- **Add**
  A user with *add* permissions can add information on the window for which the permission is granted. When you grant a user the ability to add an entity, you must also grant the ability to view that entity.

- **Edit**
  A user with *edit* permissions can view and modify information on the window for which the permission is granted. When you grant a user the ability to edit an entity, you must also grant the ability to view that entity.

- **Delete**
  A user with *delete* permissions can view and delete information on the window for which the permission is granted. When you grant a user the

ability to delete an entity, you must also grant the ability to view that entity.

- **Print**
  A user with *print* permissions can print the information displayed on the window for which the permission is granted. When you grant a user the ability to print an entity, you must also grant the ability to view that entity.

What is Region-Specific Security?

Region-specific security allows you to specify the regions for which users can view and modify information in the e*Index GUI. With region-specific security, each system that provides information to e*Index is associated with a region. In order for an e*Index user to access information from a specific system, their user profile must be associated with the region assigned to that system. To set up region-specific security, the following steps must be completed in the order given:

1. Install region-specific views to the database (see the appropriate database chapter in the *e*Index Global Identifier Installation Guide*).

2. Define regions in e*Index Administrator (see Chapter 3 of the *e*Index Administrator User's Guide*).

3. Define systems and associate each system with the appropriate region using e*Index Administrator (see Chapter 3 of the *e*Index Administrator User's Guide*).

4. Associate regions with the user profiles you create in e*Index Security (described later in this chapter).

What are E-mail Notifications?

e*Index Security provides the ability to automatically generate an e-mail message to the users you specify whenever certain events occur. e*Index can notify users each time a member profile is added, updated, merged, unmerged, or deactivated in the e*Index GUI. You can specify that a user be notified of any one or any combination of these events. When a user should no longer receive e-mails for an event, you can simply remove them from the notification list for that event.

Establishing Security

Overview

When you first establish security for e*Index, there are several steps you can follow to meet your security requirements. Complete the following steps to create user groups and user profiles, and to assign access privileges to each.

- Step 1: Obtain user and group information
- Step 2: Add user groups
- Step 3: Assign access permissions to user groups
- Step 4: Add user profiles
- Step 5: Add user profiles to user groups
- Step 6: Assign access permissions to user profiles

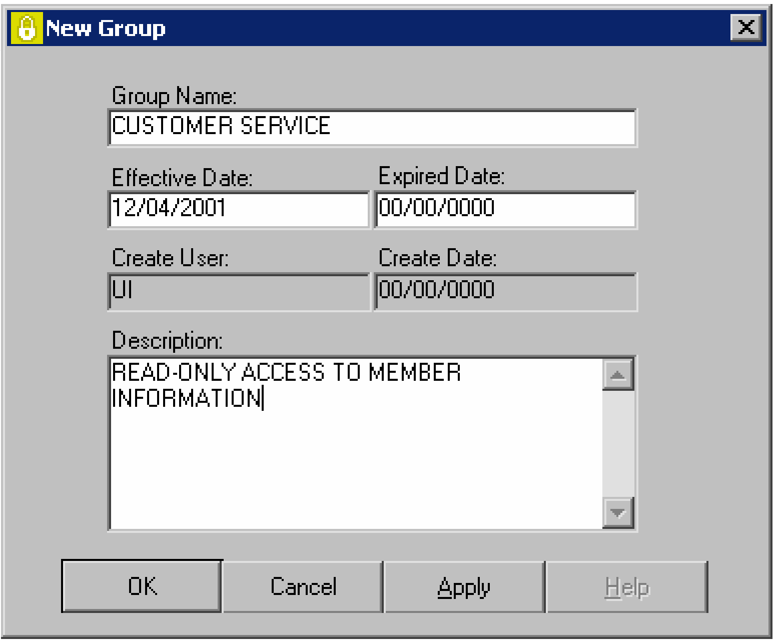
Note: *Once security is established, you may need to add additional user profiles and user groups to e*Index Security. At that time, you only need to follow the applicable steps for the new entity.*

Step 1: Obtain User and Group Information

Before you add users, identify the individuals who need to access any of the e*Index applications and determine their processing needs. Once you have identified their needs, group them into categories according to the access permissions they require. For example, place users who need to add member information into one category and users who need to resolve or merge potential duplicates in another category. With this information, you should be able to identify the user groups you need to add and the users that you should assign to each user group.

Step 2: Add User Groups

You can create user groups to ensure that all users associated with a particular user group can access the same information. To add a user group, you need to specify information such as the name of the group and the first date that members of the user group can access the functions to which the group has access.



Group Name: CUSTOMER SERVICE

Effective Date: 12/04/2001

Expired Date: 00/00/0000

Create User: UI

Create Date: 00/00/0000

Description: READ-ONLY ACCESS TO MEMBER INFORMATION

Use the New Group window to add a new user group to e*Index Security

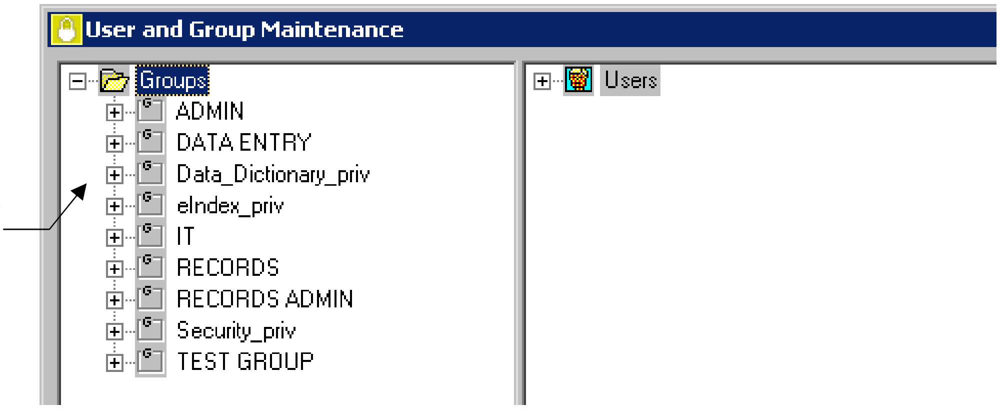
▶ To add a user group

Before you begin:

✓ Complete "Step 1: Obtain User and Group Information"

Access Setup tool

1 On the primary toolbar, click **Access Setup**. The User and Group Maintenance window appears. Double-click the **Groups** list or click the plus sign next to **Groups** to display a list of current user groups.



Existing user groups

New Group tool

2 On the User and Group Maintenance toolbar, click **New Group**. The New Group window appears.

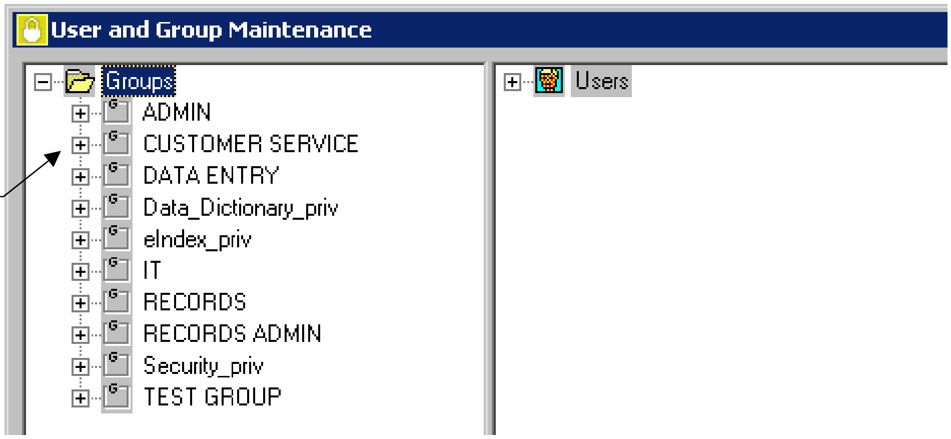
Tip: *If the New Group icon is not available, click on the Groups list in the left portion of the window.*

3 On the New Group window, identify the user group (for more information, see "About User Group Fields" following this procedure).

OK

OK button

4 On the New Group window, click **OK**. The new user group is saved to the database and the User and Group Maintenance window reappears. The new user group appears in the Groups list in the left portion of the window.



New user group, Customer Service, is added to the Groups list

5 Continue to "Step 3: Grant Access Permissions to User Groups"

Maintenance Tips — User Groups

Once you create a new user group, you can modify information about the group or expire the group if it becomes obsolete. Once expired, you can reinstate the group, if needed.

To change information about an existing user group: see "Modifying a User Group" in Chapter 4 of this guide.

To expire an obsolete user group: see "Expiring a User Group" in Chapter 4 of this guide.

To reinstate an expired user group: see "Reinstating an Expired User Group" in Chapter 4 of this guide.

About User Group Fields

The user group fields, located on the New Group and Group Properties windows, allow you to create new user groups and modify existing user groups.

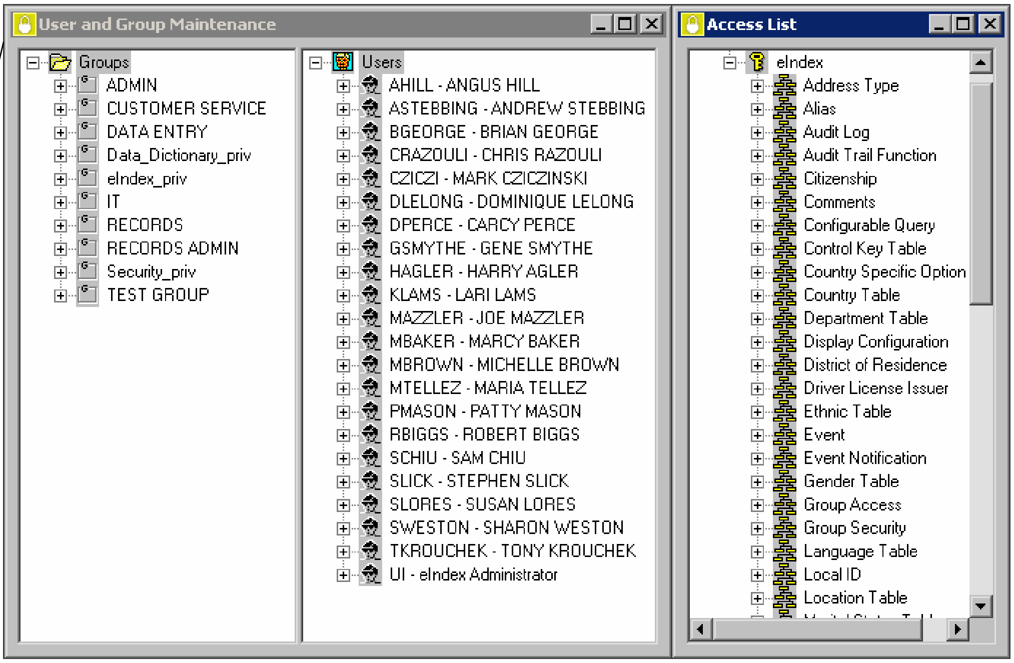
In this field...	type or select...
Group Name	The name of the user group. No default
Effective Date	The first date that a user profile assigned to this user group can access the components to which the group has access. Default: today's date
Expired Date	The date that the user group becomes disabled. On this date, users assigned to this group can no longer access components to which the group has access. No default ***Note:*** *Leave this field blank (00/00/0000) if you do not want to specify an expiration date at this time.*
Description	A brief description of the user group. This field is free form and you may enter any text you choose. No default

This field ...	displays this information ...
Create User	The login ID of the user who created the user group.
Create Date	The date the user group was created.

Step 3: Grant Access Permissions to User Groups

In order for the users you add to be able to perform the functions in any e*Index applications, you must grant the appropriate kind of access to each user profile or to the user groups to which you add them.

Use the User and Group Maintenance and the Access List windows to grant permissions to user groups



Groups
- ADMIN
- CUSTOMER SERVICE
- DATA ENTRY
- Data_Dictionary_priv
- eIndex_priv
- IT
- RECORDS
- RECORDS ADMIN
- Security_priv
- TEST GROUP

Users
- AHILL - ANGUS HILL
- ASTEBBING - ANDREW STEBBING
- BGEORGE - BRIAN GEORGE
- CRAZOULI - CHRIS RAZOULI
- CZICZI - MARK CZICZINSKI
- DLELONG - DOMINIQUE LELONG
- DPERCE - CARCY PERCE
- GSMYTHE - GENE SMYTHE
- HAGLER - HARRY AGLER
- KLAMS - LARI LAMS
- MAZZLER - JOE MAZZLER
- MBAKER - MARCY BAKER
- MBROWN - MICHELLE BROWN
- MTELLEZ - MARIA TELLEZ
- PMASON - PATTY MASON
- RBIGGS - ROBERT BIGGS
- SCHIU - SAM CHIU
- SLICK - STEPHEN SLICK
- SLORES - SUSAN LORES
- SWESTON - SHARON WESTON
- TKROUCHEK - TONY KROUCHEK
- UI - eIndex Administrator

eIndex
- Address Type
- Alias
- Audit Log
- Audit Trail Function
- Citizenship
- Comments
- Configurable Query
- Control Key Table
- Country Specific Option
- Country Table
- Department Table
- Display Configuration
- District of Residence
- Driver License Issuer
- Ethnic Table
- Event
- Event Notification
- Gender Table
- Group Access
- Group Security
- Language Table
- Local ID
- Location Table

▶ To grant permissions to user groups

Before you begin:

- ✓ Complete Step 2: Add User Groups
- ✓ Identify the user groups that require access permissions and the specific functions to which they need access (see "Step 1: Obtain User and Group Information" earlier in this chapter)

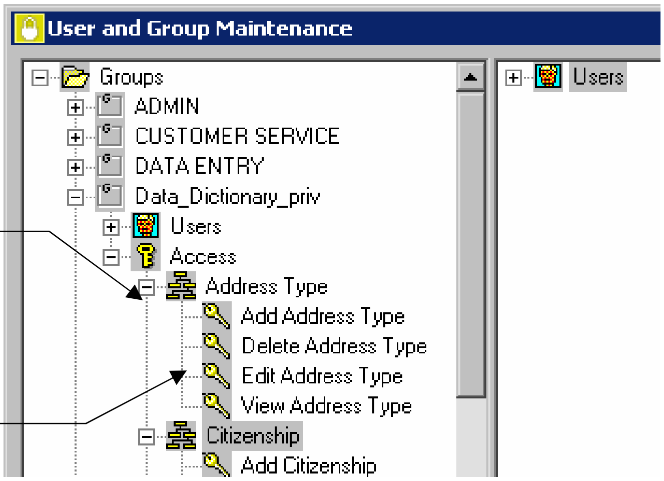
Access Setup tool

1 On the primary toolbar, click **Access Setup**. The User and Group Maintenance window appears.

Access List tool

2 On the User and Group Maintenance window, click **Access List**. The Access List window appears on the right side of the window.

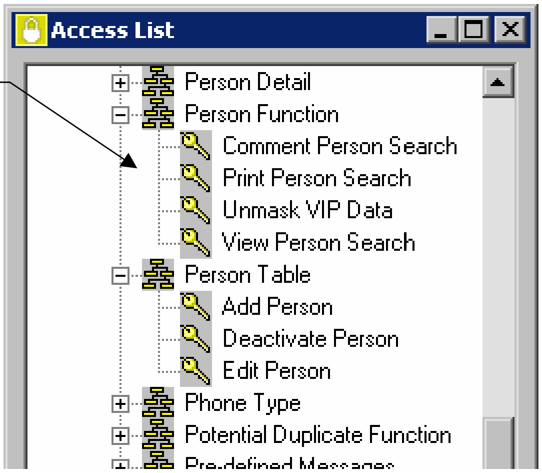
3 Verify the access permissions a user group already has by expanding the user group name and its Access list. All functions granted to the user group appear in the Access folder, and specific actions granted to the user group appear under the appropriate function.



Access to functions appear in the group's Access list

Access to specific actions within a function appear under the appropriate function

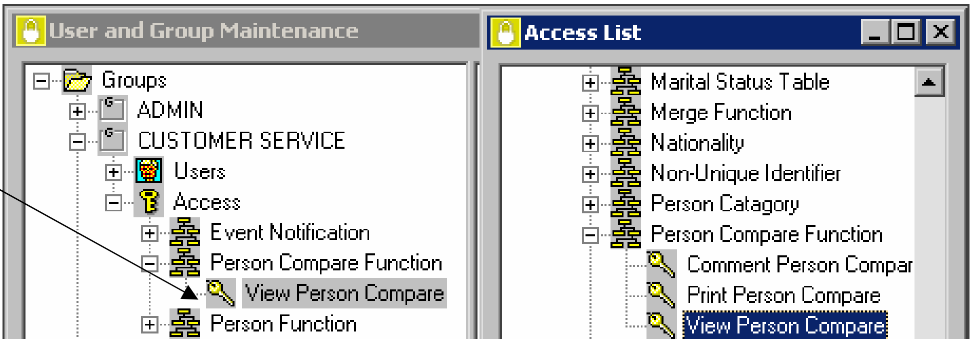
4 On the Access List window, expand the Access list until the function or action to which you want to grant access appears.



Expanding the Access List displays the available access permissions

5 Do one of the following:

To grant access permission to one action within a function, drag the action from the Access List window into the appropriate user group name on the User and Group Maintenance window, and then release the mouse button. The access permission appears in the user group's Access list.



The new access permission appears in the user group's Access list

To grant access permissions to all actions within a function, drag the function from the Access List window into the appropriate user group name on the User and Group Maintenance window, and then release the mouse button. All access permissions within the selected function appear in the user group's Access list.

6 Continue to "Step 4: Add User Profiles"

Maintenance Tips — User Group Access

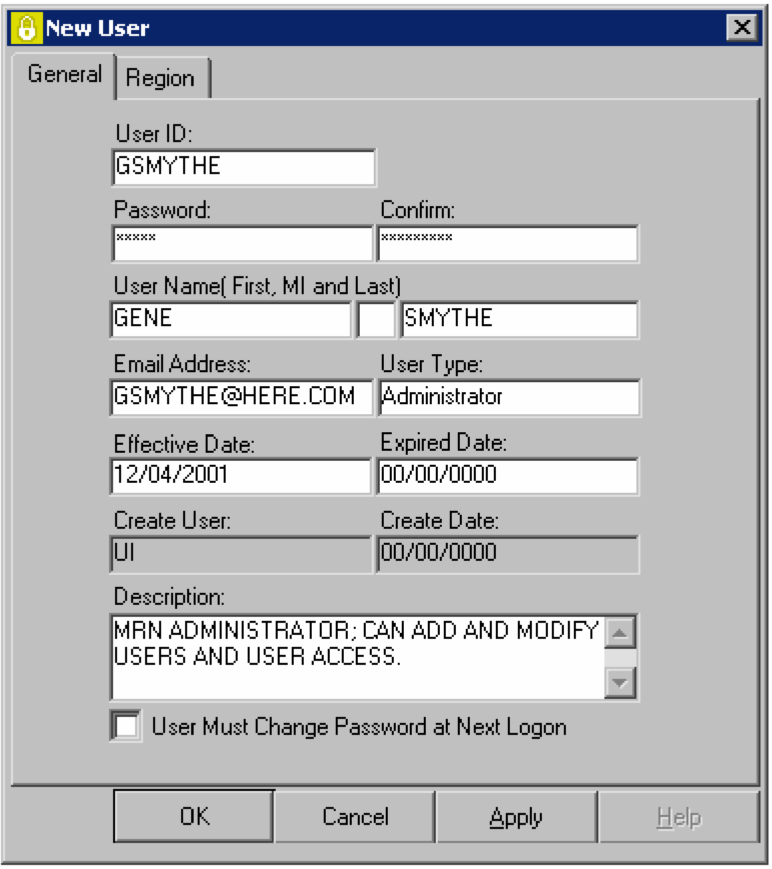
Once you assign access permissions to a user group, you can add new access permissions or expire existing ones. You can also reinstate expired access permissions if necessary.

To expire an access permission from a user group: see "Expiring Access Permissions" in Chapter 4 of this guide.

To reinstate an access permission to a user group: see "Reinstating Access Permissions" in Chapter 4 of this guide.

Step 4: Add User Profiles

Before a user can access any e*Index GUI applications, you must add a *user profile* for that user. The profile identifies the user and provides basic information such as the first and last dates the user can access an e*Index application.



Use the New User window to add a user profile to e*Index Security

User ID: GSMYTHE

Password: *****

Confirm: **********

User Name(First, MI and Last) GENE SMYTHE

Email Address: GSMYTHE@HERE.COM

User Type: Administrator

Effective Date: 12/04/2001

Expired Date: 00/00/0000

Create User: UI

Create Date: 00/00/0000

Description: MRN ADMINISTRATOR; CAN ADD AND MODIFY USERS AND USER ACCESS.

□ User Must Change Password at Next Logon

▶ To add a user profile

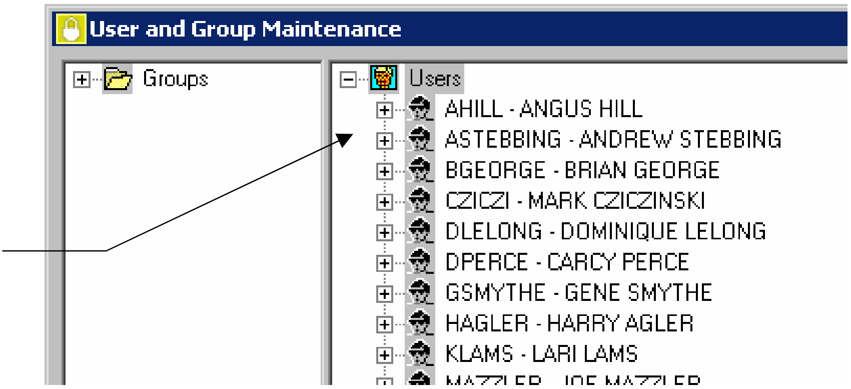
Before you begin:

- ✓ Obtain information about the user profiles you need to add
- ✓ Complete "Step 3: Grant Access Permissions to User Groups"

Access Setup tool

1 On the primary toolbar, click **Access Setup**. The User and Group Maintenance window appears, displaying a list of existing users.

2 To display a list of existing users, double-click the **Users** list, or click the plus sign next to **Users**.



AHILL - ANGUS HILL
ASTEBBING - ANDREW STEBBING
BGEORGE - BRIAN GEORGE
CZICZI - MARK CZICZINSKI
DLELONG - DOMINIQUE LELONG
DPERCE - CARCY PERCE
GSMYTHE - GENE SMYTHE
HAGLER - HARRY AGLER
KLAMS - LARI LAMS
MAZZLER - JOE MAZZLER

Existing e*Index users

New User tool

3 On the User and Group Maintenance toolbar, click **New User**. The New User window appears.

4 On the New User window, identify the user (for more information, see "About User Profile Fields" following this procedure).

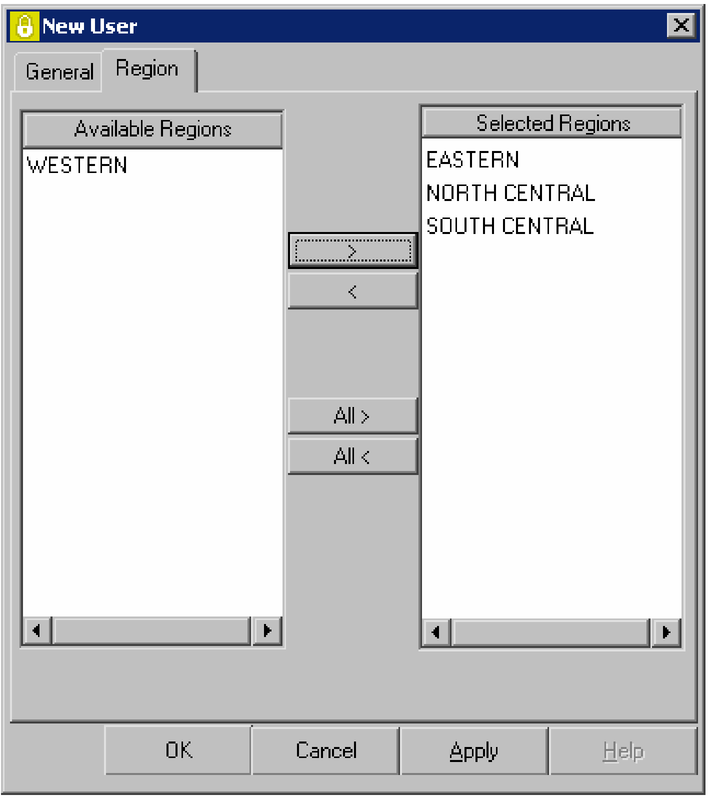
5 Do one of the following:

To add regions to the user profile (only if you are using region-specific security), click the Region tab. The Region page of the New User window appears. Continue to step 6.

OK

OK button

If you are not using region-specific security, click **OK**. The New User window closes and the new user profile is saved. Continue to step 8.



Available Regions: WESTERN

Selected Regions: EASTERN, NORTH CENTRAL, SOUTH CENTRAL

On the Region page, specify the regions for which the displayed user has access permissions

6 Do one of the following:

> Add button

To assign one region to the user profile at a time, select the region in the Available Regions list on the left side of the window, and then click **Add**. The region appears in the Selected Regions list. Repeat this step for each region you need to assign to the user profile.

