



Treehouse Software, Inc.



***Security Interface between ADABAS/NATURAL
and RACF/ACF2/TOP SECRET***
Product Overview

TREEHOUSE SOFTWARE, INC.
2605 Nicholson Road, Suite 230
Sewickley, PA 15143
Phone: 724.759.7070
Fax: 724.759.7067
E-mail: tsi@treehouse.com
<http://www.treehouse.com>

This page intentionally left blank.

Introduction

This product overview highlights the key features of **SECURITRE**. The following sections are presented:

- Security Administration in ADABAS/NATURAL Environments
- What is SECURITRE?
- ADABAS/NATURAL Control and Security with SECURITRE
- Implementing a Single Rule Base with SECURITRE
- Features of SECURITRE for ADABAS
- Features of SECURITRE for NATURAL
- Features of SECURITRE for ADABAS Utilities
- Features of SECURITRE for NATURAL Utilities
- SECURITRE Real-time Monitor
- The SECURITRE Trace Facility
- Documentation and Installation
- Customer Support
- Benefits of SECURITRE

Security Administration in ADABAS/NATURAL Environments

Most installations rely on a major operating System Security Facility (SSF), such as RACF, CA-ACF2, or CA-TOP SECRET for **centralized security administration** and access control over their non-ADABAS data and non-NATURAL applications. Centralized control of the security function is **essential to promoting the integrity** and safety of the data and applications.

ADABAS and NATURAL do not interface directly with these security systems. Instead, ADABAS and NATURAL use other security mechanisms.

ADABAS has password-based File Level Security, Field Level Security, and Security by Value to control access to data. This provides limited security. Access is restricted to those who know (or discover) the correct passwords. In spite of a site's policies, users may share passwords with others, undermining access control efforts. A user supplying the correct password to ADABAS can access secured data, even if the user is not (by the site's policies) authorized to access that data. **Accountability in this environment is therefore very poor.**

Within NATURAL, the NATURAL SECURITY System (NSS), an optional package from Software AG, may control access to NATURAL, and to individual applications, programs, and commands accessed through NATURAL. At program compile time, NSS verifies that the user compiling the program may access the databases and files indicated in the program. No checks are made at run time. Therefore, **NSS controls access to NATURAL and its applications, but does not control access to data.** Furthermore, Direct Calls, ADASQL, and other types of data access are not inhibited by NSS.

ADABAS and NATURAL Utilities are another important concern. ADABAS Utilities, for example, have functions which may alter or completely delete ADABAS data. The site may restrict access to the ADARUN module which controls utility access, but users with access to that module may use any utility against any database or file on the system. NATURAL Utilities can be used to delete or overlay important programs. Either by accident or by intentional sabotage, **data and programs can be damaged by the Utilities.** This is clearly not an acceptable situation.

Sites need to integrate the security of the ADABAS/NATURAL environment with that of the System Security Facility to achieve a single rule base. This simplifies security administration and reporting.

What is SECURITRE?

SECURITRE is an interface which allows all ADABAS/NATURAL related security data to reside in the SSF, enabling the site to have a single rule base for all resources.

SECURITRE allows the SSF to control ADABAS, NATURAL, and ADABAS/NATURAL Utilities, providing a complete security solution.