All > Add All button

To assign all regions to the user profile, click **Add All**.

< Remove button

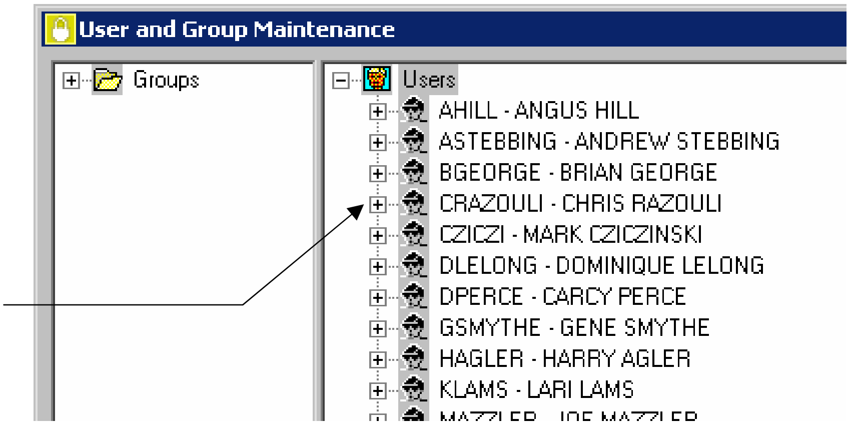
To remove a region from the user profile, select the region in the Selected Regions list on the right side of the window, and then click **Remove**. Repeat this step for each region you want to remove.

All < Remove all button

To remove all regions from the user profile, click **Remove All**.

OK OK button

7 On the New User window, click **OK**. The New User window closes and the User and Group Maintenance window reappears. The new user name appears in the Users list on the right side of the window.



User and Group Maintenance

Groups

Users
- AHILL - ANGUS HILL
- ASTEBBING - ANDREW STEBBING
- BGEORGE - BRIAN GEORGE
- CRAZOULI - CHRIS RAZOULI
- CZICZI - MARK CZICZINSKI
- DLELONG - DOMINIQUE LELONG
- DPERCE - CARCY PERCE
- GSMYTHE - GENE SMYTHE
- HAGLER - HARRY AGLER
- KLAMS - LARI LAMS
- MAZZLER - JOE MAZZLER

New user profile, CRAZOULI, is added to the Users List

8 Do one of the following:

To assign user profiles to user groups, continue to "Step 5: Assign User Profiles to User Groups."

To grant access permissions directly to user profiles without adding them to user groups, continue to "Step 6: Grant Access Permissions to User Profiles."

Maintenance Tips — User Profiles

Once you create a new user profile, you can modify the user's information, reassign regions, expire an obsolete profile, or reactivate an expired profile.

To modify a user profile: see "Modifying a User Profile" in Chapter 4 of this guide.

To reassign regions to a user profile: see "Modifying a User Profile" in Chapter 4 of this guide.

To expire a user profile: see "Expiring a User Profile" in Chapter 4 of this guide.

To reinstate an expired user profile: see "Reinstating an Expired User Profile" in Chapter 4 of this guide.

About User Profile Fields

The user profile fields, located on the New User and User Properties windows, allow you to create new user profiles and modify existing user profiles.

In this field...	type or select ...
User ID	The user’s login ID for all e*Index applications. No default
Password	The user's unique login password for all e*Index applications. No default

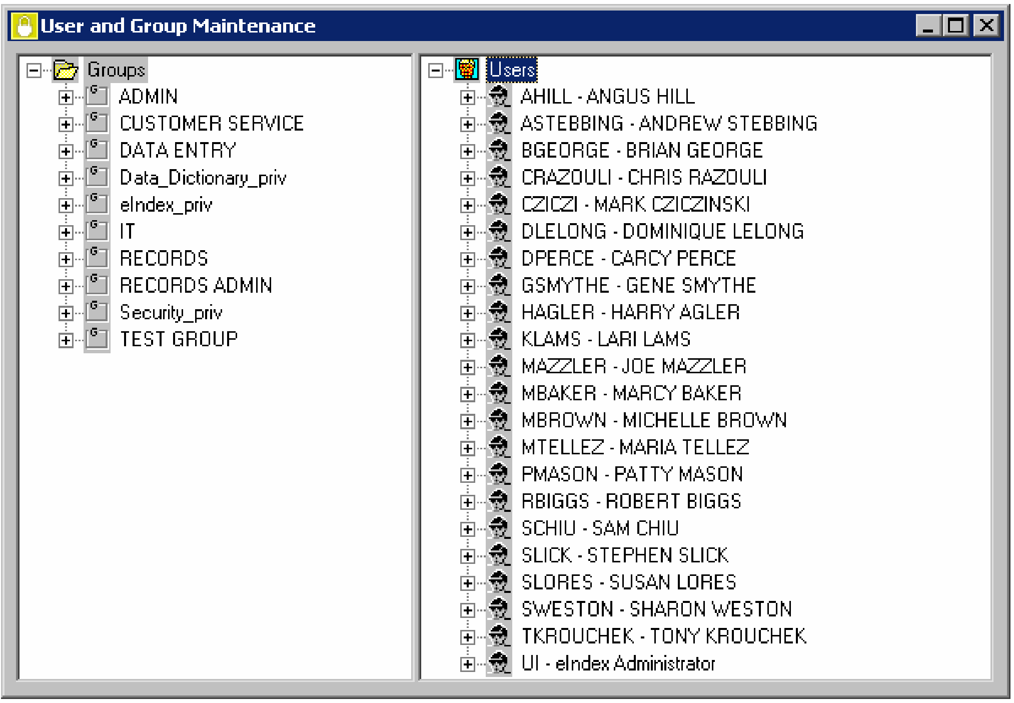
In this field...	type or select ...
Confirm	The user's password for confirmation. This is the same password you entered in the **Password** file. No default
User Name (First, MI, and Last)	The user’s last and first names, and middle initial. No default
Email Address	The e-mail address of the user you are adding. This field is required in order for the user to receive automatic e-mail notifications for e*Index GUI transactions. No default
User Type	The type of user you are adding. Select **Regular** for a user who cannot add user profiles; select **Administrator** for a user who can add user profiles. Default: **Regular**
Effective Date	The first date on which the user can log on to any e*Index application. Default: today’s date
Expired Date	The date that the user profile becomes automatically disabled. On this date, the user will no longer be able to log on to any e*Index applications. No default
Description	A brief description of the user. This field is free form, and you may enter any text you choose. No default

Select this check box ...	to specify that ...
User Must Change Password at Next Logon	The user whose profile you are adding must change their user password the next time they log on to any e*Index applications. Default: **Clear** (user does not need to change their password)

This field ...	displays this information ...
Create User	The login ID of the user who created the user profile.
Create Date	The date the user profile was created.

Step 5: Assign User Profiles to User Groups

You can grant the same access permissions to a set of user profiles by assigning those profiles to a user group. You can assign a user profile to as many groups as necessary to ensure they are granted all the required permissions, or you can assign a user profile to a user group and then grant individual permissions to the profile as needed.



Groups
- ADMIN
- CUSTOMER SERVICE
- DATA ENTRY
- Data_Dictionary_priv
- eIndex_priv
- IT
- RECORDS
- RECORDS ADMIN
- Security_priv
- TEST GROUP

Users
- AHILL - ANGUS HILL
- ASTEBBING - ANDREW STEBBING
- BGEORGE - BRIAN GEORGE
- CRAZOULI - CHRIS RAZOULI
- CZICZI - MARK CZICZINSKI
- DLELONG - DOMINIQUE LELONG
- DPERCE - CARCY PERCE
- GSMYTHE - GENE SMYTHE
- HAGLER - HARRY AGLER
- KLAMS - LARI LAMS
- MAZZLER - JOE MAZZLER
- MBAKER - MARCY BAKER
- MBROWN - MICHELLE BROWN
- MTELLEZ - MARIA TELLEZ
- PMASON - PATTY MASON
- RBIGGS - ROBERT BIGGS
- SCHIU - SAM CHIU
- SLICK - STEPHEN SLICK
- SLORES - SUSAN LORES
- SWESTON - SHARON WESTON
- TKROUCHEK - TONY KROUCHEK
- UI - eIndex Administrator

Use the User and Group Maintenance window to assign a user profile to a user group

▶ To assign a user profile to a user group

Before you begin:

✓ Complete "Step 4: Add User Profiles"

Access Setup tool

1 On the primary toolbar, click **Access Setup**. The User and Group Maintenance window appears.

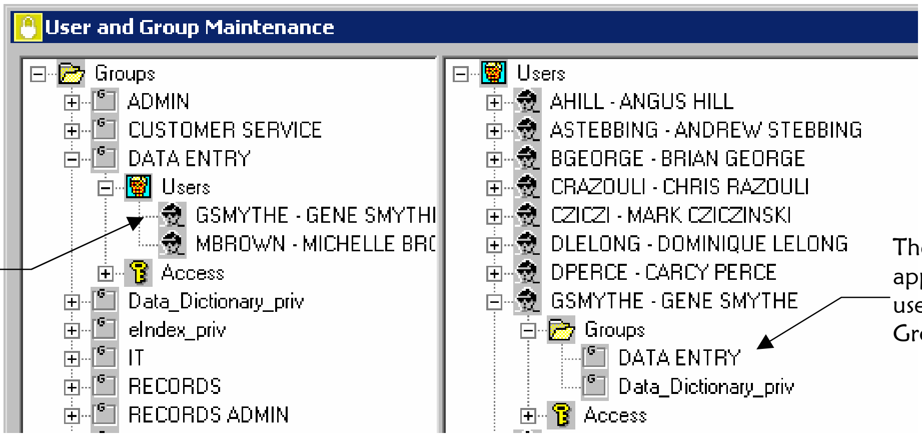
2 Expand the Groups and Users lists to display all available user profiles and user groups.

3 You can use either of the following methods to assign user profiles to user groups:

In the Users list on the right side of the window, select the user profile to be assigned to a user group. Drag the user profile into the user group on the left side of the window and then release the mouse button.

In the Groups list on the left side of the window, select the user group to which you want to assign the user profile. Drag the user group into the user profile on the right side of the window and then release the mouse button.

4 To complete the operation, click **Yes** on the confirmation dialog that appears. The user profile appears in the Groups list under the user group to which it was assigned. The user group appears in the Users list under the user profile to which it was assigned.



The user profile appears in the user group's Users list

The user group appears in the user profile's Groups list

5 To grant access permissions to the user profile in addition to those granted to the user group, continue to "Step 6: Grant Access Permissions to User Profiles."

Note: *We recommend that you only assign user profiles to the predefined user group **Data_Dictionary_priv** for administrator users. This user group has access to all functions of e*Index Administrator, including Control Key Maintenance, Event Maintenance, configuration functions, and so on. Changes made using these functions can affect how e*Index processes data.*

Maintenance Tips — User Group Assignments

Once you assign a user profile to a user group, you can assign the user profile to additional groups, modify the user profile's effective and expiration dates in the user group, or expire the user profile from existing user group assignments. You can reinstate expired user group assignments if necessary.

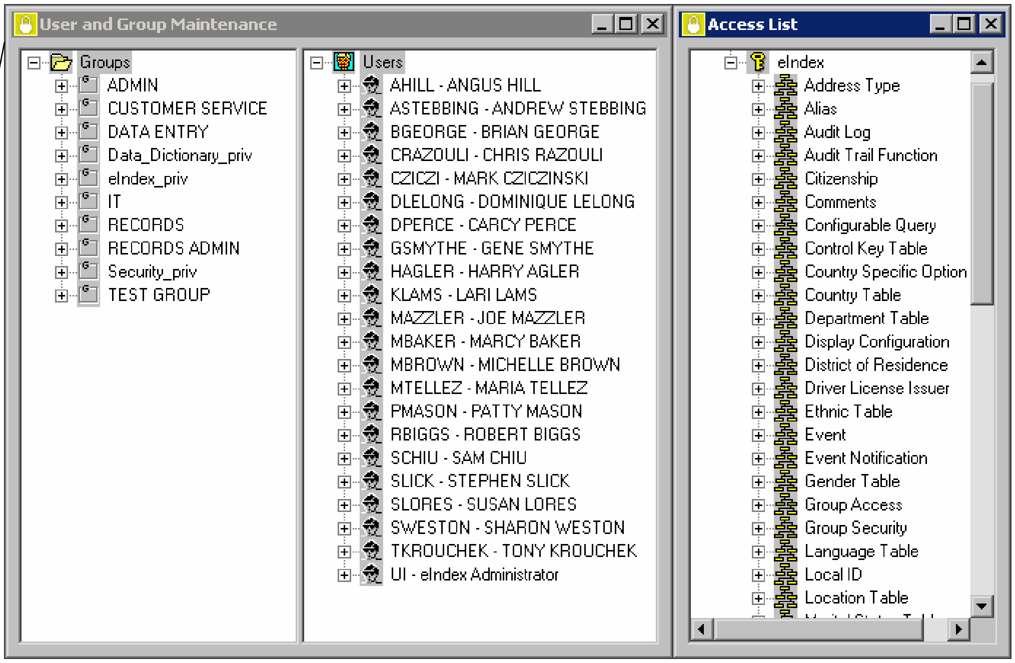
To expire a user profile from a user group: see "Expiring a User Profile from a User Group" in Chapter 4 of this guide.

To reinstate a user profile to a user group: see "Reinstating a User Profile to a User Group" in Chapter 4 of this guide.

To modify a user profile's active dates in a user group: see "Modifying a User Profile's Active Dates in a User Group" in Chapter 4 of this guide.

Step 6: Grant Access Permissions to User Profiles

In order for the users you add to be able to perform functions in any of the e*Index applications, you must grant the appropriate kind of access to each user profile or to the user groups to which they belong. If you assigned a user profile to a user group that has all of the access permissions the user profile requires, you do not need to grant any access permissions to the user profile.



Use the User and Group Maintenance window and the Access List window to grant access permissions to user profiles

Groups
- ADMIN
- CUSTOMER SERVICE
- DATA ENTRY
- Data_Dictionary_priv
- eIndex_priv
- IT
- RECORDS
- RECORDS ADMIN
- Security_priv
- TEST GROUP

Users
- AHILL - ANGUS HILL
- ASTEBBING - ANDREW STEBBING
- BGEORGE - BRIAN GEORGE
- CRAZOULI - CHRIS RAZOULI
- CZICZI - MARK CZICZINSKI
- DLELONG - DOMINIQUE LELONG
- DPERCE - CARCY PERCE
- GSMYTHE - GENE SMYTHE
- HAGLER - HARRY AGLER
- KLAMS - LARI LAMS
- MAZZLER - JOE MAZZLER
- MBAKER - MARCY BAKER
- MBROWN - MICHELLE BROWN
- MTELLEZ - MARIA TELLEZ
- PMASON - PATTY MASON
- RBIGGS - ROBERT BIGGS
- SCHIU - SAM CHIU
- SLICK - STEPHEN SLICK
- SLORES - SUSAN LORES
- SWESTON - SHARON WESTON
- TKROUCHEK - TONY KROUCHEK
- UI - eIndex Administrator

eIndex
- Address Type
- Alias
- Audit Log
- Audit Trail Function
- Citizenship
- Comments
- Configurable Query
- Control Key Table
- Country Specific Option
- Country Table
- Department Table
- Display Configuration
- District of Residence
- Driver License Issuer
- Ethnic Table
- Event
- Event Notification
- Gender Table
- Group Access
- Group Security
- Language Table
- Local ID
- Location Table

▶ To grant permissions to user profiles

Before you begin:

- ✓ Complete "Step 4: Add User Profiles" and optionally "Step 5: Assign User Profiles to User Groups"
- ✓ Identify which users require access to specific functions of any e*Index applications (see "Step 1: Obtain User and Group Information" earlier in this chapter)

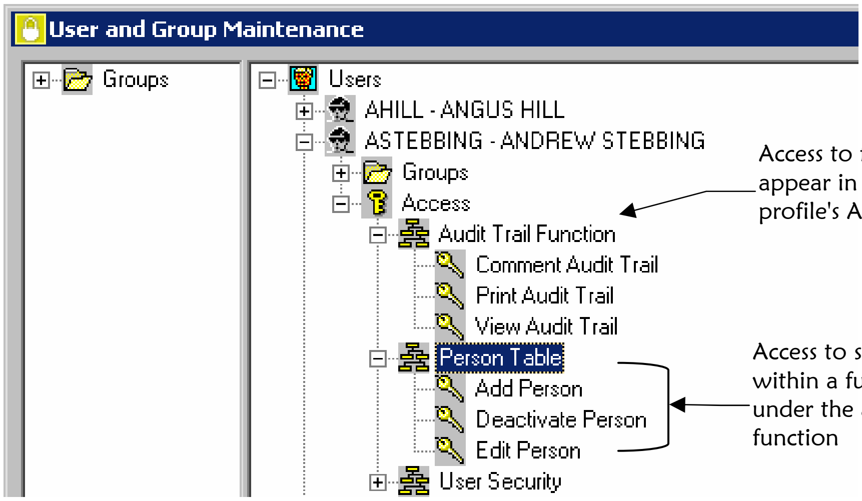
Access Setup tool

1 On the primary toolbar, click **Access Setup**. The User and Group Maintenance window appears.

Access List tool

2 On the User and Group Maintenance window, click **Access List**. The Access List window appears on the right side of the window.

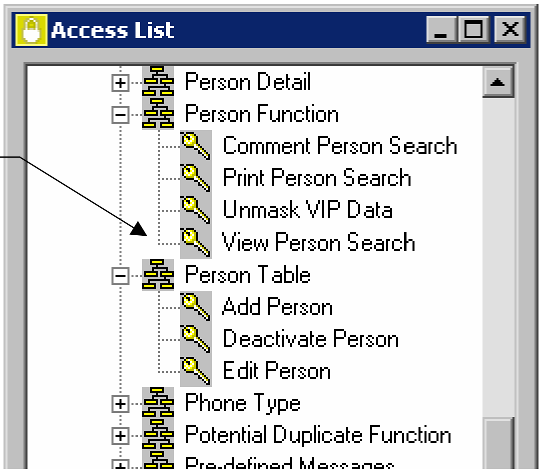
3 Verify the access permissions the user profile already has by expanding the user profile name and its Access list. All functions granted to the user profile appear in the Access folder, and specific actions granted to the user profile appear under the appropriate function.



Access to functions appear in the user profile's Access list

Access to specific actions within a function appear under the appropriate function

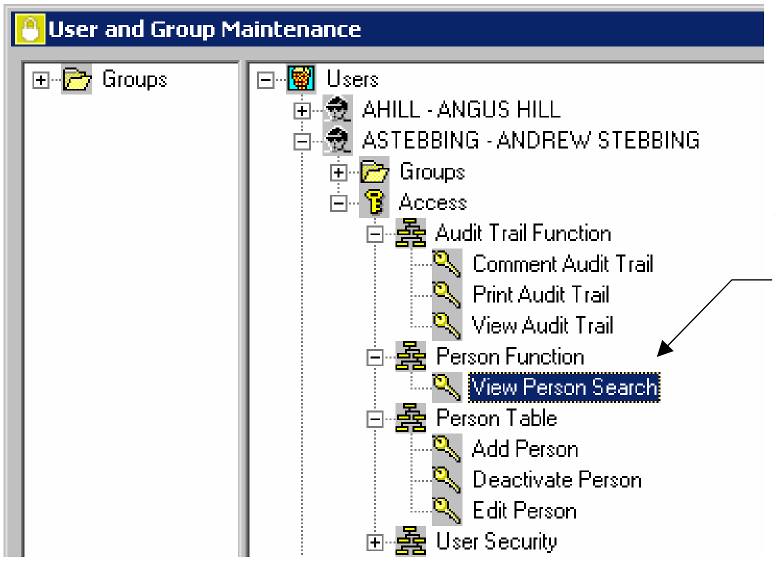
4 On the Access List window, expand the Access list until the function or action to which you want to grant access appears.



Expanding the Access List displays the available access permissions

5 Do one of the following:

To assign access permission to one action at a time, drag the action from the Access List window into the appropriate user profile name on the User and Group Maintenance window, and then release the mouse button. The access permission appears in the user profile's Access list.



User and Group Maintenance

- Groups
- Users
  - AHILL - ANGUS HILL
  - ASTEBBING - ANDREW STEBBING
    - Groups
    - Access
      - Audit Trail Function
        - Comment Audit Trail
        - Print Audit Trail
        - View Audit Trail
      - Person Function
        - View Person Search
      - Person Table
        - Add Person
        - Deactivate Person
        - Edit Person
      - User Security

The new access permission appears in the user profile's Access list

To grant access permissions to all actions within a function at one time, drag the function from the Access List window into the appropriate user profile name on the User and Group Maintenance window, and then release the mouse button. The access permissions appear in the user profile's Access list.

Maintenance Tips — User Access

Once you assign access permissions to a user profile, you can add new access permissions or expire existing ones. You can also reinstate expired access permissions if necessary.

To expire an access permission from a user profile: see "Expiring Access Permissions" in Chapter 4 of this guide.

To reinstate an access permission to a user profile: see "Reinstating Access Permissions" in Chapter 4 of this guide.

Assigning Event Notifications

Overview

When you assign event notifications to users, they automatically receive a notification via e-mail when the transactions you specify occur in the e*Index GUI. Complete the following steps to set up event notification.

- Step 1: Verify User Information
- Step 2: Assign Event Notification to User Profiles

Important! *In order for the event notification to be functional, you must develop an e-mail e*Way that subscribes to Events published from the e*Index polling e*Way. You may also need to modify the processing rules for the polling e*Way to ensure that the Events from the* ui_msg_detail *table in the e*Index database are published to the appropriate IQ. The e-mail address of the users who should receive event notification appears in the last segment (the ZEN segment) of Events in the* ui_msg_detail *table.*

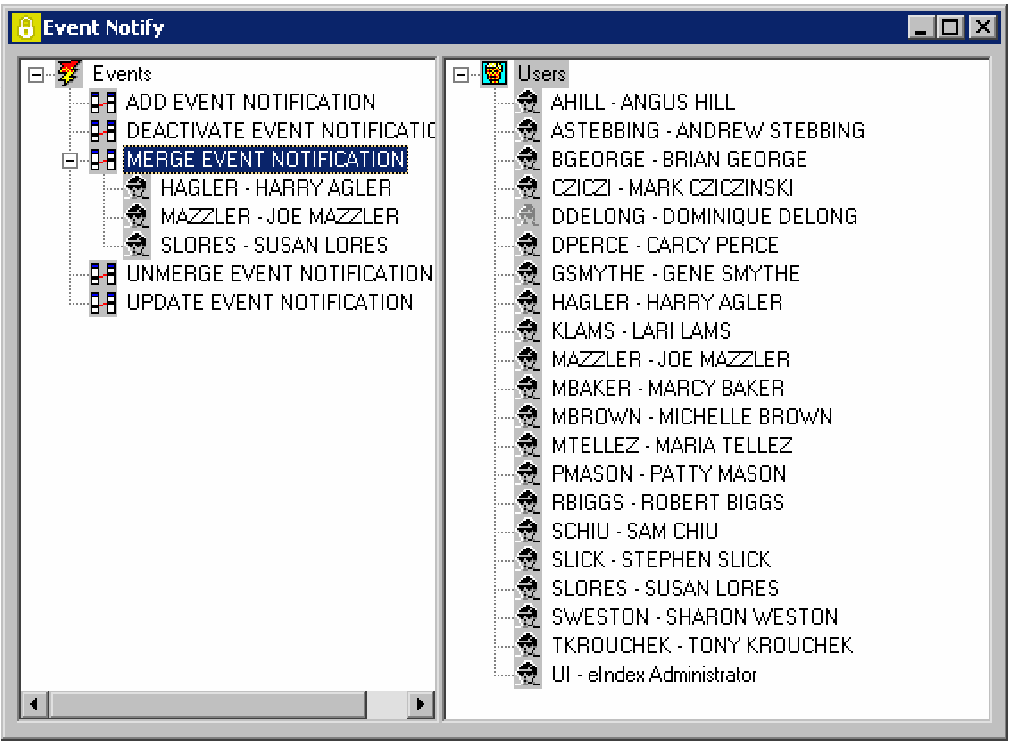
Step 1: Verify User Information

Before assigning event notification to user profiles, you need to obtain information about the users who require event notification and the events of which they require notification. You must also verify that each user profile has a current and correct e-mail address for the user.

Step 2: Assign Event Notification to User Profiles

You can assign event notification to user profiles using a simple drag-and-drop process. In order for notification to work properly for a user profile, an active e-mail address must be associated with the user profile. If a user profile is expired, the icon for that profile appears grayed out in the Users list to indicate that the profile is not currently active. You cannot assign event notifications to an inactive user profile.

Use the Event Notify window to assign event notifications to user profiles



Event Notify

- Events
  - ADD EVENT NOTIFICATION
  - DEACTIVATE EVENT NOTIFICATIC
  - MERGE EVENT NOTIFICATION
    - HAGLER - HARRY AGLER
    - MAZZLER - JOE MAZZLER
    - SLORES - SUSAN LORES
  - UNMERGE EVENT NOTIFICATION
  - UPDATE EVENT NOTIFICATION

- Users
  - AHILL - ANGUS HILL
  - ASTEBBING - ANDREW STEBBING
  - BGEORGE - BRIAN GEORGE
  - CZICZI - MARK CZICZINSKI
  - DDELONG - DOMINIQUE DELONG
  - DPERCE - CARCY PERCE
  - GSMYTHE - GENE SMYTHE
  - HAGLER - HARRY AGLER
  - KLAMS - LARI LAMS
  - MAZZLER - JOE MAZZLER
  - MBAKER - MARCY BAKER
  - MBROWN - MICHELLE BROWN
  - MTELLEZ - MARIA TELLEZ
  - PMASON - PATTY MASON
  - RBIGGS - ROBERT BIGGS
  - SCHIU - SAM CHIU
  - SLICK - STEPHEN SLICK
  - SLORES - SUSAN LORES
  - SWESTON - SHARON WESTON
  - TKROUCHEK - TONY KROUCHEK
  - UI - eIndex Administrator

▶ To assign event notification to user profiles

Before you begin:

✓ Complete "Step 1: Verify User Information"

Event Notification tool

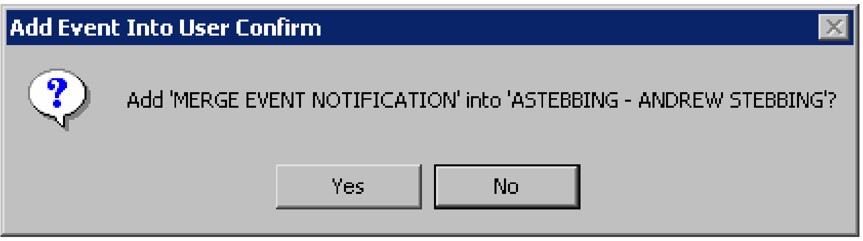
1 On the primary toolbar, click **Event Notification**. The Event Notify window appears.

2 Use one of the following two methods to assign event notification:

In the Users list on the right side of the window, select the user profile to be assigned notification, drag the user profile into the appropriate event on the left side of the window, and then release the mouse button.

In the Events list on the left side of the window, select the event for which you want to assign notification, drag the event to the appropriate user profile on the right side of the window, and then release the mouse button.

3 The Add Event confirmation dialog appears.

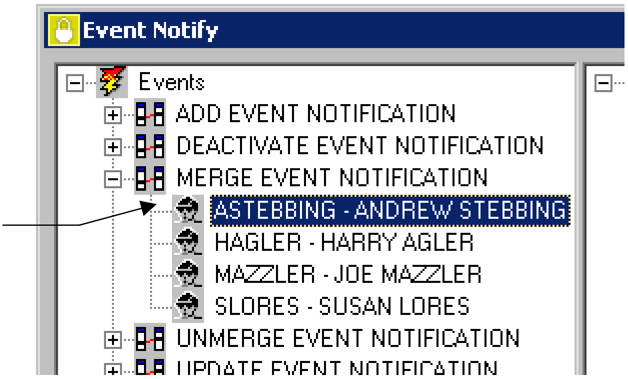


Add 'MERGE EVENT NOTIFICATION' into 'ASTEBBING - ANDREW STEBBING'?

Add Event confirmation dialog

Yes button

4 On the Add Event confirmation dialog, click **Yes**. Notification for the selected event is added to the user profile, and the user profile appears under the event in the Events list.



```
Events
  ADD EVENT NOTIFICATION
  DEACTIVATE EVENT NOTIFICATION
  MERGE EVENT NOTIFICATION
    ASTEBBING - ANDREW STEBBING
    HAGLER - HARRY AGLER
    MAZZLER - JOE MAZZLER
    SLORES - SUSAN LORES
  UNMERGE EVENT NOTIFICATION
  UPDATE EVENT NOTIFICATION
```

The user profile appears under the event for which notification was assigned

Maintenance Tips — Event Notification

Once you assign event notification to a user profile, you can add new notifications or remove existing ones.

To remove an event notification from a user profile: see "Removing Event Notifications from User Profiles" in Chapter 4 of this guide.

Chapter 4

Maintaining Security Information

About this Chapter

Overview

This chapter presents the background information and the step-by-step instructions you need to maintain information about user profiles, user groups, access permissions, and event notification. It also includes information about the control keys that you use to configure e*Index Security.

The following diagram illustrates the contents of each major topic in this chapter.

About Security Maintenance	Learn about tasks you can perform to keep security information and access permissions current
User Profiles and Groups	Learn how to maintain information about user profiles and user groups
User Access and Notification	Learn how to modify access permissions and event notification assignments
System Parameters	Learn the how to configure the system parametners for e*Index Security

Learning About Security Maintenance

Overview

This section provides the background information you need in order to maintain security information for e*Index Security.

What are Maintenance Tasks?

Once you have created the initial setup for e*Index Security, you may need to modify some of the information about users and user groups, or you may need to change their access permissions. Maintenance tasks may include adding, modifying, or expiring user profiles or user groups; removing user profiles from user groups; reinstating user profiles into user groups; expiring or reinstating access permissions; and modifying the event notifications assigned to a user profile. Maintenance also includes modifying certain system parameters for e*Index that control the time-out feature and password requirements.

What are Control Keys?

The *control keys* in the Configuration module of e*Index Security are system parameters that allow you to customize how your system processes passwords and other security information. You can perform the following actions by changing the value of the control keys.

- Specify the number of passwords stored in the password history table (passwords cannot be re-used until they are removed from the history table)
- Define the length of time that an instance of e*Index Security can remain inactive before the application shuts down
- Define a minimum password length for e*Index users
- Specify a specific length of time after which all passwords must be changed
- For more information about the available control keys, see "About Control Key Values" at the end of this chapter.

A Note About Shortcuts

For most tasks involved in security maintenance, there are three different methods of selecting commands (such as Expire User, Properties, Activate Group, and so on). The procedures in this chapter only describe selecting commands using the icons on the application toolbar, but you can use any of the following methods.

- **Application Toolbar**
  The User and Group Maintenance and Event Notify toolbars contain icons that you can click to perform certain tasks. On the User and Group Maintenance window, the icons change depending on whether you are working with the Users list or the Groups list. The procedures in this chapter illustrate these icons.

- **Pop-up Menu**
  You can right click on the entity you are modifying to display a pop-up menu of command options. These options provide the same commands as the toolbar icons that are available for the active window.

- **Main Menu**
  When you access an application window, such as the User and Group Maintenance window, a new menu appears on the Main Menu named *Actions*. This menu contains three sub-menus: Users, Groups, and Access. The options on the sub-menus provide the same commands as the toolbar icons that are available for the active window.

Maintaining User Profiles and User Groups

Overview

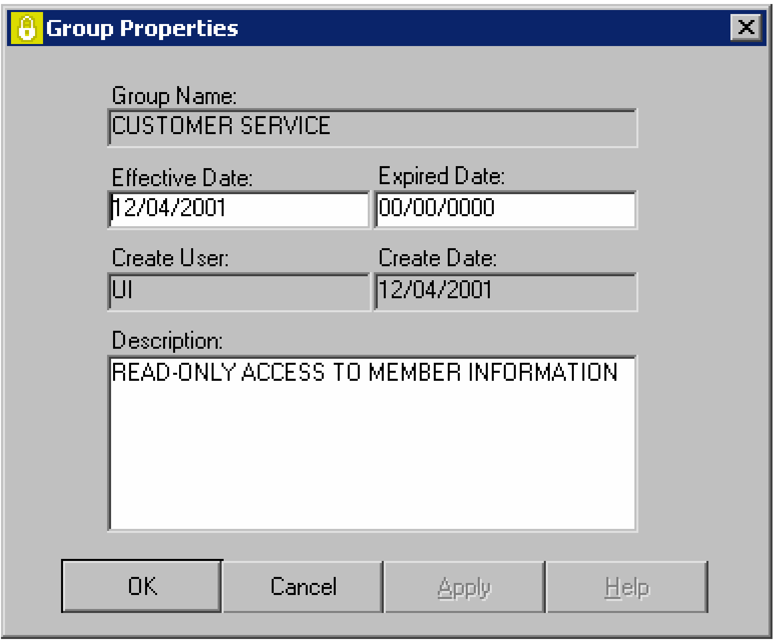
After you create user profiles and user groups, and assign user profiles to user groups, you can perform any of the following maintenance tasks:

- View user group information
- View user profile information
- Modify information about a user group
- Modify information about a user
- Expire a user group
- Reinstate an expired user group
- Expire a user profile
- Reinstate an expired user profile

Viewing User Group Information

After you add a user group to e*Index Security, you may need to view information about that user group. You can view information about the user group, the user profiles assigned to the group, and the access permissions granted to the group. Existing user groups appear in the Groups list on the User and Group Maintenance window.

View information about a user group on the Group Properties window



Group Properties

Group Name: CUSTOMER SERVICE

Effective Date: 12/04/2001

Expired Date: 00/00/0000

Create User: UI

Create Date: 12/04/2001

Description: READ-ONLY ACCESS TO MEMBER INFORMATION

▶ To view user group information

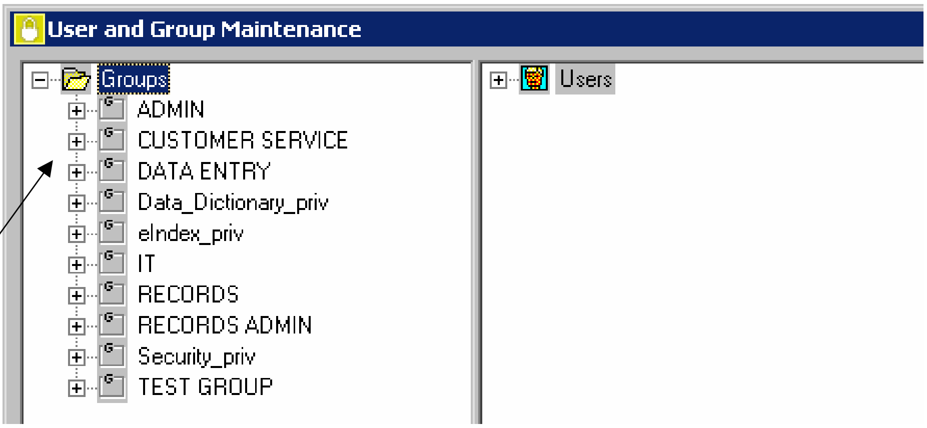
Before you begin:

- ✓ Identify the user group whose information you want to view

Access Setup tool

1 On the primary toolbar, click **Access Setup**. The User and Group Maintenance window appears.

2 Double-click the Groups list to view a list of all user groups.



User and Group Maintenance

Groups
- ADMIN
- CUSTOMER SERVICE
- DATA ENTRY
- Data_Dictionary_priv
- eIndex_priv
- IT
- RECORDS
- RECORDS ADMIN
- Security_priv
- TEST GROUP

Users

The User and Group Maintenance window displays a list of groups from which you can choose

Properties tool

3 In the Groups list, select the name of the user group whose information you want to view, and then click **Properties**. The Group Properties window appears (for more information about the fields displayed on this window, see "About User Group Fields" in Chapter 3 of this guide).

4 To modify information about the displayed user group, follow steps 4 and 5 under "Modifying a User Group" later in this chapter.

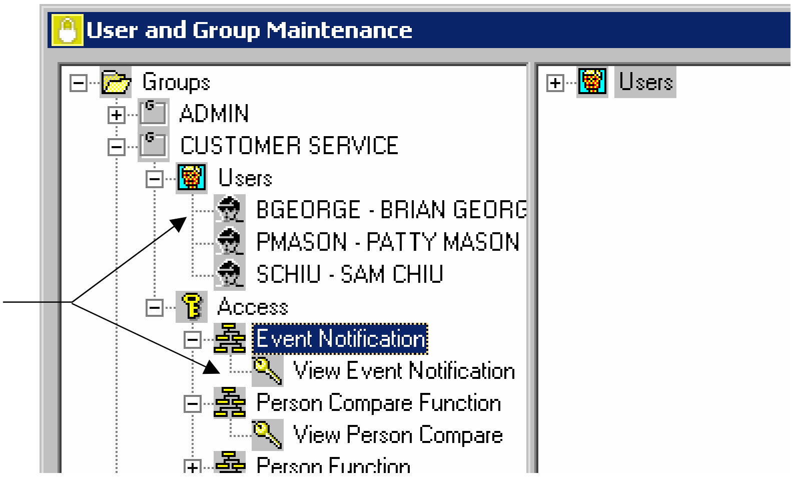
OK

OK button

5 To close the Group Properties window and return to the User and Group Maintenance window, click **OK**.

6 To view the user profiles assigned to a user group, double-click the user group name and then double-click the Users folder beneath it.

7 To view the access permissions granted to a user group, double-click the user group name and then double-click the Access folder beneath it. Double-click a function name in the Access list to view specific access permissions.



User and Group Maintenance

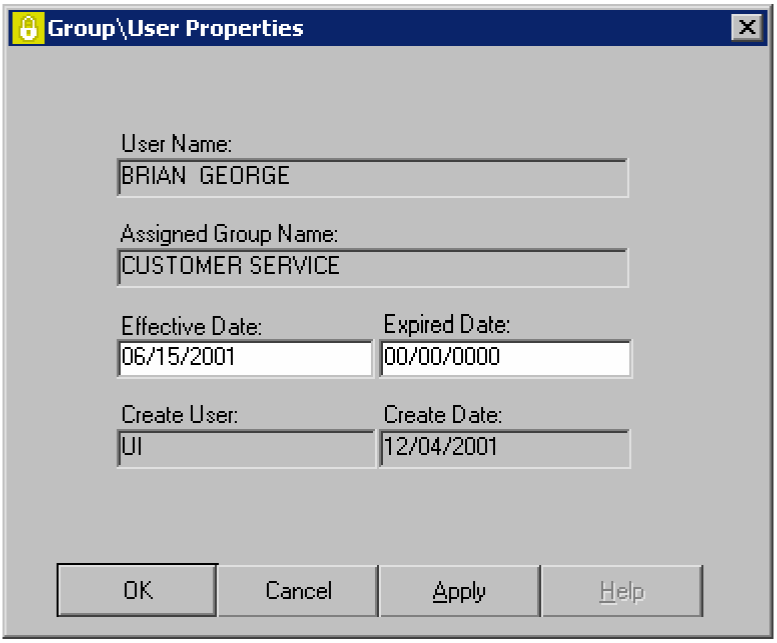
Groups
- ADMIN
- CUSTOMER SERVICE
  - Users
    - BGEORGE - BRIAN GEORG
    - PMASON - PATTY MASON
    - SCHIU - SAM CHIU
  - Access
    - Event Notification
      - View Event Notification
    - Person Compare Function
      - View Person Compare
    - Person Function

Users

Expand the Groups list to view user profiles and access permissions assigned to a user group

Properties tool

8 To view information about a user profile assigned to a user group, expand the Groups list as in step 6 above, select the user profile name, and then click **Properties**. The Group\User Properties window appears (for information about this window, see "About Group\User Properties Fields" following this procedure).



User Name: BRIAN GEORGE

Assigned Group Name: CUSTOMER SERVICE

Effective Date: 06/15/2001

Expired Date: 00/00/0000

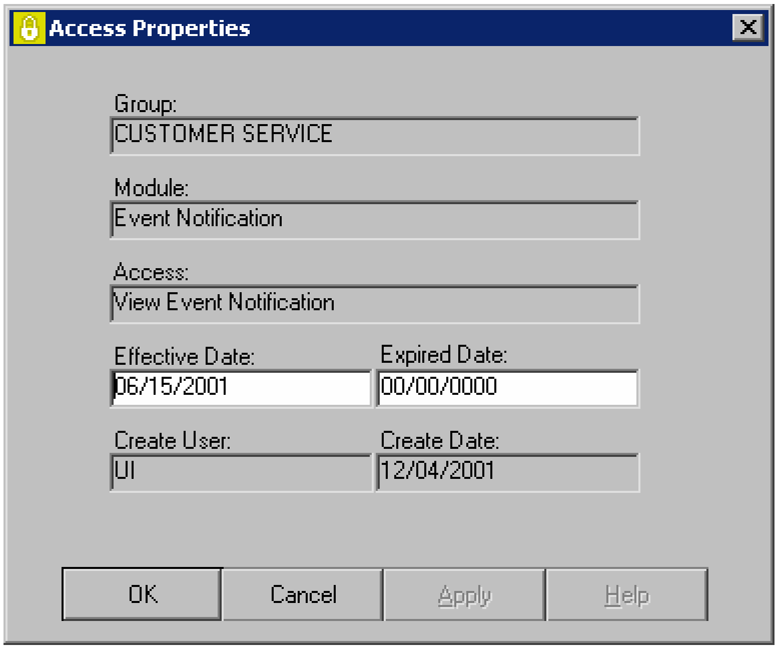
Create User: UI

Create Date: 12/04/2001

Use the Group\User Properties window to view information about the user profiles assigned to a user group

Properties tool

9 To view information about an access permission granted to a user group, expand the Groups list as in step 7 above, select the permission name, and then click **Properties**. The Access Properties window appears (for information about the fields that appear on this window, see "About Access Properties Fields" following this procedure).



Access Properties

Group: CUSTOMER SERVICE

Module: Event Notification

Access: View Event Notification

Effective Date: 06/15/2001

Expired Date: 00/00/0000

Create User: UI

Create Date: 12/04/2001

About Group\User Properties Fields

The fields on the Group\User Properties window display information about a user profile assigned to a specific user group, such as the date the user profile was assigned to the group and the login ID of the user who assigned the user profile to the user group.

In this field ...	type or select ...
Effective Date	The date the user profile became an active member of the selected user group. Default: The date the user profile was assigned to the user group
Expired Date	The date the user profile is no longer an active member of the selected user group. Default: **00/00/0000**

This field ...	displays this information ...
User Name	The name of the user whose profile you selected.
Assigned Group Name	The name of the user group you selected and of which the user profile is a member.
Create User	The login ID of the user who assigned the user profile to the user group.
Create Date	The date the user profile was assigned to the user group.

About Access Properties Fields

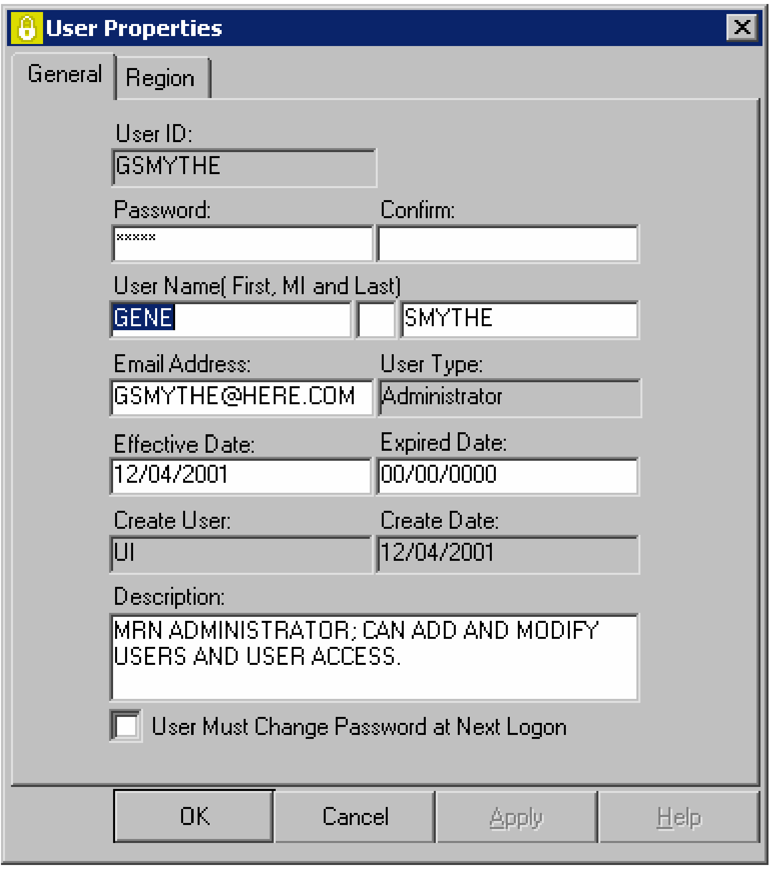
The fields on the Access Properties window display information about the access permissions assigned to a user group or user profile, such as the date the access permission was granted and the login ID of the user who granted the access permission to the user group or the user profile.

In this field …	type or select …
Effective Date	The date the user group or user profile could first use the selected access permission. Default: The date the access permission was granted to the user group or user profile
Expired Date	The date the user group or user profile is no longer able to use the selected access permission. Default: **00/00/0000**

This field …	displays this information …
Group or **User**	The name of the user group or user profile you selected.
Module	The name of primary function to which the selected access permission belongs. For example, if the selected access permission were **View Audit Trail**, then the module would be **Audit Trail Function**.
Access	The name of the selected access permission.
Create User	The login ID of the user who granted the selected access permission to the user group or user profile.
Create Date	The date the access permission was granted to the user group or user profile.

Viewing User Profile Information

After you add a user profile to e*Index Security, you may need to view information included in the user profile. You can view information about the user profile, the user groups to which the user profile is assigned, and the access permissions assigned to the user profile. Existing user profiles appear on the Users list on the User and Group Maintenance window.



User ID: GSMYTHE

Password: ***** Confirm:

User Name(First, MI and Last) GENE SMYTHE

Email Address: GSMYTHE@HERE.COM User Type: Administrator

Effective Date: 12/04/2001 Expired Date: 00/00/0000

Create User: UI Create Date: 12/04/2001

Description: MRN ADMINISTRATOR; CAN ADD AND MODIFY USERS AND USER ACCESS.

□ User Must Change Password at Next Logon

View user profile information on the User Properties window

▶ To view user profile information

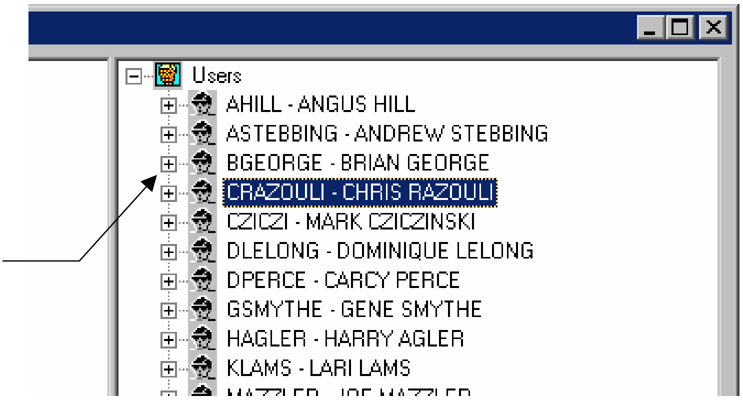
Before you begin:

✓ Identify the user profile whose information you want to view

Access Setup tool

1 On the primary toolbar, click **Access Setup**. The User and Group Maintenance window appears.

2 Double-click the Users list to view a list of all user profiles.



The User and Group Maintenance window displays a list of users from which you can choose

- Users
  - AHILL - ANGUS HILL
  - ASTEBBING - ANDREW STEBBING
  - BGEORGE - BRIAN GEORGE
  - CRAZOULI - CHRIS RAZOULI
  - CZICZI - MARK CZICZINSKI
  - DLELONG - DOMINIQUE LELONG
  - DPERCE - CARCY PERCE
  - GSMYTHE - GENE SMYTHE
  - HAGLER - HARRY AGLER
  - KLAMS - LARI LAMS
  - MAZZLER - JOE MAZZLER

Properties tool

3 In the Users list, select the name of the user profile whose information you want to view, and then click Properties. The User Properties window appears (for more information about the fields displayed on this window, see "About User Profile Fields" in Chapter 3 of this guide).

4 Do any of the following:

To view the regions associated with the displayed user profile, click the Region tab. The Region page appears, and displays the available regions and the regions associated with the profile.

To modify information about the displayed user profile, follow steps 4 and 5 under "Modifying a User Profile" later in this chapter.

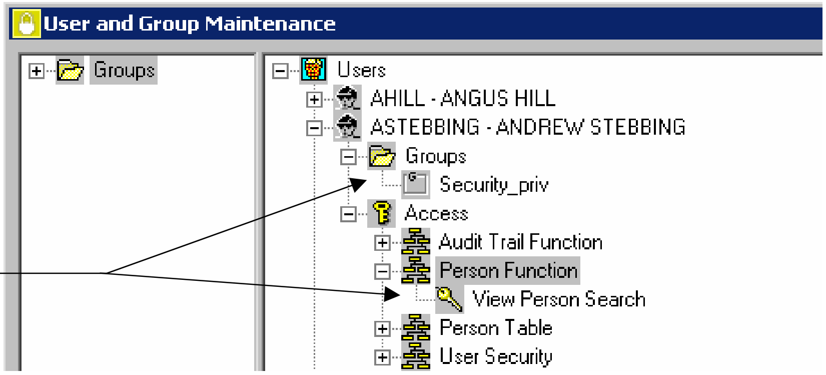
OK

OK button

5 To close the User Properties window and return to the User Maintenance window, click **OK**.

6 To view the user groups assigned to the user profile, double-click the name of the user profile, and then double-click the Groups list beneath it.

7 To view the access permissions granted to the user profile, double-click the name of the user profile, and then double-click the Access list beneath it. Double-click the name of a function to view the specific access permissions granted.