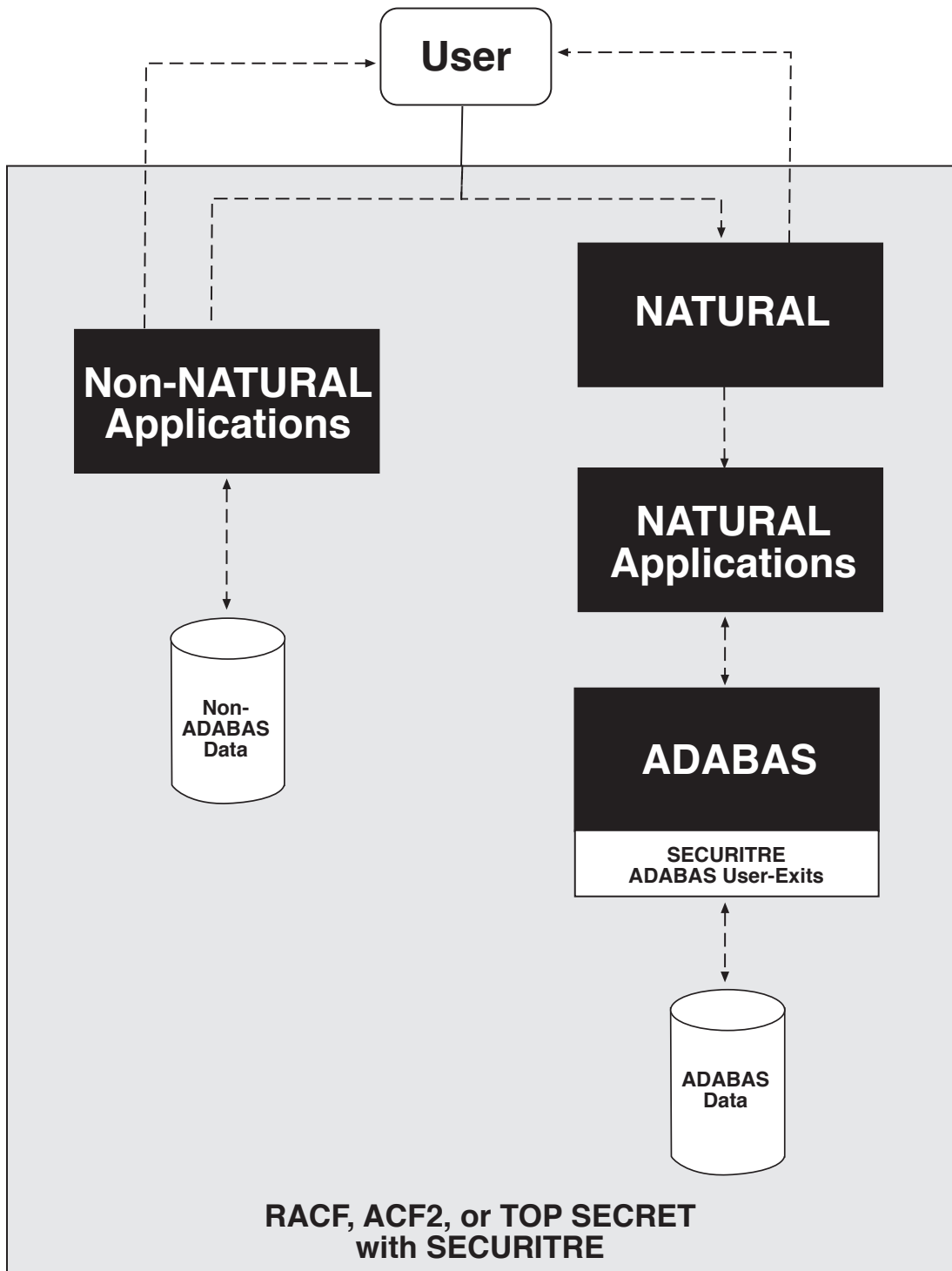
SECURITRE includes three major components:

- SECURITRE for ADABAS
 - Database Level
 - File Level
 - Field Level
 - Program Pathing Sensitivity
- SECURITRE for NATURAL
 - Session Initialization
 - Library (Logon) Level
 - Program Level
 - Program Run Level
 - DDM Security
- SECURITRE for ADABAS/NATURAL Utilities
 - Utility Level
 - Utility Function Level
 - Database Level for ADABAS Utilities
 - File Level for ADABAS Utilities
 - Library/Program Level for NATURAL Utilities through the Program Level security of SECURITRE for NATURAL

SECURITRE also includes a Real-time Monitor, and internal application security features.

With SECURITRE in place, the process of controlling access to ADABAS and NATURAL is **simplified and centralized**. The SSF controls access to ADABAS data and NATURAL environments at **all levels**, eliminating the need for separate ADABAS and NATURAL security control mechanisms and application security files. The following diagram depicts the security arrangement.