Expand the Users list to view user groups and access permissions assigned to a user profile

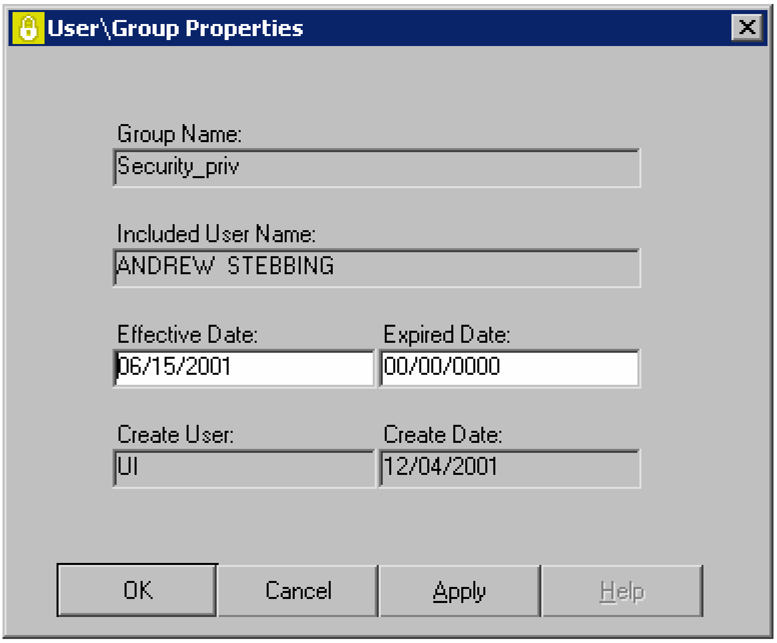
User and Group Maintenance

- Groups

- Users
  - AHILL - ANGUS HILL
  - ASTEBBING - ANDREW STEBBING
    - Groups
      - Security_priv
    - Access
      - Audit Trail Function
      - Person Function
        - View Person Search
      - Person Table
      - User Security

Properties tool

8 To view information about a user group to which a user profile is assigned, expand the Users list as in step 6 above, select the user group name, and then click **Properties**. The User\Group Properties window appears (for information about the fields that appear on this window, see "About User\Group Properties Fields" following this procedure).



Group Name: Security_priv

Included User Name: ANDREW STEBBING

Effective Date: 06/15/2001

Expired Date: 00/00/0000

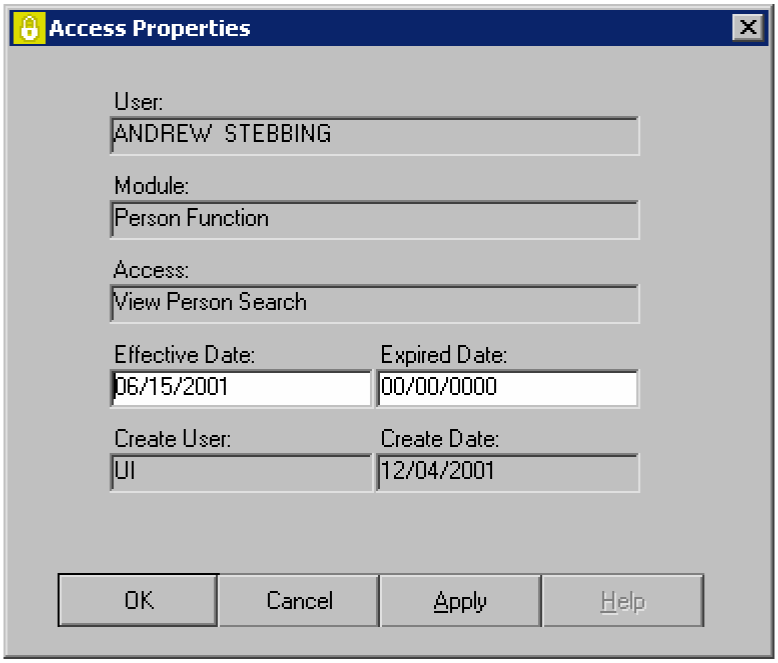
Create User: UI

Create Date: 12/04/2001

Use the User\Group Properties window to view information about the user groups to which a profile is assigned

Properties tool

9 To view information about an access permission granted to a user profile, expand the Users list as in step 7 above, select the permission name, and then click **Properties**. The Access Properties window appears (for information about the fields that appear on this window, see "About Access Properties Fields" earlier in this chapter).



User:
ANDREW STEBBING

Module:
Person Function

Access:
View Person Search

Effective Date:
06/15/2001

Expired Date:
00/00/0000

Create User:
UI

Create Date:
12/04/2001

Use the Access Properties window to view information about the access permissions granted to a user profile

About User\Group Properties Fields

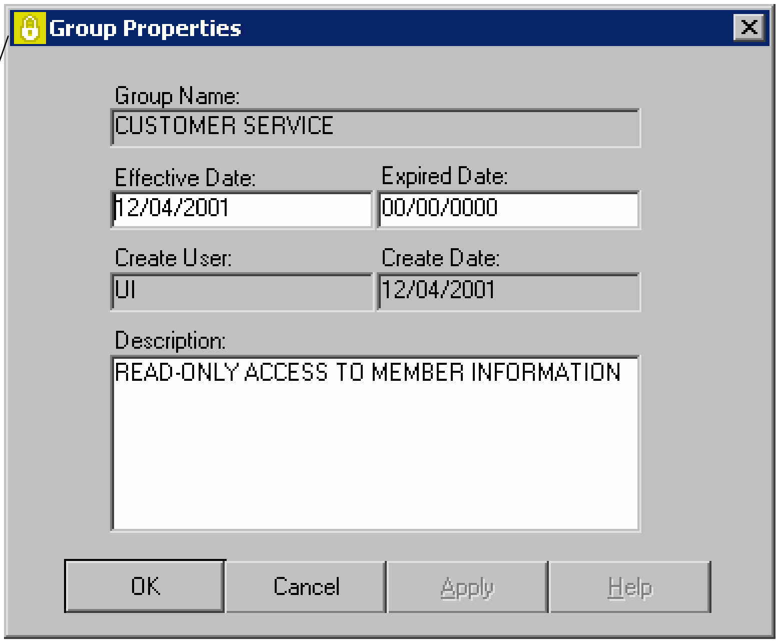
The fields on the User\Group Properties window display information about a user group to which the selected user profile is assigned, such as the date the user profile was assigned to the group and the login ID of the user who assigned the user profile to the user group.

In this field …	type or select …
Effective Date	The date the user profile became an active member of the selected user group. Default: The date the user profile was assigned to the user group
Expired Date	The date the user profile is no longer an active member of the user group. Default: **00/00/0000**

This field …	displays this information …
Group Name	The name of the selected user group.
Included User Name	The name of the selected user profile, which is assigned to the selected user group.
Create User	The login ID of the user who assigned the user profile to the user group.
Create Date	The date the user profile was assigned to the user group.

Modifying a User Group

After you add a user group to e*Index Security, you may need to modify some of the group's information. You can select the user group you want to edit from the Groups list on the User and Group Maintenance window.


Group Properties

Group Name: CUSTOMER SERVICE

Effective Date: 12/04/2001

Expired Date: 00/00/0000

Create User: UI

Create Date: 12/04/2001

Description: READ-ONLY ACCESS TO MEMBER INFORMATION

Use the Group Properties window to change information about a user group

▶ To modify a user group

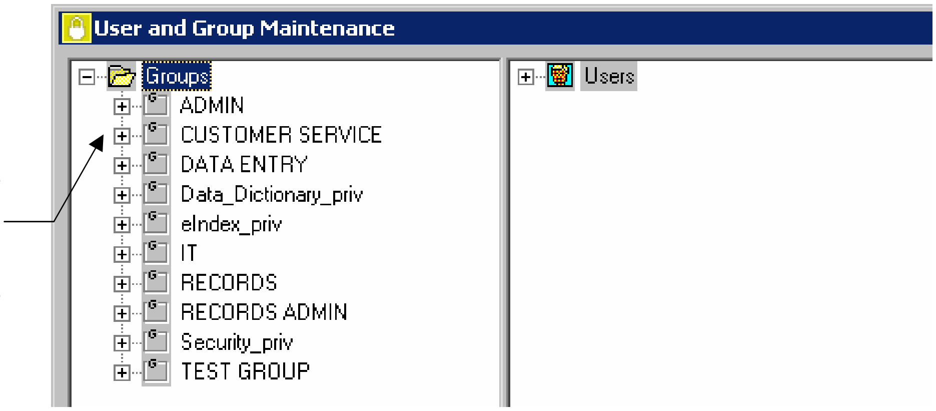
Before you begin:

- ✓ Identify the user group information you need to change

Access Setup tool

1 On the primary toolbar, click **Access Setup**. The User and Group Maintenance window appears.

2 Double-click the Groups list to view a list of existing user groups.



The User and Group Maintenance window displays a list of groups from which you can choose

Properties tool

3 Select the user group you want to modify, and then click **Properties**. The Group Properties window appears.

4 Change the value of any open field on the window (for more information, see "About User Group Fields" in Chapter 3 of this guide).

Tip: *You can modify the user group's expiration or effective date to modify the date the user group's activity begins or ends.*

Save tool

Apply

Apply button

OK

OK button

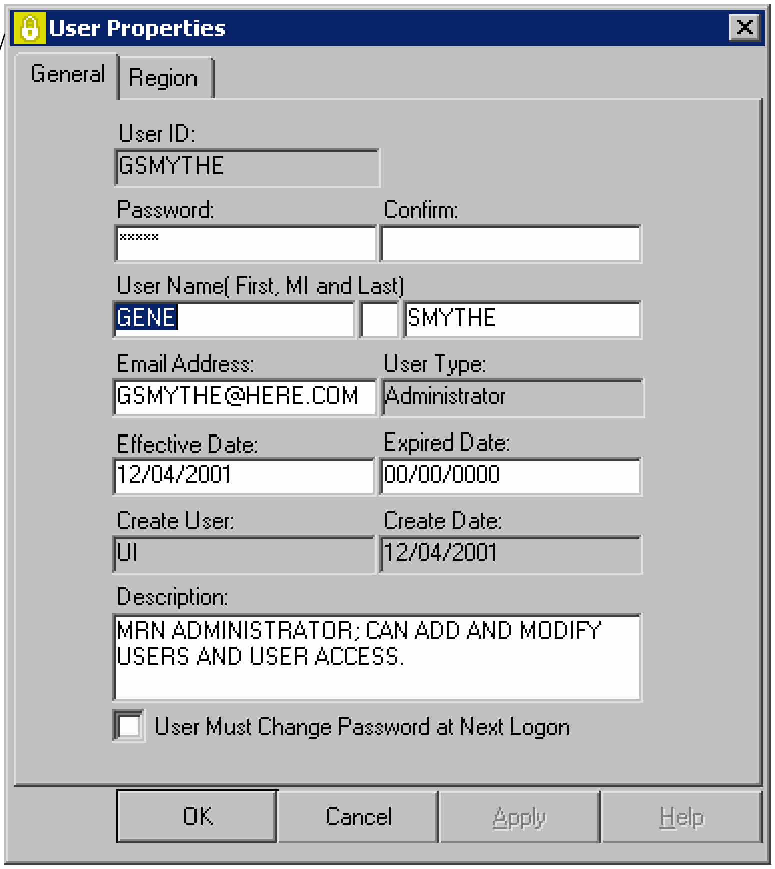
5 Do one of the following:

To save your changes and leave the Group Properties window open, click **Save** or **Apply**. The changes are saved to the database.

To save your changes and close the Group Properties window, click **OK**. The changes are saved to the database and the User and Group Maintenance window reappears.

Modifying a User Profile

After you add a user profile to e*Index Security, you may need to retrieve and modify some of the saved information. Select the user profile you want to edit from the Users list on the User Maintenance window.



User ID: GSMYTHE

Password: *****
Confirm:

User Name(First, MI and Last)
GENE | | SMYTHE

Email Address: GSMYTHE@HERE.COM
User Type: Administrator

Effective Date: 12/04/2001
Expired Date: 00/00/0000

Create User: UI
Create Date: 12/04/2001

Description:
MRN ADMINISTRATOR; CAN ADD AND MODIFY USERS AND USER ACCESS.

□ User Must Change Password at Next Logon

Use the User Properties window to modify user profile information

▶ To modify a user profile

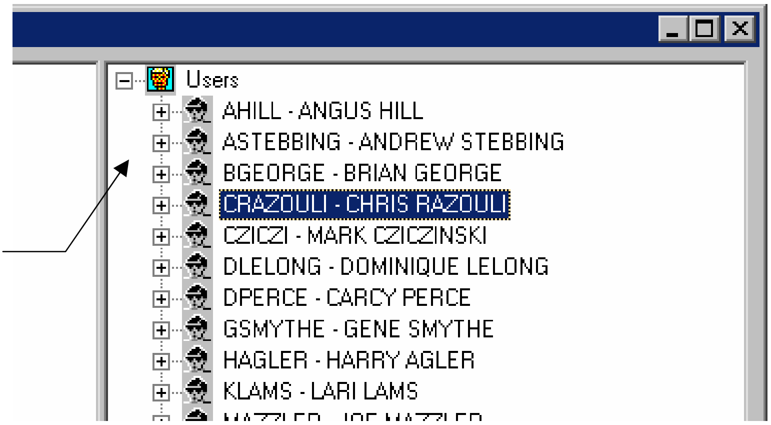
Before you begin:

- ✓ Identify the profile information you need to change

Access Setup tool

1 On the primary toolbar, click **Access Setup**. The User and Group Maintenance window appears.

2 Double-click the Users list to view a list of existing user profiles.



Users

AHILL - ANGUS HILL

ASTEBBING - ANDREW STEBBING

BGEORGE - BRIAN GEORGE

CRAZOULI - CHRIS RAZOULI

CZICZI - MARK CZICZINSKI

DLELONG - DOMINIQUE LELONG

DPERCE - CARCY PERCE

GSMYTHE - GENE SMYTHE

HAGLER - HARRY AGLER

KLAMS - LARI LAMS

MAZZLER - JOE MAZZLER

The User and Group Maintenance window displays a list of users from which you can choose

Properties tool

3 Select the user profile you want to modify, and then click **Properties**. The User Properties window appears.

4 Change the value of any open field on the window (for more information, see "About User Profile Fields" in Chapter 3 of this guide).

Tip: *You can change the user profile's expiration or effective date to modify the date the user profile's activity begins or ends.*

---

5 To change the regions to which a user profile is assigned, click the Region tab and do any of the following:

[>] Add button

To assign a new region to the user profile, select the region in the Available Regions list on the left side of the window, and then click **Add**. The region appears in the Selected Regions list. Repeat this step for each region you need to assign to the user profile.

[All >] Add All button

To assign all regions to the user profile, click **Add All**.

[<] Remove button

To remove a region from the user profile, select the region in the Selected Regions list on the right side of the window, and then click **Remove**. Repeat this step for each region you want to remove.

[All <] Remove All button

To remove all regions from the user profile, click **Remove All**.

Save tool

Apply

Apply button

OK

OK button

6 Do one of the following:

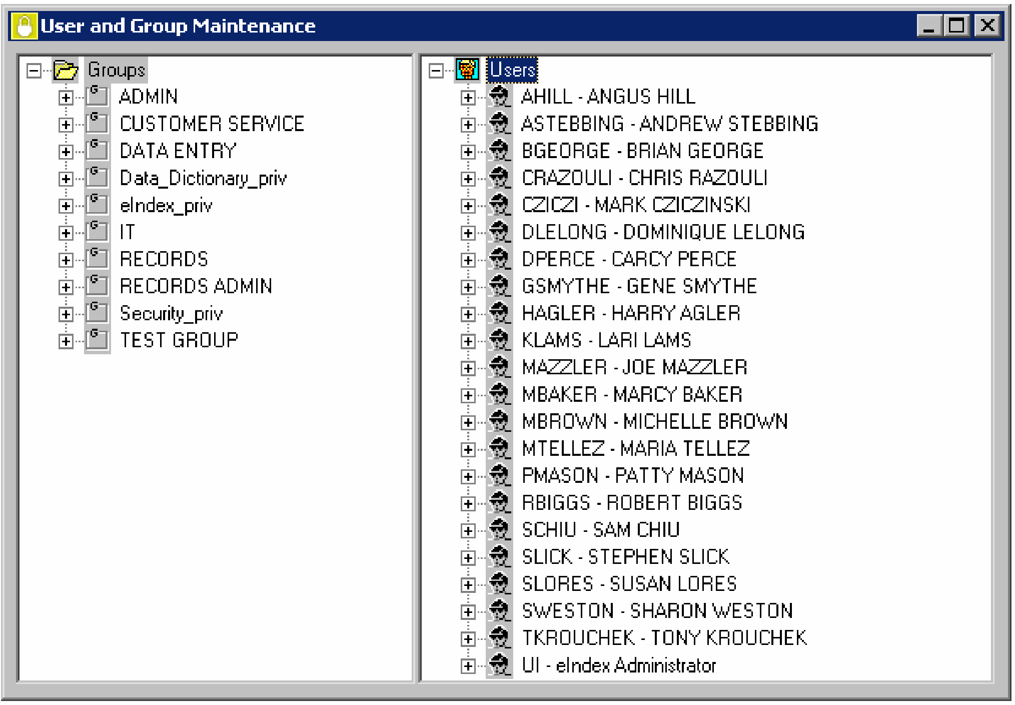
To save your changes and leave the User Properties window open, click **Save** or **Apply**. The changes are saved to the database.

To save your changes and close the User Properties window, click **OK**. The changes are saved to the database and the User and Group Maintenance window reappears.

Expiring a User Group

If a user group is no longer valid, you can expire the group. When you expire a group, any access permissions granted to the group are no longer valid. You may need to reassign user profiles to new user groups or verify user access permissions after you expire a user group.

Use the User and Group Maintenance window to expire a user group



Groups
- ADMIN
- CUSTOMER SERVICE
- DATA ENTRY
- Data_Dictionary_priv
- eIndex_priv
- IT
- RECORDS
- RECORDS ADMIN
- Security_priv
- TEST GROUP

Users
- AHILL - ANGUS HILL
- ASTEBBING - ANDREW STEBBING
- BGEORGE - BRIAN GEORGE
- CRAZOULI - CHRIS RAZOULI
- CZICZI - MARK CZICZINSKI
- DLELONG - DOMINIQUE LELONG
- DPERCE - CARCY PERCE
- GSMYTHE - GENE SMYTHE
- HAGLER - HARRY AGLER
- KLAMS - LARI LAMS
- MAZZLER - JOE MAZZLER
- MBAKER - MARCY BAKER
- MBROWN - MICHELLE BROWN
- MTELLEZ - MARIA TELLEZ
- PMASON - PATTY MASON
- RBIGGS - ROBERT BIGGS
- SCHIU - SAM CHIU
- SLICK - STEPHEN SLICK
- SLORES - SUSAN LORES
- SWESTON - SHARON WESTON
- TKROUCHEK - TONY KROUCHEK
- UI - eIndex Administrator

▶ To expire a user group

Before you begin:

✓ Obtain the name of the user group to be expired

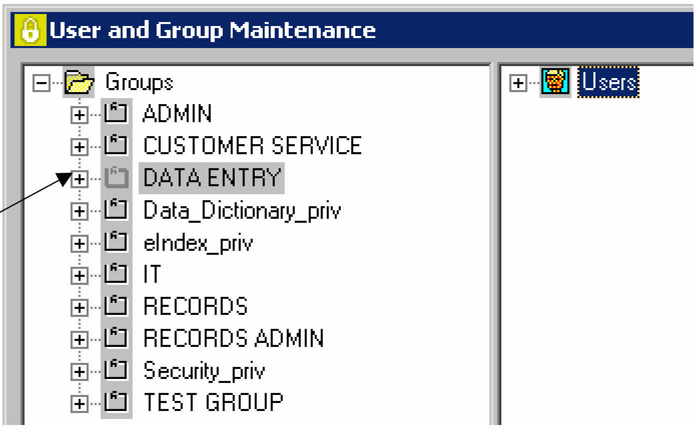
Access Setup tool

1 On the primary toolbar, click **Access Setup**. The User and Group Maintenance window appears.

2 Double-click the Groups list to display a list of existing groups.

Expire Group tool

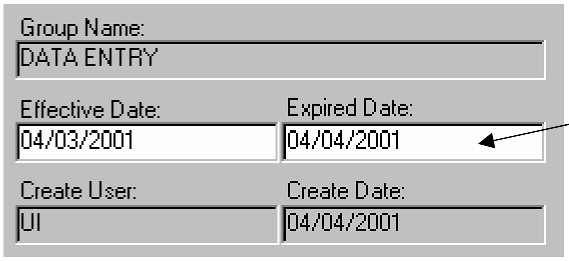
3 Select the name of the user group you want to expire, and click **Expire Group**. The icon for the selected group becomes grayed out to indicate that it is no longer active.



The icon for an expired user group is grayed out

Properties tool

4 To view the expiration date for the expired user group, click **Properties**. Today's date appears in the **Expired Date** field.



Group Name: DATA ENTRY

Effective Date: 04/03/2001

Expired Date: 04/04/2001

Create User: UI

Create Date: 04/04/2001

The date the user group was expired appears on the Group Properties window

***Tip:** You can also expire a user group by modifying the **Expired Date** directly. For more information, see "Modifying a User Group" earlier in this chapter.*

Reinstating an Expired User Group

You can reinstate an expired user group, if necessary. All previous user profile assignments are reinstated when you reinstate the group. If individual profiles were previously removed from the group, they are not reinstated when you reinstate the group.

▶ To reinstate an expired user group

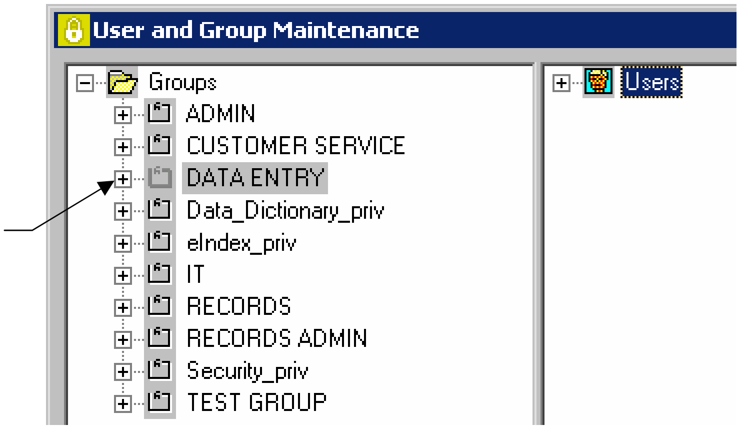
Before you begin:

✓ Obtain the name of the user group to be reinstated

Access Setup tool

1 On the primary toolbar, click **Access Setup**. The User and Group Maintenance window appears.

2 Double-click the Groups list to display a list of user groups.


User and Group Maintenance

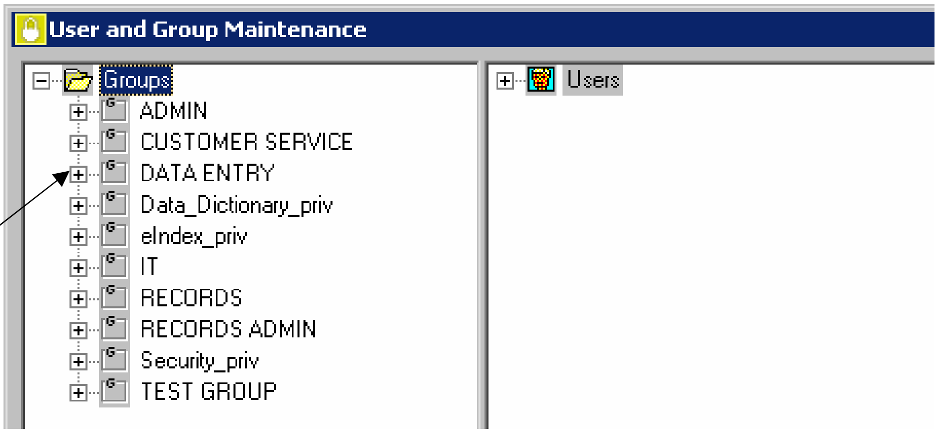
Groups
- ADMIN
- CUSTOMER SERVICE
- DATA ENTRY
- Data_Dictionary_priv
- eIndex_priv
- IT
- RECORDS
- RECORDS ADMIN
- Security_priv
- TEST GROUP

Users

The User and Group Maintenance window displays a list of all user groups

Activate Group tool

3 Select the user group to reinstate, and then click **Activate Group**. The icon for the user group is no longer grayed out, indicating that it is currently active.


User and Group Maintenance

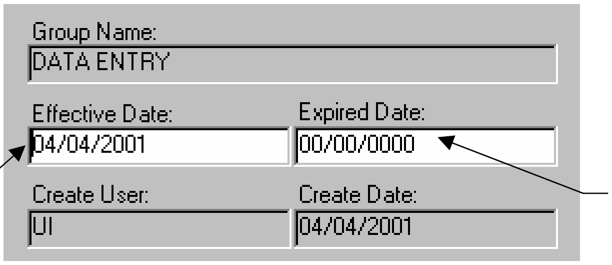
Groups
- ADMIN
- CUSTOMER SERVICE
- DATA ENTRY
- Data_Dictionary_priv
- eIndex_priv
- IT
- RECORDS
- RECORDS ADMIN
- Security_priv
- TEST GROUP

Users

The icon for the reactivated user group returns to its active state

Properties tool

4 To view the user group's new effective and expiration dates, click **Properties.** On the Group Properties window, the expiration date is 00/00/0000, and the effective date is the current date.


Group Name: DATA ENTRY

Effective Date: 04/04/2001
Expired Date: 00/00/0000

Create User: UI
Create Date: 04/04/2001

The effective date changes to today's date

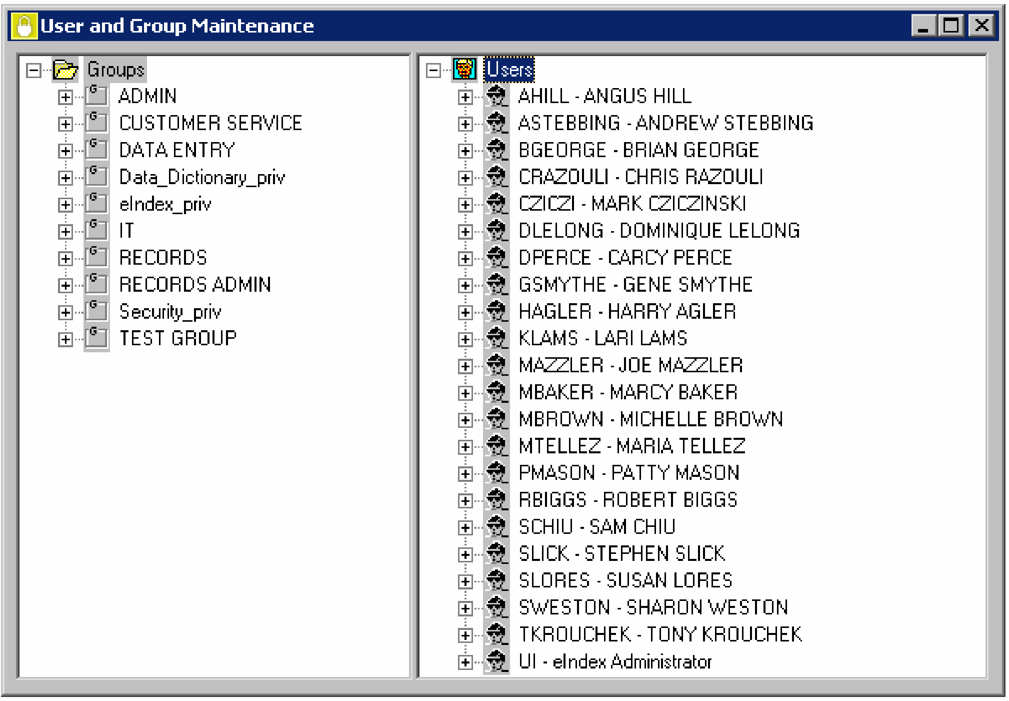
The expiration date becomes 00/00/0000

Tip: You can also reinstate a user group by modifying the ***Expired Date*** *directly. For more information, see "Modifying a User Group" earlier in this chapter.*

Expiring a User Profile

If a user profile is no longer valid, you can expire the profile. When you expire a user profile, that user can no longer log in to any e*Index applications.

Use the User and Group Maintenance window to expire user profiles



Groups
ADMIN
CUSTOMER SERVICE
DATA ENTRY
Data_Dictionary_priv
eIndex_priv
IT
RECORDS
RECORDS ADMIN
Security_priv
TEST GROUP

Users
AHILL - ANGUS HILL
ASTEBBING - ANDREW STEBBING
BGEORGE - BRIAN GEORGE
CRAZOULI - CHRIS RAZOULI
CZICZI - MARK CZICZINSKI
DLELONG - DOMINIQUE LELONG
DPERCE - CARCY PERCE
GSMYTHE - GENE SMYTHE
HAGLER - HARRY AGLER
KLAMS - LARI LAMS
MAZZLER - JOE MAZZLER
MBAKER - MARCY BAKER
MBROWN - MICHELLE BROWN
MTELLEZ - MARIA TELLEZ
PMASON - PATTY MASON
RBIGGS - ROBERT BIGGS
SCHIU - SAM CHIU
SLICK - STEPHEN SLICK
SLORES - SUSAN LORES
SWESTON - SHARON WESTON
TKROUCHEK - TONY KROUCHEK
UI - eIndex Administrator

▶ To expire a user profile

Before you begin:

✓ Obtain the name of the user profile to expire

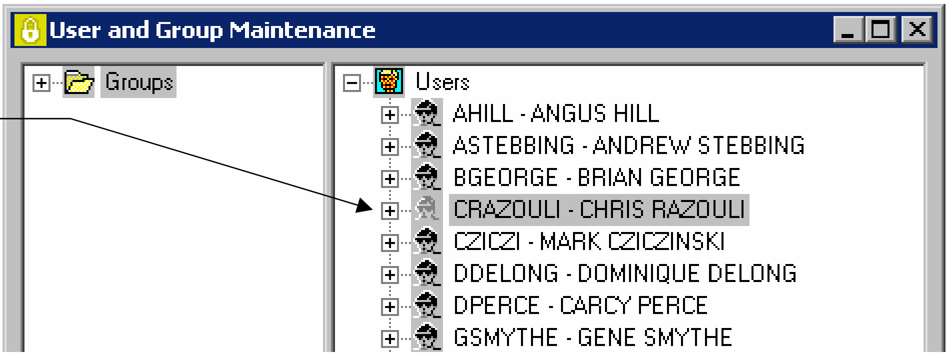
Access Setup tool

1 On the primary toolbar, click **Access Setup**. The User and Group Maintenance window appears.

2 Double-click the Users list to display a list of existing user profiles.

Expire User tool

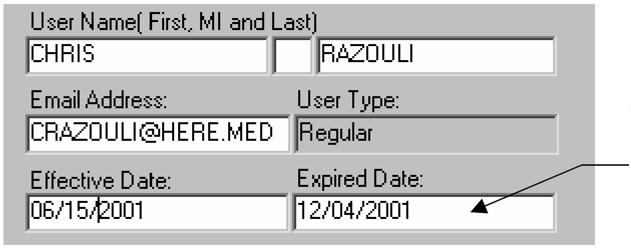
3 Select the name of the user profile you want to expire, and click **Expire User**. The icon for the selected user profile becomes grayed out to indicate that it is no longer active.



The icon for an expired user profile becomes grayed out

Properties tool

4 To view the expiration date for the expired user profile, click **Properties**. Today's date appears in the **Expired Date** field.



User Name(First, MI and Last)		
CHRIS		RAZOULI
Email Address:	User Type:	
CRAZOULI@HERE.MED	Regular	
Effective Date:	Expired Date:	
06/15/2001	12/04/2001	

The date the user profile was expired appears on the User Properties window

***Tip:** You can also expire a user profile by modifying the **Expired Date** directly. For more information, see "Modifying a User Profile" earlier in this chapter.*

Reinstating an Expired User Profile

You can reinstate an expired user profile, if necessary. All previous group assignments are reinstated when you reinstate the profile. If a user profile was previously removed from a particular group, it is not reassigned to that group when you reinstate the profile.

▶ To reinstate an expired user profile

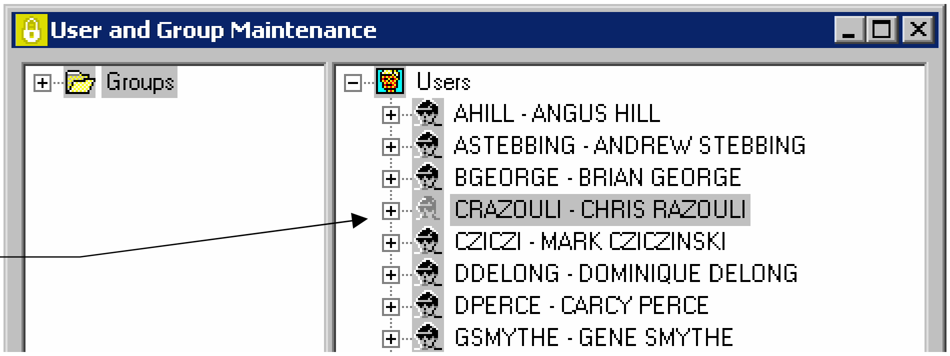
Before you begin:

✓ Obtain the name of the expired user profile to be reinstated

Access Setup tool

1 On the primary toolbar, click **Access Setup**. The User and Group Maintenance window appears.

2 Double-click the Users list to display a list of user profiles, and then highlight the user profile you want to reinstate.

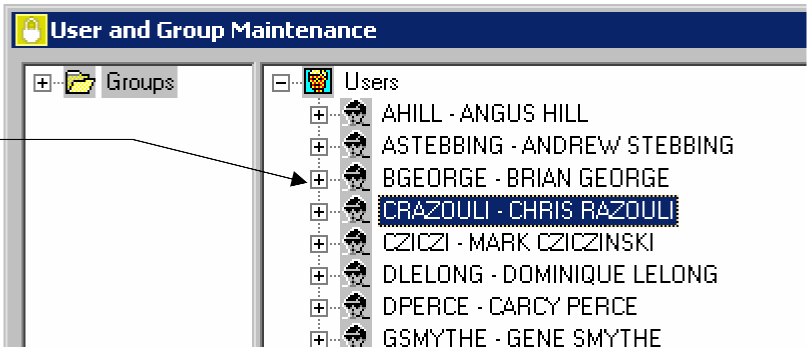


AHILL - ANGUS HILL
ASTEBBING - ANDREW STEBBING
BGEORGE - BRIAN GEORGE
CRAZOULI - CHRIS RAZOULI
CZICZI - MARK CZICZINSKI
DDELONG - DOMINIQUE DELONG
DPERCE - CARCY PERCE
GSMYTHE - GENE SMYTHE

The User and Group Maintenance window displays a list of all user profiles

Activate User tool

3 On the User Group Maintenance toolbar, click **Activate User**. The icon for the user profile is no longer grayed out, indicating that it is currently active.

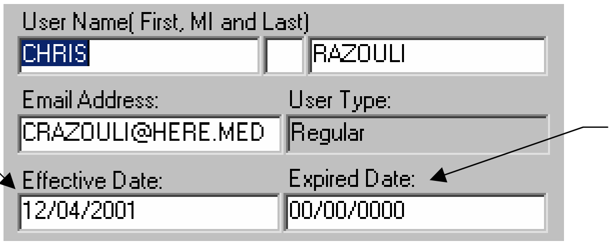


AHILL - ANGUS HILL
ASTEBBING - ANDREW STEBBING
BGEORGE - BRIAN GEORGE
CRAZOULI - CHRIS RAZOULI
CZICZI - MARK CZICZINSKI
DLELONG - DOMINIQUE LELONG
DPERCE - CARCY PERCE
GSMYTHE - GENE SMYTHE

The icon for the reactivated user profile returns to its active state

Properties tool

4 To view the new effective and expiration dates for the user profile, click **Properties**. On the User Properties window, the expiration date is 00/00/0000, and the effective date is the current date.



User Name(First, MI and Last)
CHRIS RAZOULI

Email Address: CRAZOULI@HERE.MED
User Type: Regular
Effective Date: 12/04/2001
Expired Date: 00/00/0000

The effective date changes to today's date

The expiration date becomes 00/00/0000

Tip: You can also reinstate a user profile by modifying the ***Expired Date*** *directly. For more information, see "Modifying a User Profile" earlier in this chapter.*

Maintaining User Access and Notification

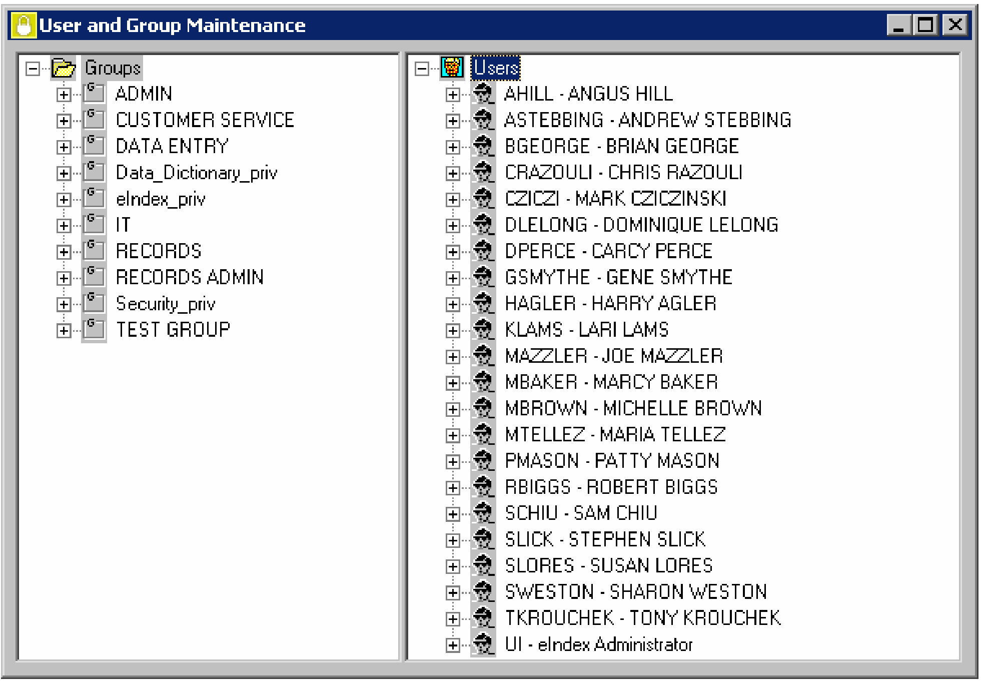
Overview

When user access requirements change, you may need to update their assigned access permissions, change the user group to which a user profile belongs, or change the events of which the user is currently notified. To maintain user access permissions and event notification for e*Index, you can perform any of the following tasks:

- Expire a user profile from a user group
- Reinstate a user profile to a user group
- Modify a users active dates in a user group
- Expire access permissions
- Reinstate access permissions
- Modify access permission active dates
- Remove event notification from a user profile

Expiring a User Profile from a User Group

If a user's responsibilities change, you may need to expire their user profile from one or more of the user groups to which it is assigned. When you expire a user profile from a user group, the user no longer has the access permissions of that user group.



Groups
- ADMIN
- CUSTOMER SERVICE
- DATA ENTRY
- Data_Dictionary_priv
- eIndex_priv
- IT
- RECORDS
- RECORDS ADMIN
- Security_priv
- TEST GROUP

Users
- AHILL - ANGUS HILL
- ASTEBBING - ANDREW STEBBING
- BGEORGE - BRIAN GEORGE
- CRAZOULI - CHRIS RAZOULI
- CZICZI - MARK CZICZINSKI
- DLELONG - DOMINIQUE LELONG
- DPERCE - CARCY PERCE
- GSMYTHE - GENE SMYTHE
- HAGLER - HARRY AGLER
- KLAMS - LARI LAMS
- MAZZLER - JOE MAZZLER
- MBAKER - MARCY BAKER
- MBROWN - MICHELLE BROWN
- MTELLEZ - MARIA TELLEZ
- PMASON - PATTY MASON
- RBIGGS - ROBERT BIGGS
- SCHIU - SAM CHIU
- SLICK - STEPHEN SLICK
- SLORES - SUSAN LORES
- SWESTON - SHARON WESTON
- TKROUCHEK - TONY KROUCHEK
- UI - eIndex Administrator

Use the User and Group Maintenance window to expire a user profile from a user group

▶ To expire a user profile from a user group

Before you begin:

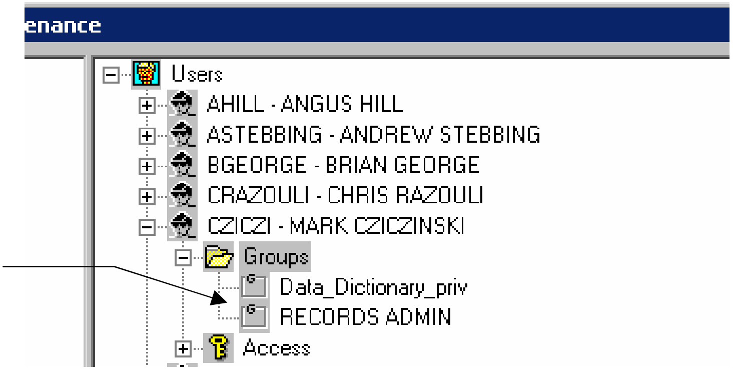
✓ Identify the user profile and the user group from which it should be expired

Access Setup tool

1 On the Primary toolbar, click **Access Setup**. The User and Group Maintenance window appears.

2 To expire the user from a user group using the Users list:

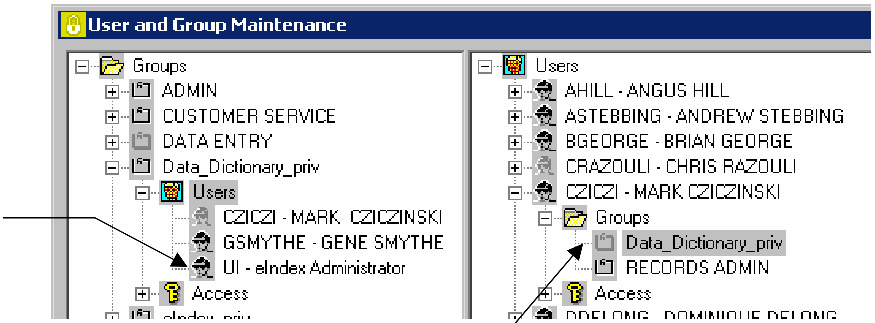
- Expand the Users list until the user group from which you want to expire the user profile appears under the user profile name.



Expand the Users list to display the user group from which you want to expire the user profile

Expire User/Group tool

- Select the name of the user group, and then click **Expire User/Group**. The user group icon is grayed out for the selected user profile. In the Groups list, the user profile icon becomes grayed out for the selected user group.

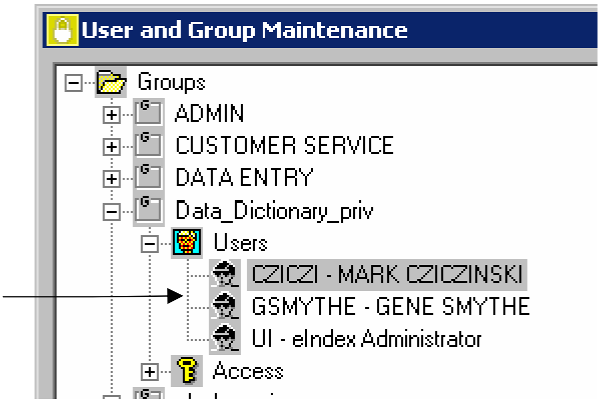


The icon for the user profile becomes grayed out under the user group

The icon for the user group becomes grayed out under the user profile

3 To expire the user profile from a user group using the Groups list:

- Expand the Groups list until the user profile you want to expire appears under the user group name.



Expand the Groups list to view the user profile you want to expire

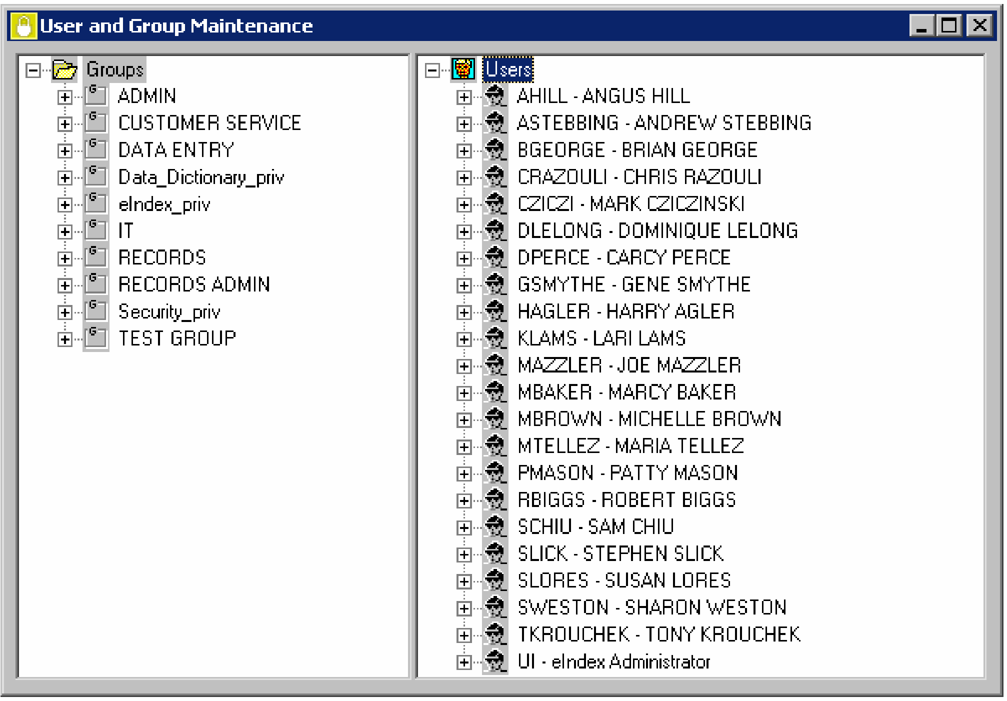
Expire Group/User tool

- Select the name of the user profile, and then click **Expire Group/User**. The icons become grayed out as described in step 2 to indicate the user profile is expired from the user group.

Tip: *You can also expire a user profile from a user group by modifying the expiration date on either the User\Group Properties window or the Group\User Properties window. For more information, see "Modifying a User's Active Dates in a User Group" later in this chapter.*

Reinstating a User Profile to a User Group

If a user profile is expired from a user group in error, or needs to be granted that group's access permissions again, you can reinstate the user profile to the user group. This action changes the effective date to the current date, and the expiration date to 00/00/0000.



Groups
- ADMIN
- CUSTOMER SERVICE
- DATA ENTRY
- Data_Dictionary_priv
- eIndex_priv
- IT
- RECORDS
- RECORDS ADMIN
- Security_priv
- TEST GROUP

Users
- AHILL - ANGUS HILL
- ASTEBBING - ANDREW STEBBING
- BGEORGE - BRIAN GEORGE
- CRAZOULI - CHRIS RAZOULI
- CZICZI - MARK CZICZINSKI
- DLELONG - DOMINIQUE LELONG
- DPERCE - CARCY PERCE
- GSMYTHE - GENE SMYTHE
- HAGLER - HARRY AGLER
- KLAMS - LARI LAMS
- MAZZLER - JOE MAZZLER
- MBAKER - MARCY BAKER
- MBROWN - MICHELLE BROWN
- MTELLEZ - MARIA TELLEZ
- PMASON - PATTY MASON
- RBIGGS - ROBERT BIGGS
- SCHIU - SAM CHIU
- SLICK - STEPHEN SLICK
- SLORES - SUSAN LORES
- SWESTON - SHARON WESTON
- TKROUCHEK - TONY KROUCHEK
- UI - eIndex Administrator

Use the User and Group Maintenance window to reinstate a user profile to a user group

▶ To reinstate a user profile to a user group

Before you begin:

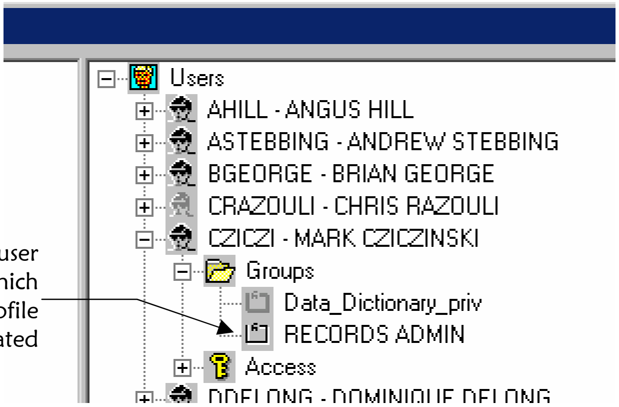
- ✓ Identify the user profile and the user group to which it should be reinstated

Access Setup tool

1 On the Primary toolbar, click **Access Setup**. The User and Group Maintenance window appears.

2 To reinstate the user to a user group using the Users list:

- Expand the Users list until the user group to which you want to reinstate the user profile appears under the user profile name.

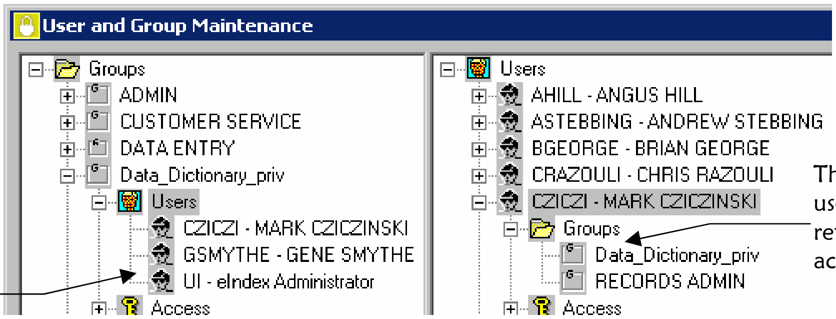


```
Users
  AHILL - ANGUS HILL
  ASTEBBING - ANDREW STEBBING
  BGEORGE - BRIAN GEORGE
  CRAZOULI - CHRIS RAZOULI
  CZICZI - MARK CZICZINSKI
    Groups
      Data_Dictionary_priv
      RECORDS ADMIN
    Access
  DDELONG - DOMINIQUE DELONG
```

Display the user group to which the user profile will be reinstated

Activate User/Group tool

- Select the name of the user group, and then click **Activate User/Group**. The user group icon returns to its active state for the selected user profile. In the Groups list, the user profile icon returns to its active state for the selected user group.