ADABAS/NATURAL Control and Security with SECURITRE



Implementing A Single Rule Base with SECURITRE

The major SSFs see the mainframe as a set of resources (datasets) to which users do or do not have access. For example, the SSF might refer to a Payroll dataset used by a COBOL program as:

```
PAYROLL.MASTER.FILE.1
```

When a user attempts to access this dataset, the SSF verifies that the user is authorized to do so. If the user is not authorized, access is denied. However, the SSF cannot determine when users access specific ADABAS or NATURAL resources. As a result, the SSF cannot control access to those resources. The SSF needs "eyes" into ADABAS/NATURAL.

SECURITRE Provides the SSF with "Eyes" into the ADABAS/NATURAL World

SECURITRE "sees" attempts to access ADABAS/NATURAL resources. Each time SECURITRE detects an access attempt, it identifies the user and constructs a site-defined pseudo dataset name for the resource. For example, if the site refers to file 125 on Production database 210 as the "Benefits Master File", SECURITRE may construct this dataset name:

```
ADABAS.PROD.BENEFITS
```

SECURITRE interfaces with the SSF to determine if the user is authorized to access the dataset. The SSF checks its rule base to determine if the request is authorized and returns the result of this check to SECURITRE. If the request is authorized, SECURITRE allows ADABAS to process the request to access file 125 on database 210.

Minimizing Overhead

SECURITRE minimizes the overhead involved with security checking by "remembering" the results of previous access attempts in an internal table. When the same user later accesses the same resource, SECURITRE recalls the result of the earlier attempt and acts accordingly. The table may be automatically or manually refreshed to reflect any updates made to SSF rules.

Single Rule Base Realized

With SECURITRE installed and implemented, the site realizes the potential of a Single Rule Base for security information. ADABAS, NATURAL, COBOL, and all other security rules are now stored in one location, the SSF.

Features of SECURITRE for ADABAS

SECURITRE for ADABAS provides the following ADABAS access controls:

- Database
- File
- Field*
- Program Pathing Sensitivity

SECURITRE for ADABAS offers complete flexibility in the use of these levels of controls. Some files can be placed under no security. Other files can be secured at the file level, and others at the field level. In addition, Program Pathing can also be in effect for any file.

Program Pathing

Some files require very strict security. The Security Administrator needs to ensure that authorized users do not make modifications to data using unauthorized programs, jobs, or ADABAS commands. Program Pathing allows a site to limit access to ADABAS files by:

- Filename
- MVS Jobname
- Node or SMFID of Calling Program
- FUSER/DBID of Calling Program
- Program Name
- NATURAL Library
- CICS Tranid and/or Termid
- ADABAS Command Code

The Security Administrator selects the Program Pathing options desired and codes the appropriate rules in the SSF.

* See the *ADABAS/NATURAL Security and SECURITRE On-line Evaluator Kit* on our Web site, at <http://www.treehouse.com> for a discussion of how Security By Field Value (SBV) is handled with SECURITRE.

Features of SECURITRE for NATURAL

SECURITRE for NATURAL offers the ability to control access to NATURAL at the following levels:

- **NATURAL Session Initialization**

SECURITRE controls which users may initiate a NATURAL session, and the DBID, FDIC, FNAT, and FUSER combinations (specified as the start-up parameters) the users may access.

- **Library Level Security**

SECURITRE controls the libraries or applications to which users may LOGON. Some libraries, such as SYSLIB, may be defined to SECURITRE as "public", so authorization to access them is not checked. Some may be defined as "restricted", such as PAYROLL, and may only be accessed by authorized users. Others may be specified as "private", and can only be accessed by individuals with a User-Id matching the library name.