User and Group Maintenance

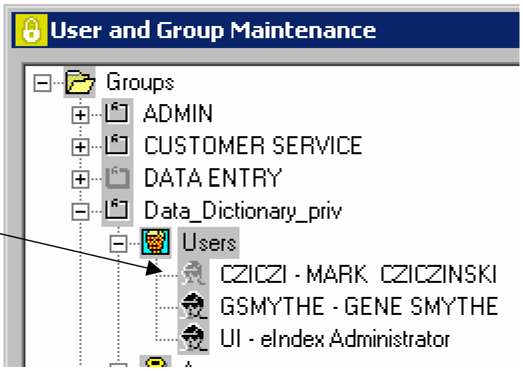
```
Groups                                  Users
  ADMIN                                   AHILL - ANGUS HILL
  CUSTOMER SERVICE                        ASTEBBING - ANDREW STEBBING
  DATA ENTRY                              BGEORGE - BRIAN GEORGE
  Data_Dictionary_priv                    CRAZOULI - CHRIS RAZOULI
    Users                                 CZICZI - MARK CZICZINSKI
      CZICZI - MARK CZICZINSKI              Groups
      GSMYTHE - GENE SMYTHE                   Data_Dictionary_priv
      UI - eIndex Administrator               RECORDS ADMIN
    Access                                  Access
```

The icon for the user profile returns to its active state

The icon for the user group returns to its active state

3 To reinstate the user profile to a user group using the Groups list:

- Expand the Groups list until the user profile you want to reinstate appears under the user group name.



User and Group Maintenance

```
Groups
  ADMIN
  CUSTOMER SERVICE
  DATA ENTRY
  Data_Dictionary_priv
    Users
      CZICZI - MARK  CZICZINSKI
      GSMYTHE - GENE SMYTHE
      UI - eIndex Administrator
```

Expand the Groups list to view the icon for the user profile to be reinstated

Activate Group/User tool

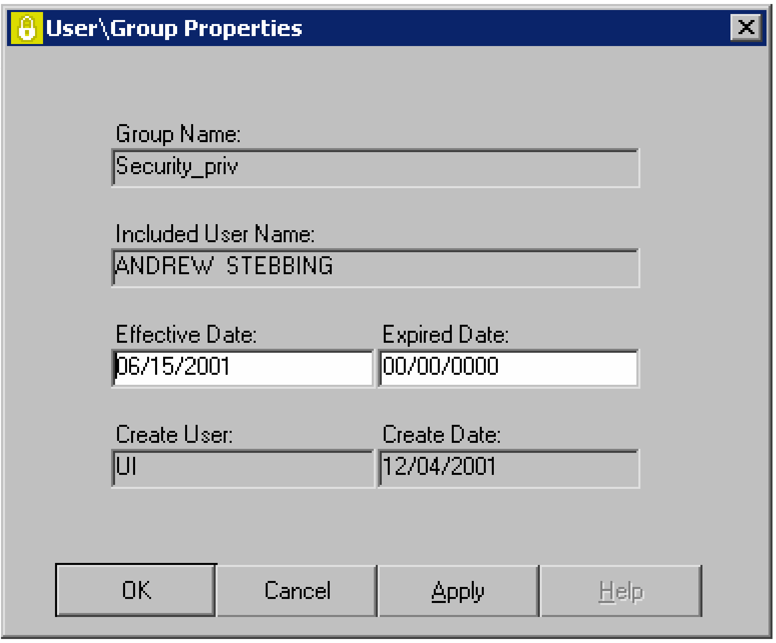
- Select the name of the user profile, and then click **Activate Group/User**. The user profile icon returns to its active state for the selected user group. In the Users list, the user group icon returns to its active state for the selected user profile.

Tip: *You can also reinstate a user profile to a user group by modifying the expiration date on either the User\Group Properties window or the Group\User Properties window. For more information, see "Modifying a User's Active Dates in a User Group" later in this chapter.*

Modifying a User's Active Dates in a User Group

When you add a user profile to a user group, you may want to specify a specific date on which the user profile should be activated in the user group or on which the user profile is automatically expired from the user group. You can do this by modifying the effective or expiration date on either the User\Group Properties window or the Group\User Properties window. Information updated on one window is automatically updated on the other.

Use the User\Group Properties window (or the Group\User Properties window) to modify a user's active dates within a user group


User\Group Properties

Group Name: Security_priv

Included User Name: ANDREW STEBBING

Effective Date: 06/15/2001

Expired Date: 00/00/0000

Create User: UI

Create Date: 12/04/2001

▶ To modify a user's active dates in a user group

Before you begin:

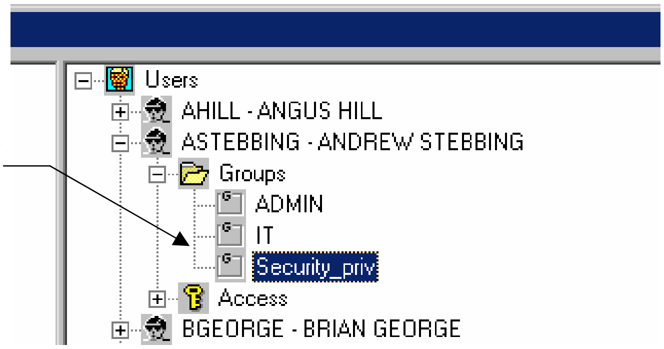
- ✓ Identify the user profile whose information you want to modify

Access Setup tool

1 On the Primary toolbar, click **Access Setup**. The User and Group Maintenance window appears.

2 To modify the information from the User\Group Properties window:

- Expand the Users list to display all user profiles, double-click the name of the user profile, and then double-click the Groups list beneath the user profile.



Expand the user profile's Groups list to see all user groups to which it is assigned

Properties tool

- Select the name of the user group for which you want to modify user assignment information, and then click **Properties**. The User\Group Properties window appears.
- Modify the date fields as needed (for more information about the fields on this window, see "About User\Group Properties Fields" earlier in this chapter).

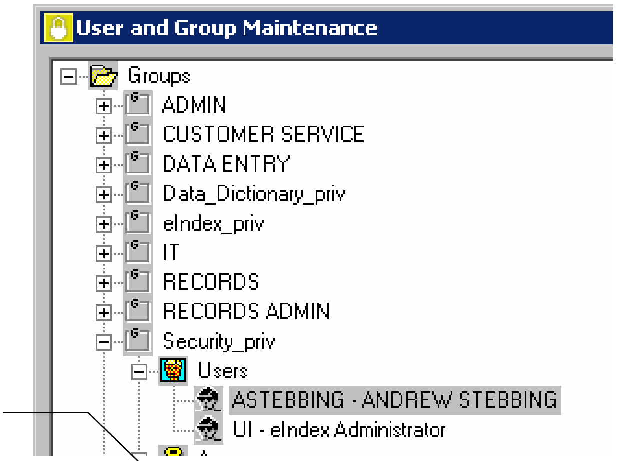
OK

OK button

- On the User\Group Properties window, click **OK**. The User\Group Properties window closes.

3 To modify the information from the Group\User Properties window:

- Expand the Groups list to display all user groups, double-click the name of the user group, and then double-click the Users list beneath the user profile.



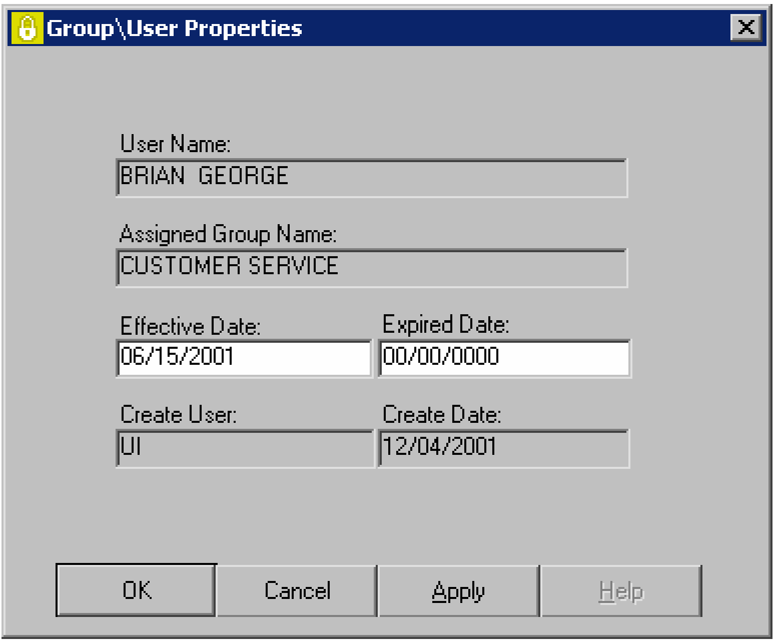
User and Group Maintenance

- Groups
  - ADMIN
  - CUSTOMER SERVICE
  - DATA ENTRY
  - Data_Dictionary_priv
  - eIndex_priv
  - IT
  - RECORDS
  - RECORDS ADMIN
  - Security_priv
    - Users
      - ASTEBBING - ANDREW STEBBING
      - UI - eIndex Administrator

Expand the user group's Users list

Properties tool

- Select the name of the user profile you want to modify, and then click **Properties**. The Group\User Properties window appears.



Group\User Properties

User Name:	BRIAN GEORGE
Assigned Group Name:	CUSTOMER SERVICE
Effective Date:	06/15/2001
Expired Date:	00/00/0000
Create User:	UI
Create Date:	12/04/2001

On the Group\User Properties window, modify expiration and effective dates for a user profile's user group assignments

- Modify the date fields as needed (for more information about these fields, see "About Group\User Properties Fields" earlier in this chapter).

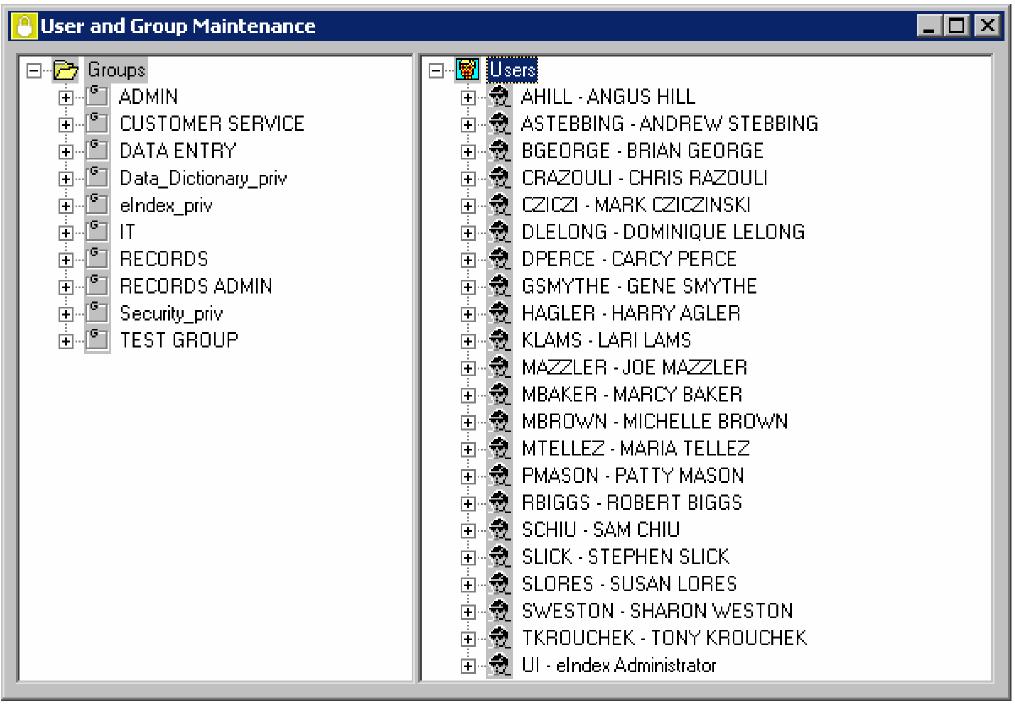
OK

OK button

- On the Group\User Properties window, click **OK**. The Group\User Properties window closes.

Expiring Access Permissions

If a user or user group no longer requires access to a specific function, you can expire their access to that function. If you know that a user or user group will no longer require access to a specific function as of a certain date in the future, you can specify an expiration date in advance. For more information about setting future expiration dates, see "Modifying Access Permission Active Dates" later in this chapter.



User and Group Maintenance

Groups

- ADMIN
- CUSTOMER SERVICE
- DATA ENTRY
- Data_Dictionary_priv
- eIndex_priv
- IT
- RECORDS
- RECORDS ADMIN
- Security_priv
- TEST GROUP

Users

- AHILL - ANGUS HILL
- ASTEBBING - ANDREW STEBBING
- BGEORGE - BRIAN GEORGE
- CRAZOULI - CHRIS RAZOULI
- CZICZI - MARK CZICZINSKI
- DLELONG - DOMINIQUE LELONG
- DPERCE - CARCY PERCE
- GSMYTHE - GENE SMYTHE
- HAGLER - HARRY AGLER
- KLAMS - LARI LAMS
- MAZZLER - JOE MAZZLER
- MBAKER - MARCY BAKER
- MBROWN - MICHELLE BROWN
- MTELLEZ - MARIA TELLEZ
- PMASON - PATTY MASON
- RBIGGS - ROBERT BIGGS
- SCHIU - SAM CHIU
- SLICK - STEPHEN SLICK
- SLORES - SUSAN LORES
- SWESTON - SHARON WESTON
- TKROUCHEK - TONY KROUCHEK
- UI - eIndex Administrator

Use the User and Group Maintenance window to expire access permissions from a user profile or user group

▶ To expire access permissions

Before you begin:

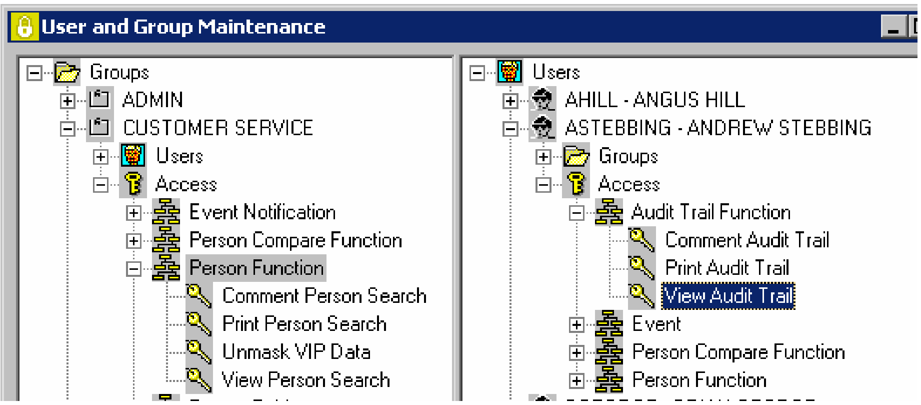
- ✓ Identify the kinds of access you need to expire for certain user profiles and user groups
- ✓ Make sure that the user profiles and user groups for whom you want to remove access have already been assigned the permissions

Access Setup tool

1. On the primary toolbar, click **Access Setup**. The User and Group Maintenance window appears.

2. Expand either the Groups or Users list until you see the user group or user profile from which you want to expire access permissions, and then double-click the name of the user profile or user group.

3 Double-click the access folder under the appropriate user group or user profile, and then double-click the function associated with the action you want to modify.

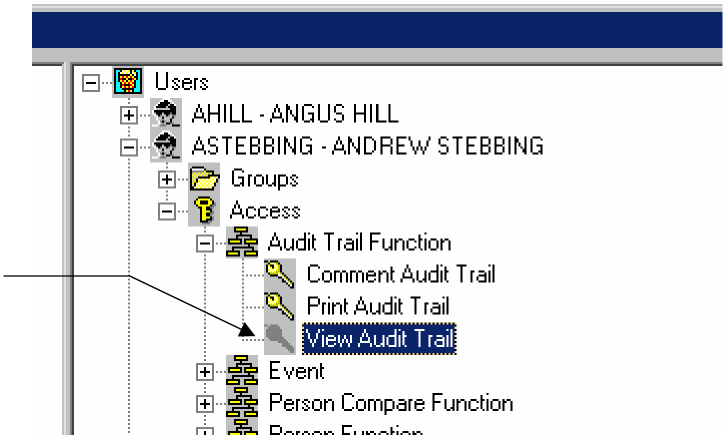


Expand the Users or Groups list to view the access permission you want to expire

4 Do one of the following:

Expire Current Access

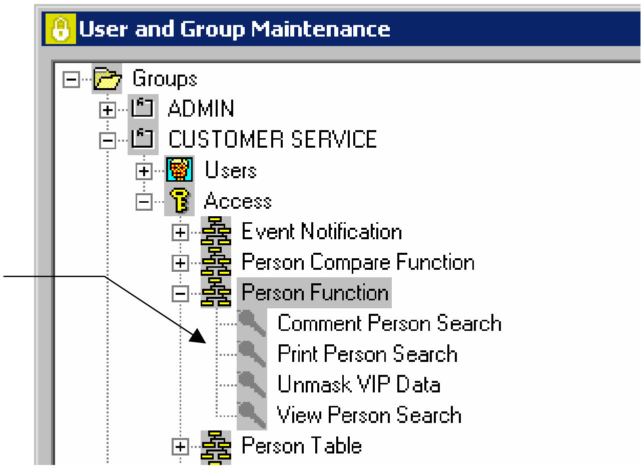
To expire access permission to only one action, select the access permission you want to expire, and then click **Expire Current Access**. The icon for the expired access permission is grayed out to indicate that it is not currently active.



The icon for the selected action (View Audit Trail) you expired becomes grayed out

Expire all Access tool

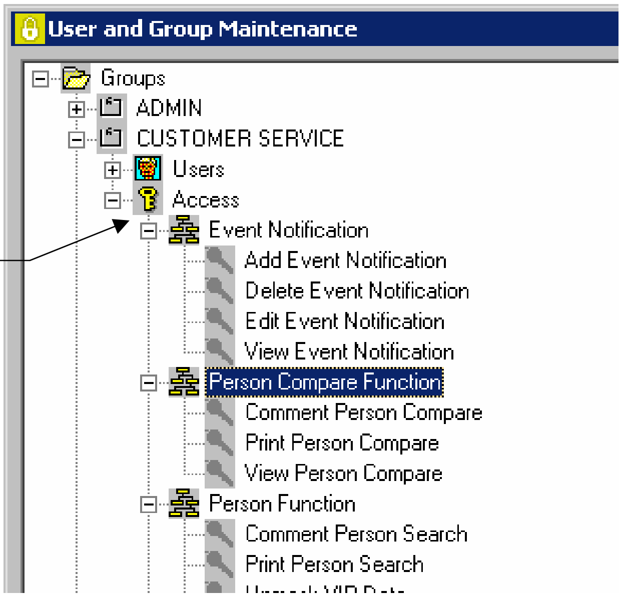
To expire access permissions to an entire function (such as the Person Compare Function) and all associated actions, select the function you want to expire and then click **Expire all Access**.



All icons under the selected function (Person Compare) become grayed out to indicate they are no longer active

Expire all Access Under Current Group tool

To expire all access permissions for the selected user profile or user group, select the Access list for the user profile or user group and then click **Expire all Access Under Current Group**.

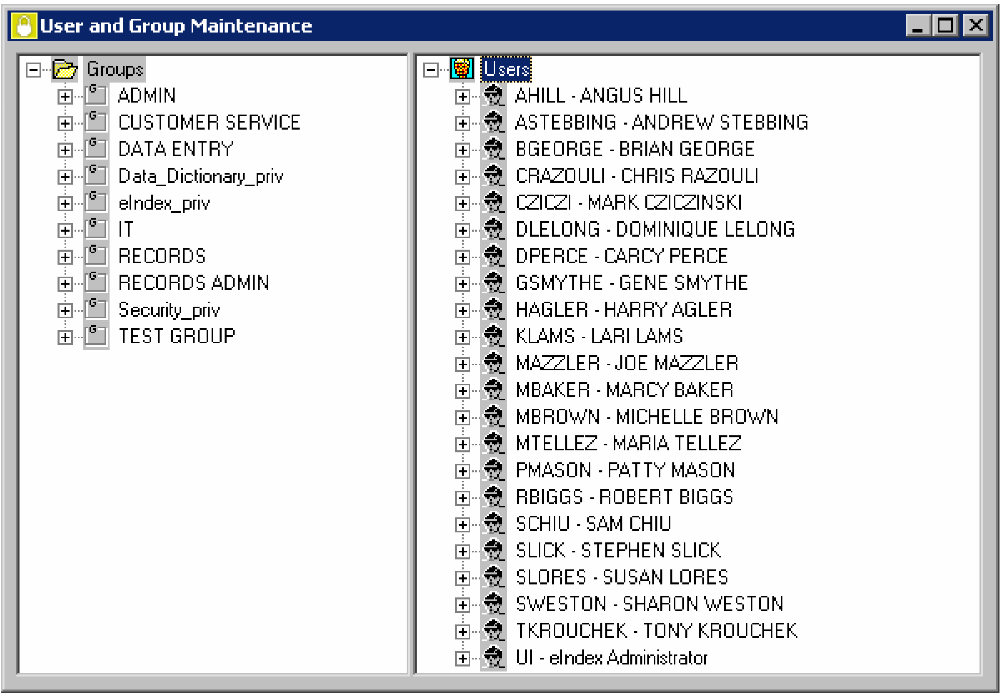


All icons under the selected Access list become grayed out to indicate they are no longer active

Tip: *You can also expire access permissions from user profiles and user groups by modifying the expiration date on the Access Properties window for either the user group or user profile. For more information, see "Modifying Access Permission Active Dates" later in this chapter.*

Reinstating Access Permissions

If necessary, you can restore previously expired access permissions to a user profile or user group. When you restore an access permission, the expiration date is removed and the current date is inserted as the new effective date.



User and Group Maintenance

- Groups
  - ADMIN
  - CUSTOMER SERVICE
  - DATA ENTRY
  - Data_Dictionary_priv
  - eIndex_priv
  - IT
  - RECORDS
  - RECORDS ADMIN
  - Security_priv
  - TEST GROUP

- Users
  - AHILL - ANGUS HILL
  - ASTEBBING - ANDREW STEBBING
  - BGEORGE - BRIAN GEORGE
  - CRAZOULI - CHRIS RAZOULI
  - CZICZI - MARK CZICZINSKI
  - DLELONG - DOMINIQUE LELONG
  - DPERCE - CARCY PERCE
  - GSMYTHE - GENE SMYTHE
  - HAGLER - HARRY AGLER
  - KLAMS - LARI LAMS
  - MAZZLER - JOE MAZZLER
  - MBAKER - MARCY BAKER
  - MBROWN - MICHELLE BROWN
  - MTELLEZ - MARIA TELLEZ
  - PMASON - PATTY MASON
  - RBIGGS - ROBERT BIGGS
  - SCHIU - SAM CHIU
  - SLICK - STEPHEN SLICK
  - SLORES - SUSAN LORES
  - SWESTON - SHARON WESTON
  - TKROUCHEK - TONY KROUCHEK
  - UI - eIndex Administrator

Use the User and Group Maintenance window to reinstate access permissions to a user profile or user group

▶ To reinstate access permissions

Before you begin:

- ✓ Identify the kinds of access you need to reinstate for certain user profiles and user groups
- ✓ Make sure that the user profiles and user groups for whom you want to reinstate access have already had the appropriate permissions expired

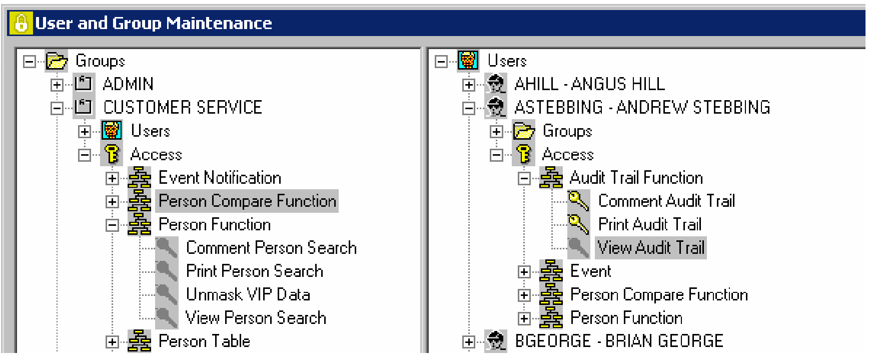
Access Setup tool

1. On the primary toolbar, click **Access Setup**. The User and Group Maintenance window appears.

2. Expand either the Groups or Users list, and then double-click the user group or user profile to which you want to reinstate access permissions.