- **Program Level Security**

SECURITRE controls the programs within libraries to restrict who can EXECUTE, EDIT, SAVE, and STOW programs. Some users may be granted access to all programs in a given library, others to only a few. End users needing access to a program in order to EXECUTE it can be restricted from being able to EDIT, SAVE, or STOW that program. SECURITRE can also control who may RUN a given program. Programmers can be given complete access to the program in order to modify and test it.

- **DDM Level Security**

SECURITRE controls which users may access DDMs. Users without authorization to access certain DDMs are not able to compile programs which refer to those DDMs. In addition, controls are provided to restrict the ability to change DDMs.

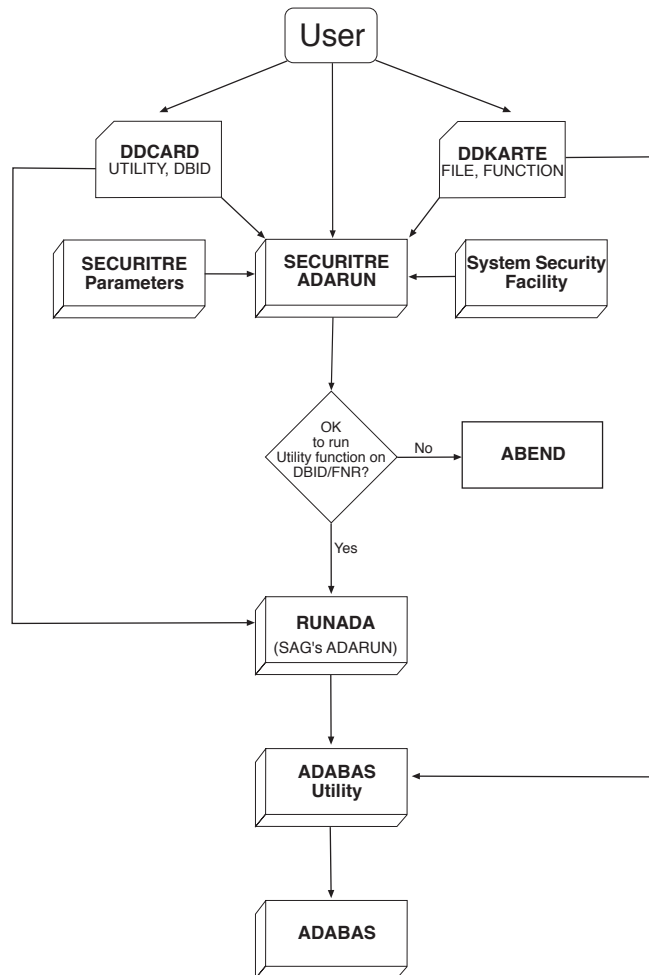
SECURITRE for NATURAL offers complete flexibility in the use of these levels of controls. For example, some libraries and DDMs can be placed under strict security, while others can be left unsecured. Several libraries can be given the same dataset name (e.g., all Test libraries) and secured in the SSF with only one rule. Dataset naming with SECURITRE for NATURAL is just as flexible as with SECURITRE for ADABAS.

Features of SECURITRE for ADABAS Utilities

ADABAS Utilities can erase entire files or significantly change data. Therefore, Utility Security is essential. To provide effective Utility Security, a site must control access to utilities and utility functions. Security Administrators may wish to place restrictions on:

- The utilities a user may execute
- The utility functions each user may perform
- The databases on which the user may perform the functions
- The files on which the user may perform the functions

With SECURITRE Utility Security, users submit utility jobs as they always have. Through its front-end to ADARUN, SECURITRE identifies the user, the utility, utility function, and database/file involved. SECURITRE then constructs a dataset name according to site standards, and contacts the SSF for authorization information. If the requested utility function is not authorized for this database and file, for this user, SECURITRE will abend the job. If access is approved, control is passed to ADARUN for processing.



Features of SECURITRE for NATURAL Utilities

NATURAL Utilities, such as SYSMAIN, can accidentally or intentionally overlay or delete programs. Therefore, only authorized users should have access to NATURAL Utilities. For this reason, SECURITRE includes NATURAL Utility Security. Through Program Level Security, SECURITRE for NATURAL helps guard against users adversely affecting NATURAL programs through the use of NATURAL Utilities.