3. Double-click the Access list under the selected user group or user profile, and then double-click the function name associated with the access permission you want to reinstate.

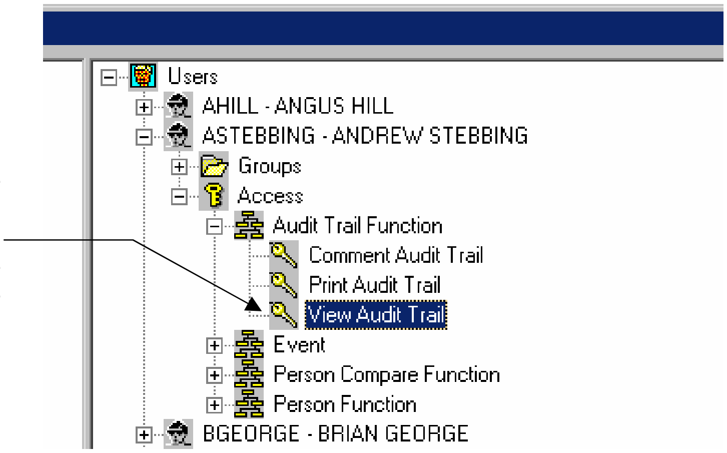
Expand the Users or Groups list to view the access permission you want to reinstate



5 Do one of the following:

Activate Current Access

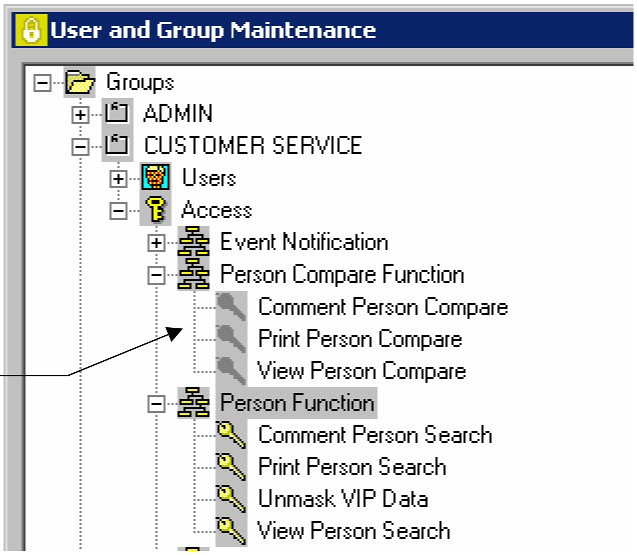
To reinstate access permission to only one action, select the access permission you want to reinstate, and then click **Activate Current Access**. The icon for the expired access permission returns to its active state.



The icon for the access permission you reactivated returns to its active state

Activate all Access tool

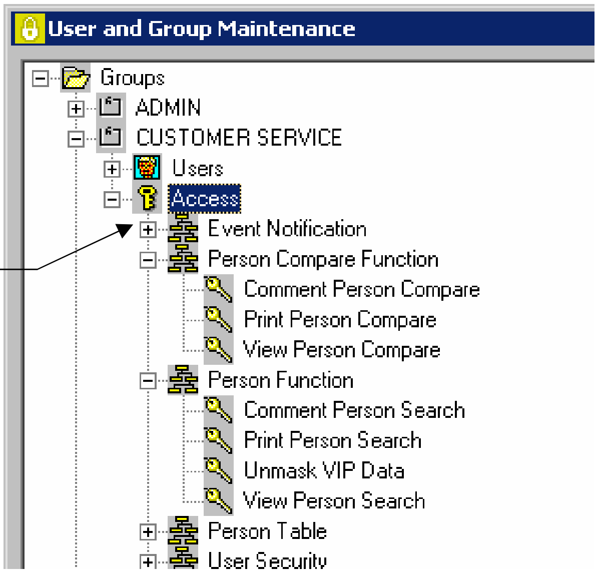
To reinstate access permissions to an entire function (such as the Person Compare Function) and all associated actions, select the function you want to reinstate and then click **Activate all Access**.



All icons under the selected function return to their active states to indicate they are activate again

Activate all Access Under Current Group tool

To reinstate access permissions to all actions for a user group or user profile, select the Access list of the user group or user profile and then click **Activate all Access Under Current Group**.

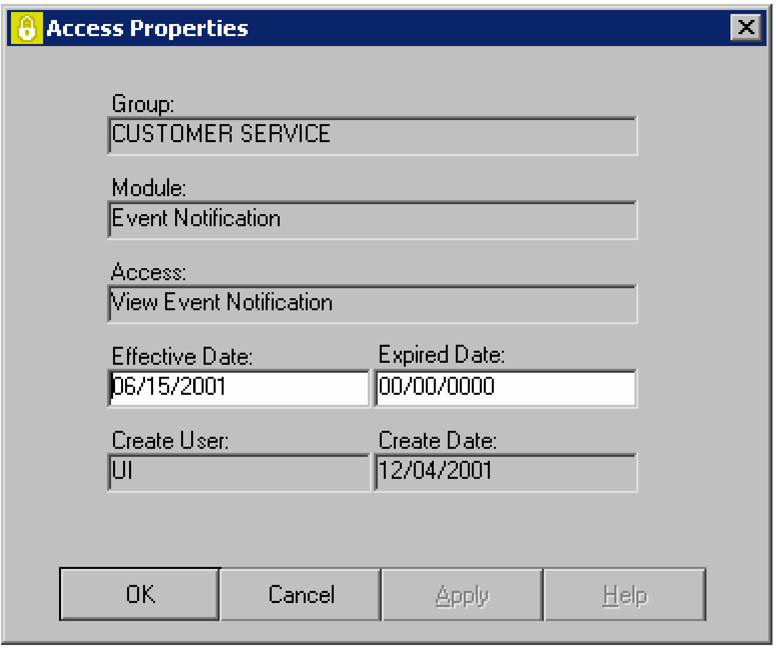


All icons under the selected Access list return to their active state to indicate they are active again

Tip: *You can also reinstate access permissions to user profiles and user groups by modifying the expiration date on either the Access Properties window for the group or profile. For more information, see "Modifying Access Permission Active Dates" later in this chapter.*

Modifying Access Permission Active Dates

By modifying the active dates for an access permission granted to a user profile or user group, you can specify that the access permission is not available to the user group or user profile until a future date. You can also specify the current date or a future date for the access permission to expire from the user group or user profile.



Group: CUSTOMER SERVICE

Module: Event Notification

Access: View Event Notification

Effective Date: 06/15/2001

Expired Date: 00/00/0000

Create User: UI

Create Date: 12/04/2001

Modify the effective and expiration dates for an access permission on the Access Properties window

▶ To modify access properties

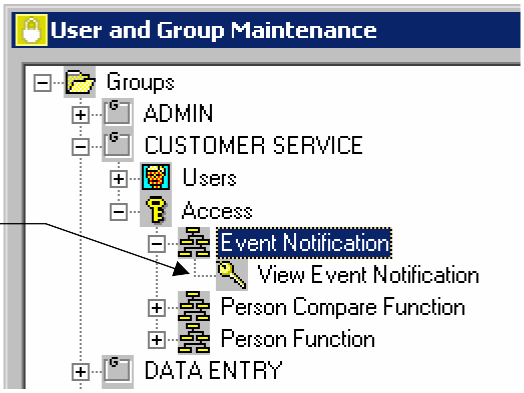
Before you begin:

- ✓ Identify the kinds of access you need to modify for certain user profiles and user groups
- ✓ Make sure that the user profiles and user groups for whom you want to modify access properties already have the appropriate access permissions assigned

Access Setup tool

1. On the primary toolbar, click **Access Setup**. The User and Group Maintenance window appears.
2. Expand either the Groups or Users list, and then double-click the user group or user profile for which you want to modify access permission dates.

3 Double-click the Access folder for the appropriate user group or user profile, and then double-click the name of the function associated with the access permission you want to modify.



Expand the Access list to view a list of access permissions

Properties tool

4 Select the access permission you want to modify, and click **Properties**. The Access Properties window appears.

5 Modify any of the date fields on the Access Properties window (for more information, see "About Access Properties Fields" earlier in this chapter).

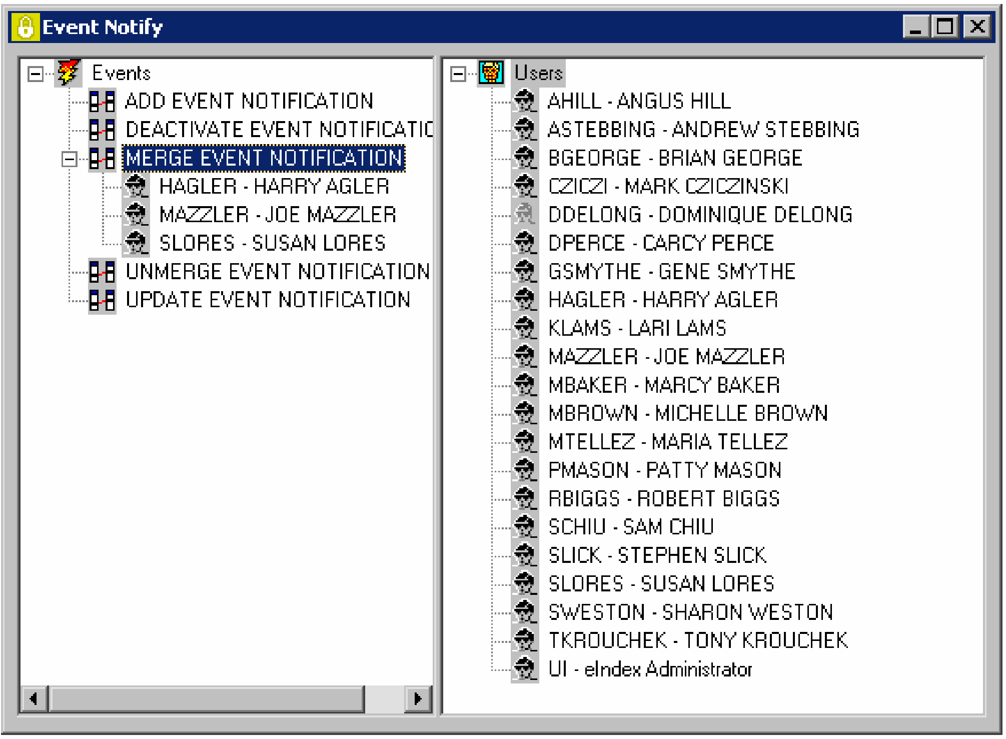
OK

OK button

6 On the Access Properties window, click **OK**. The Access Properties window closes and the User and Group Maintenance window reappears. If you expired the access permission, the associated icon is grayed out to indicate the permission is inactive.

Removing Event Notification from a User Profile

When a user no longer requires notification of certain events for which they are currently receiving emails, you can remove the user profile from the appropriate event notification lists.



Event Notify

Events
- ADD EVENT NOTIFICATION
- DEACTIVATE EVENT NOTIFICATIC
- MERGE EVENT NOTIFICATION
  - HAGLER - HARRY AGLER
  - MAZZLER - JOE MAZZLER
  - SLORES - SUSAN LORES
- UNMERGE EVENT NOTIFICATION
- UPDATE EVENT NOTIFICATION

Users
- AHILL - ANGUS HILL
- ASTEBBING - ANDREW STEBBING
- BGEORGE - BRIAN GEORGE
- CZICZI - MARK CZICZINSKI
- DDELONG - DOMINIQUE DELONG
- DPERCE - CARCY PERCE
- GSMYTHE - GENE SMYTHE
- HAGLER - HARRY AGLER
- KLAMS - LARI LAMS
- MAZZLER - JOE MAZZLER
- MBAKER - MARCY BAKER
- MBROWN - MICHELLE BROWN
- MTELLEZ - MARIA TELLEZ
- PMASON - PATTY MASON
- RBIGGS - ROBERT BIGGS
- SCHIU - SAM CHIU
- SLICK - STEPHEN SLICK
- SLORES - SUSAN LORES
- SWESTON - SHARON WESTON
- TKROUCHEK - TONY KROUCHEK
- UI - eIndex Administrator

Use the Event Notify window to remove event notifications from user profiles

▶ To remove event notifications from user profiles

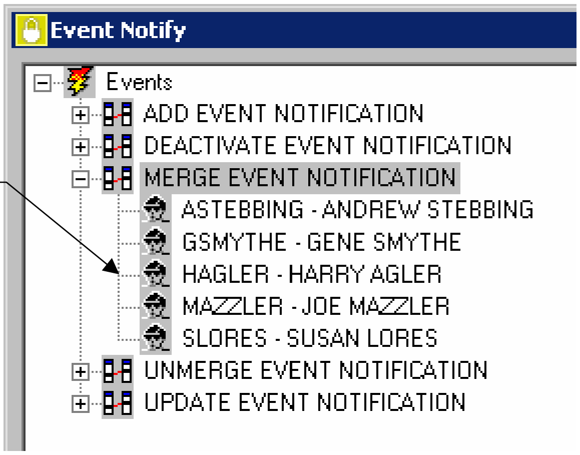
Before you begin:

✓ Identify the users who no longer need to receive all of their currently assigned email notifications

Event Notification tool

1 On the primary toolbar, click **Event Notification**. The Event Notify window appears, displaying a list of events for which users can be notified on the left and a list of existing user profiles on the right.

2 In the Event list on the left side of the window, expand the event for which you want to remove notification.

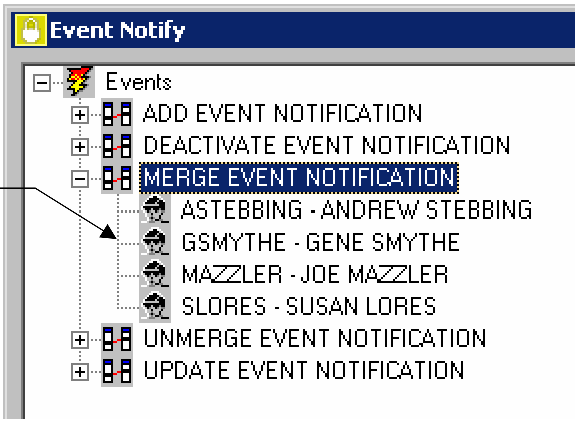


Highlight the user profile to be removed from the event notification list

3 Do one of the following:

Remove Current User tool

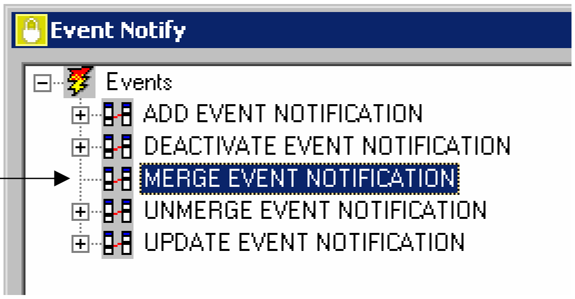
To remove notification for a single user, select the appropriate user profile and then click **Remove Current Users**. The user profile is removed from the event.



The selected user profile, HAGLER is removed from the list

Remove All Users tool

To remove the event notification for all users, select the event from which you want to remove all user profiles and then click **Remove All Users**. All user profiles that were previously assigned the selected event are removed.


Event Notify
Events
ADD EVENT NOTIFICATION
DEACTIVATE EVENT NOTIFICATION
MERGE EVENT NOTIFICATION
UNMERGE EVENT NOTIFICATION
UPDATE EVENT NOTIFICATION

All user profiles are removed from the selected event's notification list

Configuring Security Parameters

Overview

When e*Index Security is installed at your location, the control keys are set to their default values. You may need to modify these values to suit your security requirements. Configuring your control keys is a 2-step process.

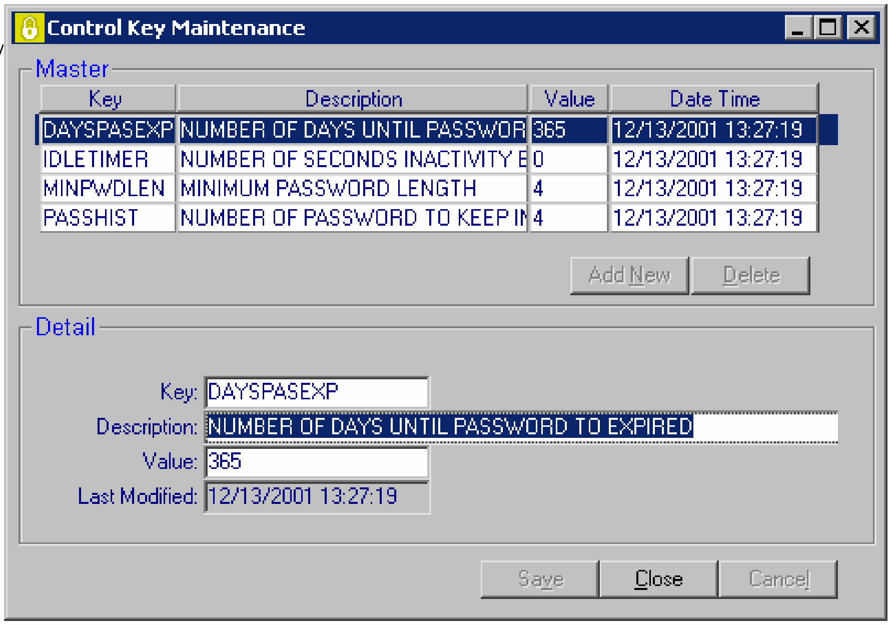
- Step 1: Determine Your Configuration Requirements
- Step 2: Modify Control Key Values

Step1: Determine Your Configuration Requirements

Before you begin to modify your control key values, you should determine the values that will best suit your security requirements. Analyze your current internal security policies to determine the most appropriate values for the control keys. Before you begin, review the control key descriptions under "About Control Key Values" later in this chapter. Your SeeBeyond project manager can also help you determine the appropriate values for your system.

Step 2: Modify Control Key Values

You can modify the value of any existing control key in e*Index Security. Before you modify these values, you should perform an analysis of how your changes may affect processing.



Key	Description	Value	Date Time
DAYSPASEXP	NUMBER OF DAYS UNTIL PASSWOR	365	12/13/2001 13:27:19
IDLETIMER	NUMBER OF SECONDS INACTIVITY E	0	12/13/2001 13:27:19
MINPWDLEN	MINIMUM PASSWORD LENGTH	4	12/13/2001 13:27:19
PASSHIST	NUMBER OF PASSWORD TO KEEP IN	4	12/13/2001 13:27:19

Key: DAYSPASEXP
Description: NUMBER OF DAYS UNTIL PASSWORD TO EXPIRED
Value: 365
Last Modified: 12/13/2001 13:27:19

Use the Control Key Maintenance window to modify control key values in e*Index Security

▶ To modify control key values

Before you begin:

✓ Complete "Step1: Determine Your Configuration Requirements"

Control Key tool

1 On the Primary toolbar, click **Control Key**. The Control Key Maintenance window appears.

2 In the upper portion of the Control Key Maintenance window, select the control key you want to modify. The detailed information for that key appears in the lower portion of the window.

3 In the lower portion of the window, modify the control key value (for more information, see “About Control Key Fields” and "About Control Key Values" following this procedure).

Save tool

4 When you have filled in the fields, click **Save**. Your changes are saved to the database.

About Control Key Fields

The control key fields, located on the Control Key Maintenance window, allow you to specify the values you want to associate with each control key.

In this field …	type or select …
Description	A short description of the control key. This description is predefined, but you can modify it if desired.
Value	The value associated with the selected control key (for more information about the keys and their default values, see "About Control Key Values" following this section).

This field …	displays this information …
Key	The name of the control key you are modifying.
Last Modified	The date that the control key was created or was last updated.

About Control Key Values

When you modify control keys, you typically only need to modify the value of the control key. The table below lists and describes each control key along with their default values.

This control key ...	allows you to ...
DAYSPASEXP	Specify the length of time (in days) a password can be active. At the end of the predetermined time period, the password expires and the user is prompted to enter a new password upon logging on to the system. Default: **365**
MINPWDLEN	Specify a minimum password length that is enforced by e*Index Security. A warning message appears when a user creates a password that does not meet the minimum number of characters allowable, and the user is prompted for a different password. Default: **4**
IDLETIMER	Specify a period of inactivity (in seconds) after which any of the e*Index applications automatically signs a user off. For example, if this value is set to **15**, and a user is running e*Index Administrator, then the application will close automatically if it is not used for 15 seconds. This does not apply to the security application, which closes automatically after 10 minutes of inactivity regardless of the value of this control key. Default: **0**
PASSHIST	Define a specific number of passwords that are retained in each user's password history. A history of passwords per user is maintained in the database, and passwords that still exist in the password history cannot be reused. Current passwords are not stored in the password history table. Default: **4**

Appendix A

Access Permission Definitions

About this Appendix

Overview

This appendix provides descriptions for each of the access permissions that you can assign to the users of the e*Index applications. The permissions are categorized by e*Index application and then by the functions that appear in the Access List of e*Index Security.

e*Index Global Identifier Access Permissions

The following access permissions appear in the Access List of e*Index Security and allow users to perform specific functions in the e*Index Global Identifier GUI.

Alias Access Permissions

This access permission …	**allows a user to …**
Add Alias	Add an alias to a member profile on the View/Edit Person window. To activate this permission, you must also grant access to the View Person Search permission (located in Person Function).
Delete Alias	Delete an alias from a member profile on the View/Edit Person window. To activate this permission, you must also grant access to the View Person Search permission (located in Person Function).
Edit Alias	Modify information about an alias on the View/Edit Person window. To activate this permission, you must also grant access to the View Person Search permission (located in Person Function).

Audit Log Access Permissions

This access permission ...	allows a user to ...
View Audit Log	Perform a search for audit log entries and view the search results. This permission also gives you the ability to view details about the audit log entries.

Audit Trail Function Access Permissions

This access permission ...	allows a user to ...
Comment Audit Trail	View and add comments from the Audit Trail window. To activate this permission, you must also grant the View Audit Trail permission.
Print Audit Trail	Print member histories from the Audit Trail window. To activate this permission, you must also grant the View Audit Trail permission.
View Audit Trail	View member histories on the Audit Trail window.

Comments Access Permissions

This access permission ...	allows a user to ...
Add Comments	Add comments to a member profile from the Potential Duplicate, Comparison, Merge, and Audit Trail windows. In order to activate this permission, you must also grant access to view one of these functions and to view the comments for that function. Note: The access permission to give users the ability to view comments from the Merge window is the Comment Person Compare permissions under the Person Compare function.
Delete Comments	Delete comments from a member profile from the Potential Duplicate, Comparison, Merge, and Audit Trail windows. In order to activate this permission, you must also grant access to view one of these functions and to view the comments for that function.
Print Comments	Print comments for a member profile from the Potential Duplicate, Comparison, Merge, and Audit Trail windows. In order to activate this permission, you must also grant access to view one of these functions and to view the comments for that function.

Local ID Access Permissions

This access permission ...	allows a user to ...
Add New Local ID	Add new local identifier and system pairs to member profiles. To activate this permission, you must also grant the View Local ID permission and the View Person Search permission (located in Person Function).
Deactivate Local ID	Deactivate existing local identifier and system pairs in member profiles. To activate this permission, you must also grant the View Local ID permission and the View Person Search permission (located in Person Function).
Edit Local ID	Modify local identifier and system pairs to member profiles. To activate this permission, you must also grant the View Local ID permission and the View Person Search permission (located in Person Function).
View Local ID	View a member's local identifiers on the Local ID tab of the View/Edit Persons window. To activate this permission, you must also grant the View Person Search permission (located in Person Function).

Merge Access Permissions

This access permission ...	allows a user to ...
View Merge	View member profiles on the Merge window. This permission does not allow you to perform a Merge. To assign merge privileges, you must grant the Merge Potential Duplicates permission (located in Potential Duplicate Function).

Person Compare Access Permissions

This access permission ...	allows a user to ...
Comment Person Compare	View and add comments associated with the member profiles displayed on the Compare Persons or Merge Persons window. To activate this permission, you must also grant the View Person Compare permission or the View Merge permission.
Print Person Compare	Print a comparison of the member profiles displayed on the Compare Persons window. To activate this permission, you must also grant the View Person Compare permission.
View Person Compare	View a comparison of two member profiles on the Compare Persons window.

Person Detail Access Permissions

This access permission ...	allows a user to ...
Print Person Detail	Print detailed information about member profiles from the View/Edit Person window. To activate this permission, you must also grant the View Person Search permission (located under Person Function).

Person Function Access Permissions

This access permission ...	allows a user to ...
Comment Person Search	View, add, and delete comments from the View/Edit Person window. To activate this permission, you must also grant the View Person Search permission.
Print Person Search	Print a list of member profiles returned from a search on the Search window. To activate this permission, you must also grant the View Person Search permission.
Unmask VIP Data	View all data for member profiles with a VIP status of VIP or employee (otherwise, certain data is hidden). To activate this permission, you must also grant the View Person Search permission.
View Person Search	Perform a search for member profiles and view the results list. This permissions also grants permission to view detailed information about member profiles on the View/Edit Person window. This does not grant permission to view local ID and systems assigned to a user profile.

Person Table Access Permissions

This access permission ...	allows a user to ...
Add Person	Add new member profiles to the e*Index database using the Add Person window.
Deactivate Person	Deactivate member profiles using the View/Edit Person window. To activate this permission, you must also grant the View Person Search permission (located under Person Function).
Edit Person	Modify information about members using the View/Edit Person window. To activate this permission, you must also grant the View Person Search permission (located under Person Function).

Potential Duplicate Function Access Permissions

This access permission …	allows a user to …
Associated Record Potential Duplicate	Print the records displayed on the Associated Records dialog. This dialog appears when you select a potential duplicate pair with multiple associated potential duplicates. To activate this permission, you must also grant the View Potential Duplicate permission
Comment Potential Duplicate	View and add comments associated with the member profiles displayed on the Potential Duplicate Compare window. To activate this permission, you must also grant the View Potential Duplicate permission or the View Merge permission.
Merge Potential Duplicate	Merge two potential duplicate profiles that are displayed on the Potential Duplicate Compare, Merge Persons, or Compare Persons window. To activate this permission, you must also grant the View Potential Duplicate, View Merge, or View Person Compare permission.
Print Potential Duplicate	Print potential duplicate comparisons from the Potential Duplicate Compare window. To activate this permission, you must also grant the View Potential Duplicate permission.
Resolved Potential Duplicate	Resolve potential duplicates that you determine are not duplicates of one another (on either the Potential Duplicate Compare window or the Compare Persons window). To activate this permission, you must also grant the View Potential Duplicate permission or the View Person Compare permission.
View Potential Duplicate	Perform a search for potential duplicates, and view the results list and side-by-side comparisons of potential duplicate records.

UnMerge Function Access Permissions

This access permission …	allows a user to …
View UnMerge	Unmerge two member profiles that were previously merged.

e*Index Administrator Access Permissions

The following access permissions appear in the Access List of e*Index Security and allow users to perform specific functions in the e*Index Administrator GUI.

Address Type Access Permissions

this access permission ...	allows a user to ...
Add Address Type	Add new address types in Common Table Maintenance. To activate this permission, you must also grant the View Address Type permission.
Delete Address Type	Delete existing address types in Common Table Maintenance. To activate this permission, you must also grant the View Address Type permission.
Edit Address Type	Modify information about existing address types in Common Table Maintenance. To activate this permission, you must also grant the View Address Type permission.
View Address Type	View information about the existing address types in Common Table Maintenance.

Citizenship Access Permissions

This access permission ...	allows a user to ...
Add Citizenship	Add new citizenships in Common Table Maintenance. To activate this permission, you must also grant the View Citizenship permission.
Delete Citizenship	Delete existing citizenships in Common Table Maintenance. To activate this permission, you must also grant the View Citizenship permission.
Edit Citizenship	Modify information about existing citizenships in Common Table Maintenance. To activate this permission, you must also grant the View Citizenship permission.
View Citizenship	View information about the existing citizenships in Common Table Maintenance.

Configurable Query Access Permissions

This access permission ...	allows a user to ...
Add Configurable Query	This access permission is not currently active, but may be used for future functionality.
Delete Configurable Query	This access permission is not currently active, but may be used for future functionality.
Edit Configurable	Edit queries in the Configurable Query function. To activate this function, you must also grant access to the View Configurable Query permission.
View Configurable Query	View queries in the Configurable Query function.

Control Key Table Access Permissions

This access permission ...	allows a user to ...
Add Control Key	Add new control keys to e*Index on the Control Key Maintenance window. To activate this permission, you must also grant the View Control Key permission. It is not recommended that you grant this permission to users.
Delete Control Key	Delete control keys from e*Index on the Control Key Maintenance window. To activate this permission, you must also grant the View Control Key permission. It is strongly recommended that you do not grant this permission to any user.
Edit Control Key	Edit the values of the system parameters on the Control Key Maintenance window. To activate this permission, you must also grant the View Control Key permission.
View Control Key	View the system parameters for e*Index on the Control Key Maintenance window.

Country Specific Option Access Permissions

This access permission ...	allows a user to ...
Edit Country Specific Option	Modify the configuration settings on the Country Specific Options window. To activate this permission, you must also grant the View Country Specific Options permission.
View Country Specific Option	View the configuration settings on the Country Specific Options window.

Country Table Access Permissions

This access permission ...	allows a user to ...
Add Country	Add new countries in Common Table Maintenance. To activate this permission, you must also grant the View Country permission.
Delete Country	Delete existing countries in Common Table Maintenance. To activate this permission, you must also grant the View Country permission.
Edit Country	Modify information about existing countries in Common Table Maintenance. To activate this permission, you must also grant the View Country permission.
View Country	View information about the existing countries in Common Table Maintenance.

Department Table Access Permissions

This access permission ...	allows a user to ...
Add Department	Add new departments in Common Table Maintenance. To activate this permission, you must also grant the View Department permission.
Delete Department	Delete existing departments in Common Table Maintenance. To activate this permission, you must also grant the View Department permission.
Edit Department	Modify information about existing departments in Common Table Maintenance. To activate this permission, you must also grant the View Department permission.
View Department	View information about the existing departments in Common Table Maintenance.

Display Configuration Access Permissions

This access permission ...	allows a user to ...
Add Display Configuration	This access permission is not currently active, but may be used for future functionality.
Delete Display Configuration	This access permission is not currently active, but may be used for future functionality.
Edit Display Configuration	Edit field labels in the Display Configuration function. To activate this function, you must also grant access to the View Display Configuration permission.

This access permission ...	allows a user to ...
View Display Configuration	View field labels in the Display Configuration function.

District of Residence Access Permissions

This access permission ...	allows a user to ...
Add District of Residence	Add new districts of residence (DORs) in Common Table Maintenance. To activate this permission, you must also grant the View District of Residence permission.
Delete District of Residence	Delete existing DORs in Common Table Maintenance. To activate this permission, you must also grant the View District of Residence permission.
Edit District of Residence	Modify information about existing DORs in Common Table Maintenance. To activate this permission, you must also grant the View District of Residence permission.
View District of Residence	View information about the existing DORs in Common Table Maintenance.

Driver License Issuer Access Permissions

This access permission ...	allows a user to ...
Add Driver License Issuer	Add new driver license issuers in Common Table Maintenance. To activate this permission, you must also grant the View Driver License Issuer permission.
Delete Driver License Issuer	Delete existing driver license issuers in Common Table Maintenance. To activate this permission, you must also grant the View Driver License Issuer permission.
Edit Driver License Issuer	Modify information about existing driver license issuers in Common Table Maintenance. To activate this permission, you must also grant the View Driver License Issuer permission.
View Driver License Issuer	View information about the existing driver license issuers in Common Table Maintenance.

Ethnic Table Access Permissions

This access permission ...	allows a user to ...
Add Ethnicity	Add new ethnicities in Common Table Maintenance. To activate this permission, you must also grant the View Ethnicity permission.
Delete Ethnicity	Delete existing ethnicities in Common Table Maintenance. To activate this permission, you must also grant the View Ethnicity permission.
Edit Ethnicity	Modify information about existing ethnicities in Common Table Maintenance. To activate this permission, you must also grant the View Ethnicity permission.
View Ethnicity	View information about the existing ethnicities in Common Table Maintenance.

Event Access Permissions

This access permission ...	allows a user to ...
Add Event	Add new events in Common Table Maintenance. To activate this permission, you must also grant the View Event permission.
Delete Event	Delete existing events in Common Table Maintenance. To activate this permission, you must also grant the View Event permission.
Edit Event	Modify information about existing events in Common Table Maintenance. To activate this permission, you must also grant the View Event permission.
View Event	View information about the existing events in Common Table Maintenance.

Event Notification Access Permissions

This access permission ...	allows a user to ...
Add Event Notification	Add new event notification codes in Common Table Maintenance. To activate this permission, you must also grant the View Event Notification permission.
Delete Event Notification	Delete existing event notification codes in Common Table Maintenance. To activate this permission, you must also grant the View Event Notification permission.

This access permission ...	allows a user to ...
Edit Event Notification	Modify information about existing event notification codes in Common Table Maintenance. To activate this permission, you must also grant the View Event Notification permission.
View Event Notification	View information about the existing event notification codes in Common Table Maintenance.

Gender Table Access Permissions

This access permission ...	allows a user to ...
Add Gender	Add new genders in Common Table Maintenance. To activate this permission, you must also grant the View Sex permission.
Delete Gender	Delete existing genders in Common Table Maintenance. To activate this permission, you must also grant the View Sex permission.
Edit Gender	Modify information about existing genders in Common Table Maintenance. To activate this permission, you must also grant the View Sex permission.
View Gender	View information about the existing genders in Common Table Maintenance.

Language Table Access Permissions

This access permission ...	allows a user to ...
Add Language	Add new languages in Common Table Maintenance. To activate this permission, you must also grant the View Language permission.
Delete Language	Delete existing languages in Common Table Maintenance. To activate this permission, you must also grant the View Language permission.
Edit Language	Modify information about existing languages in Common Table Maintenance. To activate this permission, you must also grant the View Language permission.
View Language	View information about the existing languages in Common Table Maintenance.

Location Table Access Permissions

This access permission ...	allows a user to ...
Add Location	Add new locations in Common Table Maintenance. To activate this permission, you must also grant the View Location permission.
Delete Location	Delete existing locations in Common Table Maintenance. To activate this permission, you must also grant the View Location permission.
Edit Location	Modify information about existing locations in Common Table Maintenance. To activate this permission, you must also grant the View Location permission.
View Location	View information about the existing locations in Common Table Maintenance.

Marital Status Access Permissions

This access permission ...	allows a user to ...
Add Marital Status	Add new marital statuses in Common Table Maintenance. To activate this permission, you must also grant the View Marital Status permission.
Delete Marital Status	Delete existing marital statuses in Common Table Maintenance. To activate this permission, you must also grant the View Marital Status permission.
Edit Marital Status	Modify information about existing marital statuses in Common Table Maintenance. To activate this permission, you must also grant the View Marital Status permission.
View Marital Status	View information about the existing marital statuses in Common Table Maintenance.

Nationality Access Permissions

This access permission ...	allows a user to ...
Add Nationality	Add new nationalities in Common Table Maintenance. To activate this permission, you must also grant the View Nationality permission.
Delete Nationality	Delete existing nationalities in Common Table Maintenance. To activate this permission, you must also grant the View Nationality permission.
Edit Nationality	Modify information about existing nationalities in Common Table Maintenance. To activate this permission, you must also grant the View Nationality permission.

This access permission ...	allows a user to ...
View Nationality	View information about the existing nationalities in Common Table Maintenance.

Non-unique Identifier Access Permissions

This access permission ...	allows a user to ...
Add Non-unique ID	Add new non-unique ID types in NonUnique ID Definition Maintenance. To activate this permission, you must also grant the View Non-unique ID permission.
Delete Non-unique ID	Delete existing non-unique ID types in NonUnique ID Definition Maintenance. To activate this permission, you must also grant the View Non-unique ID permission.
Edit Non-unique ID	Modify information about existing non-unique ID types in NonUnique ID Definition Maintenance. To activate this permission, you must also grant the View Non-unique ID permission.
View Non-unique ID	View information about the existing non-unique ID types in NonUnique ID Definition Maintenance.

Person Category Access Permissions

This access permission ...	allows a user to ...
Add Person Category	Add new person categories in Common Table Maintenance. To activate this permission, you must also grant the View Person Category permission.
Delete Person Category	Delete existing person categories in Common Table Maintenance. To activate this permission, you must also grant the View Person Category permission.
Edit Person Category	Modify information about existing person categories in Common Table Maintenance. To activate this permission, you must also grant the View Person Category permission.
View Person Category	View information about the existing person categories in Common Table Maintenance.

Phone Type Access Permissions

This access permission ...	allows a user to ...
Add Phone Type	Add new phone types in Common Table Maintenance. To activate this permission, you must also grant the View Phone Types permission.
Delete Phone Type	Delete existing phone types in Common Table Maintenance. To activate this permission, you must also grant the View Phone Types permission.
Edit Phone Type	Modify information about existing phone types in Common Table Maintenance. To activate this permission, you must also grant the View Phone Types permission.
View Phone Type	View information about the existing phone types in Common Table Maintenance.

Pre-defined Messages Access Permissions

This access permission ...	allows a user to ...
Add Pre-defined Messages	Add new predefined messages in Pre-defined Msg Maintenance. To activate this permission, you must also grant the View Pre-defined Messages permission.
Delete Pre-defined Messages	Delete existing predefined messages in Pre-defined Msg Maintenance. To activate this permission, you must also grant the View Pre-defined Messages permission.
Edit Pre-defined Messages	Modify information about existing predefined messages in Pre-defined Msg Maintenance. To activate this permission, you must also grant the View Pre-defined Messages permission.
View Pre-defined Messages	View information about the existing predefined messages in Pre-defined Msg Maintenance.

Race Table Access Permissions

This access permission ...	allows a user to ...
Add Race	Add new races in Common Table Maintenance. To activate this permission, you must also grant the View Race permission.
Delete Race	Delete existing races in Common Table Maintenance. To activate this permission, you must also grant the View Race permission.

This access permission ...	allows a user to ...
Edit Race	Modify information about existing races in Common Table Maintenance. To activate this permission, you must also grant the View Race permission.
View Race	View information about the existing races in Common Table Maintenance.

Region Table Access Permissions

This access permission ...	allows a user to ...
Add Region	Add new regions in Common Table Maintenance. To activate this permission, you must also grant the View Region permission.
Delete Region	Delete existing regions in Common Table Maintenance. To activate this permission, you must also grant the View Region permission.
Edit Region	Modify information about existing regions in Common Table Maintenance. To activate this permission, you must also grant the View Region permission.
View Region	View information about the existing regions in Common Table Maintenance.

Religion Table Access Permissions

This access permission ...	allows a user to ...
Add Religion	Add new religions in Common Table Maintenance. To activate this permission, you must also grant the View Religion permission.
Delete Religion	Delete existing religions in Common Table Maintenance. To activate this permission, you must also grant the View Religion permission.
Edit Religion	Modify information about existing religions in Common Table Maintenance. To activate this permission, you must also grant the View Religion permission.
View Religion	View information about the existing religions in Common Table Maintenance.

Rule Set Access Permissions

This access permission ...	allows a user to ...

This access permission ...	**allows a user to ...**
Edit Rule Set	Modify rule set information and load new rule set files in the Rule Set Maintenance function, and modify the content of the rule set files in the View File Content function. To activate this permission, you must also grant the View Rule Set permission. Important! Editing the Vality rule sets requires a very strong knowledge of the Vality matching algorithm and how it is implemented in e*Index. This permission should be granted sparingly.
View Rule Set	View information in Rule Set Maintenance about the Vality rule sets that are available to the matching algorithm. This access permission also allows users to view the rule set files in the View File Content function.

Source Table Access Permissions

This access permission ...	**allows a user to ...**
Add Source	Add new sources in Common Table Maintenance. To activate this permission, you must also grant the View Source permission.
Delete Source	Delete existing sources in Common Table Maintenance. To activate this permission, you must also grant the View Source permission.
Edit Source	Modify information about existing sources in Common Table Maintenance. To activate this permission, you must also grant the View Source permission.
View Source	View information about the existing sources in Common Table Maintenance.

State Code Access Permissions

This access permission ...	**allows a user to ...**
Add State	Add new states in Common Table Maintenance. To activate this permission, you must also grant the View State permission.
Delete State	Delete existing states in Common Table Maintenance. To activate this permission, you must also grant the View State permission.
Edit State	Modify information about existing states in Common Table Maintenance. To activate this permission, you must also grant the View State permission.

This access permission ...	allows a user to ...
View State	View information about the existing states in Common Table Maintenance.

Status Table Access Permissions

This access permission ...	allows a user to ...
Add Status	Add new member statuses in Common Table Maintenance. To activate this permission, you must also grant the View Status permission.
Delete Status	Delete existing member statuses in Common Table Maintenance. To activate this permission, you must also grant the View Status permission.
Edit Status	Modify information about existing member statuses in Common Table Maintenance. To activate this permission, you must also grant the View Status permission.
View Status	View information about the existing member statuses in Common Table Maintenance.

Suffix Table Access Permissions

This access permission ...	allows a user to ...
Add Suffix	Add new suffix in Common Table Maintenance. To activate this permission, you must also grant the View Suffix permission.
Delete Suffix	Delete existing suffixes in Common Table Maintenance. To activate this permission, you must also grant the View Suffix permission.
Edit Suffix	Modify information about existing suffix in Common Table Maintenance. To activate this permission, you must also grant the View Suffix permission.
View Suffix	View information about the existing suffix in Common Table Maintenance.

System Messages Access Permissions

This access permission ...	allows a user to ...
Add System Messages	Add new system messages in System Message Maintenance. To activate this permission, you must also grant the View System Messages permission.

This access permission ...	allows a user to ...
Delete System Messages	Delete existing system messages in System Message Maintenance. To activate this permission, you must also grant the View System Messages permission.
Edit System Messages	Modify information about existing system messages in System Message Maintenance. To activate this permission, you must also grant the View System Messages permission.
View System Messages	View information about the existing system messages in System Message Maintenance.

System Table Access Permissions

This access permission ...	allows a user to ...
Add System	Add new systems in System Maintenance. To activate this permission, you must also grant the View System permission.
Delete System	Delete existing systems in System Maintenance. To activate this permission, you must also grant the View System permission.
Edit System	Modify information about existing systems in System Maintenance. To activate this permission, you must also grant the View System permission.
View System	View information about the existing systems in System Maintenance.

Title Table Access Permissions

This access permission ...	allows a user to ...
Add Title	Add new titles in Common Table Maintenance. To activate this permission, you must also grant the View Title permission.
Delete Title	Delete existing titles in Common Table Maintenance. To activate this permission, you must also grant the View Title permission.
Edit Title	Modify information about existing titles in Common Table Maintenance. To activate this permission, you must also grant the View Title permission.
View Title	View information about the existing titles in Common Table Maintenance.

Veteran Status Table Access Permissions

This access permission …	**allows a user to …**
Add Veteran Status	Add new veteran statuses in Common Table Maintenance. To activate this permission, you must also grant the View Veteran Status permission.
Delete Veteran Status	Delete existing veteran statuses in Common Table Maintenance. To activate this permission, you must also grant the View Veteran Status permission.
Edit Veteran Status	Modify information about existing veteran statuses in Common Table Maintenance. To activate this permission, you must also grant the View Veteran Status permission.
View Veteran Status	View information about the existing veteran statuses in Common Table Maintenance.

VIP Table Access Permissions

This access permission …	**allows a user to …**
Add VIP	Add new VIP statuses in Common Table Maintenance. To activate this permission, you must also grant the View VIP permission.
Delete VIP	Delete existing VIP statuses in Common Table Maintenance. To activate this permission, you must also grant the View VIP permission.
Edit VIP	Modify information about existing VIP statuses in Common Table Maintenance. To activate this permission, you must also grant the View VIP permission.
View VIP	View information about the existing VIP statuses in Common Table Maintenance.

Zip Code Access Permissions

This access permission …	**allows a user to …**
Add Zip Code	Add new zip codes in Zip Code Maintenance. To activate this permission, you must also grant the View Zip Code permission.
Delete Zip Code	Delete existing zip codes in Zip Code Maintenance. To activate this permission, you must also grant the View Zip Code permission.
Edit Zip Code	Modify information about existing zip codes in Zip Code Maintenance. To activate this permission, you must also grant the View Zip Code permission.
View Zip Code	View information about the existing zip codes in Zip Code Maintenance.

e*Index Security Access Permissions

The following access permissions appear in the Access List of e*Index Security and allow users to perform specific functions in the e*Index Security GUI.

Group Access Access Permissions

this access permission ...	allows a user to ...
Add Group Access	Add access permissions to a user group on the User and Group Maintenance window. To activate this permission, you must also grant the View Group permission in the Group Access function.
Edit Group Access	Activate and expire access permissions in a user group on the User and Group Maintenance window. To activate this permission, you must also grant the View Group permission in the Group Access function.
View Group Access	View the Access list for a user group on the User and Group Maintenance window. This access permission also allows you to view the Access Properties windows for user groups.

Group Security Access Permissions

This access permission ...	allows a user to ...
Add Group	Add a user group in the User and Group Maintenance function. To activate this permission, you must also grant access to the View Group permission in the Group Security function.
Edit Group	Edit information about a user group, including effective and expiration dates, in the User and Group Maintenance function. To activate this permission, you must also grant access to the View Group permission in the Group Security function.
View Group	View user groups on the User and Group Maintenance window. This permission also allows you to view the User Group Properties window.

Security Control Table Access Permissions

This access permission ...	allows a user to ...
Edit Security Control Key	Modify the values assigned to the security system parameters on the Control Key Maintenance window. To activate this permission, you must also grant the View Security Control Key permission
View Security Control Key	View the security system parameters defined on the Control Key Maintenance window.

User Access Access Permissions

This access permission ...	allows a user to ...
Add User Access	Add access permissions to a user profile on the User and Group Maintenance window. To activate this permission, you must also grant the View User Access permission.
Edit User Access	Activate and expire access permissions in a user profile on the User and Group Maintenance window. To activate this permission, you must also grant the View User Access permission.
View User Access	View the Access list for a user profile on the User and Group Maintenance window. This access permission also allows you to view the Access Properties windows for user profile.

User Security Access Permissions

This access permission ...	allows a user to ...
Add User	Add a user profile in the User and Group Maintenance function. To activate this permission, you must also grant access to the View User permission.
Edit User	Edit information about a user profile, including effective and expiration dates, in the User and Group Maintenance function. To activate this permission, you must also grant access to the View User permission.
View User	View user groups on the User and Group Maintenance window. This permission also allows you to view the User Properties window.

User-Group Security Access Permissions

This access permission ...	allows a user to ...
Add User-Group	Add a user profile in the User and Group Maintenance function. To activate this permission, you must also grant access to the View User-Group permission.
Edit User-Group	Expire and activate user profiles in user groups in the User and Group Maintenance function. To activate this permission, you must also grant access to the View User-Group permission.
View User-Group	View the Users list for a user group or the User Groups list for a user profile on the User and Group Maintenance window. This permission also allows you to view the User\Group Properties and Group\User Properties windows.

Glossary of Terms

Access permission

The ability to perform a specific action or function defined in e*Index Security. You can grant access permissions to user profiles and user groups.

Action

A specific task within an e*Index function to which users can be granted access. For example, viewing potential duplicates and merging potential duplicates are each a specific action within the potential duplicate function. Actions are also known as *sub-modules*.

Application window

All e*Index Security windows except for the first window that appears. Application windows are used for specific functions and purposes, such as adding user profiles and assigning access permissions.

Application window toolbar

The application window toolbar is located beneath the primary toolbar and is unique to each application window. This toolbar contains tools for various functions that you can perform from the active application window.

Balloon help

A description of each toolbar button that appears when you hold the mouse pointer briefly over the button.

Control keys

A set of system parameters that control Security configuration. These keys allow you to customize how your system processes passwords and to define the length of time that an instance of e*Index Security can remain inactive before the application shuts down

Control table

The maintenance function that allows you to configure certain aspects of e*Index Security, such as a minimum password length, a period of time after which a user must change their password, and so on.

Entity

A specific instance of an entity type. For example, information about John Smith is a specific instance (an entity) within a set of users (entity type). Information about the Audit Trail module is a specific instance (an entity) within the set of modules (entity type).

Entity type

An object of interest about which data can be collected and processed. In e*Index Security, entity types include users, user groups, modules, and so on.

Field

Any area on a e*Index Security window that contains information. Most field types contain text or numerical information. Some fields require you to select a predefined value.

Functions

A set of related actions within an e*Index application to which users can be granted access. For example, the potential duplicate function in e*Index includes the actions of viewing, merging, resolving, or printing potential duplicates. Functions are also known as *modules*.

GUI

Graphical User Interface. This refers to the windows, buttons, and tools that you use to perform functions within e*Index Security.

Login ID

The identification code that allows you to log on to an e*Index application. This code is assigned to you by your system administrator.

Main menu

The uppermost menu on the e*Index Security windows. You can access all of the primary functions of e*Index Security from this menu.

Module

A set of e*Index windows and tools that perform a related function. For example, to work with potential duplicates you use e*Index's Potential Duplicate module, or to perform merges you use e*Index's Merge module. Modules are also referred to as *functions*. Access permissions can be granted by module.

Online documentation

Documentation that is provided in PDF format. These documents can be viewed and printed using Acrobat Reader 3.0 or above.

Online help

A set of information and procedures that can be viewed on your computer monitor to help you perform the functions of e*Index Security.

Password

The unique password that, when used with your login ID, allows you to log on to e*Index Security. Your system administrator assigns your password, and may specify that you change your password at certain intervals.

Primary toolbar

The uppermost toolbar on the e*Index Security windows. This toolbar allows you to access all of the primary functions of e*Index Security by clicking on specific tools.

Security administration

A variety of security tasks that includes adding user profiles and groups, assigning user profiles to groups, expiring and reinstating user profiles, assigning access permissions to user profiles and user groups, and maintaining module and sub-module information.

System Administrator

The person (or persons) who maintains the security and database integrity for e*Index.

User groups

Entities you can add to e*Index Security that allow you to grant access permissions to a set of users with similar processing needs without having to define individual permissions for each user.

User profile

A set of information that describes characteristics of an individual user. A profile includes a user's name, login information, user type, and so on.

Index