SECURITRE Real-time Monitor

The **SECURITRE Real-time Monitor (RTM)** provides the Security Administrator with a valuable tool to assist in the **on-line monitoring of ADABAS security**. With the SECURITRE RTM, the Security Administrator may perform the following functions:

- **Force a user** from the SECURITRE tables, thereby causing a refresh of that user information in the tables.
- **Force all users** from the SECURITRE tables, thereby causing a refresh of all users' information in the tables.
- **Display** the current SECURITRE parameter settings and modify certain settings on-line.
- **Reload** the SECURITRE **user-exits**, or any other ADABAS User-Exit-1 into the ADABAS region.
- **Reload** the SECURITRE environmental **parameters** into the ADABAS region. This allows modifications to the parameters which have been made (off-line) to be implemented without bringing the database down and up.
- **Alter** the status of the SECURITRE **Trace Facility**.
- **Invoke the Real-time Monitor of Treehouse Software's TRIM** product (ADABAS/NATURAL performance monitor), if TRIM is installed at the site. This enables the Security Administrator to evaluate the performance effect of SECURITRE parameter settings to ensure optimal performance.
- **Display** the current **parameters** of SECURITRE for NATURAL.
- **Display** the current SECURITRE **table sizes**.

The SECURITRE Trace Facility

The SECURITRE Trace Facility can help customers diagnose any problems they are experiencing, and help Treehouse Software technical personnel assist the customer in solving any problems which might arise. The Trace Facility shows detailed information, including the dataset names being communicated to the SSF and the result of that communication.

Documentation and Installation

SECURITRE documentation is contained in a detailed **Reference Manual** and **Administrator Guide**. Both manuals are fully indexed, and both are available in hard copy or on a CD, free of charge.

SECURITRE is available for MVS/ESA, MVS/XA, MVS (OS/390), and OS/VS1 operating systems under any TP system which supports ADABAS and NATURAL.

SECURITRE will issue all GETMAIN requests above the 16M line, if ADABAS is running above the line (i.e., ADARUN is relinked AMODE=31).

Installation can be accomplished in a short time. Treehouse Software technical personnel are available to visit sites to help install, demonstrate, and present SECURITRE. Contact TSI for details.

SECURITRE is reliable and efficient. It has been tested with all the major SSFs, the latest versions of Adabas and Natural, and under a variety of conditions in large and small shops.

Customer Support

Treehouse Software, Inc. supports SECURITRE and its other products from its headquarters in Pennsylvania. Support representatives in several foreign countries are available to answer customer questions. SECURITRE users always have **direct input to the product developers**. User questions are answered quickly, problems are discussed directly, and change/enhancement requests are reviewed and implemented in a timely manner. SECURITRE is so easy to use that formal instruction is typically not necessary.

Benefits of SECURITRE

SECURITRE offers many benefits to an organization:

- More control over ADABAS and NATURAL resources
- Better accountability when changes are made to ADABAS data
- Better protection against accidental damage or intentional sabotage to ADABAS data and NATURAL programs
- Easier security administration and reporting
- No need for separate security packages and options to control ADABAS and NATURAL
- Greater flexibility to meet changing security needs
- Uniformity of access controls throughout the computer system
- Reduced training costs related to security administration

These benefits are accomplished through a comprehensive set of features not available in any other ADABAS/NATURAL security solution. **SECURITRE is the "ideal approach" to meeting ADABAS and NATURAL security requirements.**

ADABAS, NATURAL, NATURAL SECURITY, and ADASQL are all products of Software AG. RACF is a product of IBM. CA-ACF2 and CA-TOP SECRET are products of Computer Associates. The information used in the examples in this overview is for illustrative purposes only.

This page intentionally left blank.



2605 Nicholson Road, Suite 230
Sewickley, PA 15143
Phone: 724.759.7070
Fax: 724.759.7067
E-mail: tsi@treehouse.com
<http://www.treehouse.com>