

# ***E-SRF***

**EKC Security  
Reporting Facility**

**Release 2.3.1**

**Release Guide  
*and* Change Summary**



E-SRF™ is a proprietary product

developed and maintained by

EKC Inc.  
10400 West Higgins Road  
Rosemont, Illinois 60018  
USA

**(847) 296-8010**

Technical Support:

**(847) 296-8035**

EKC, Inc. provides only software program products, which fully comply with, and maintain MVS integrity.

The vendor hereby warrants that:

- 1) E-SRF™ ("Software") performs only those functions which are described in the published specifications;
- 2) There are no methods for gaining access to the Software or other computer resources or data of Licensee (such as a master access key, ID, password, or trap door) other than set forth in the published specifications;
- 3) The Software does not introduce any MVS integrity exposures. The program code, with the exception of one utility, runs totally in non-authorized, problem state. The one utility, EKCRXCAT, requires APF-authorization to read the MVS System Catalogs. This utility is optional, and not required to run the E-SRF product.
- 4) The software shall be year 2000 compliant, and shall function correctly regardless of date according to published specifications as long as regular software maintenance is applied.

Copyright © EKC Inc. USA 2011  
All Rights Reserved

Reproduction of this manual without written permission of EKC Inc. is strictly prohibited.

**Version 2, Release 3.1 January, 2011**

All product names referenced herein are trademarks of their respective companies.

Printed in USA

---

# Contents

<b>Chapter 1:</b>	<b>E-SRF z/OS Security Reporting Release 2.3.1 Changes.....</b>	<b>1-1</b>
	SCOPE .....	1-1
<b>Chapter 2:</b>	<b>Access Analysis Reporting Function.....</b>	<b>2-1</b>
	PERFORMANCE IMPROVEMENTS .....	2-1
	FUNCTIONAL IMPROVEMENTS .....	2-1
	<i>CA-ACF2 Release 14 \$ROLESET support</i> .....	2-1
	<i>CA-ACF2 for DB2 support</i> .....	2-1
	ENHANCEMENTS IN V2.3.1 .....	2-1
	<i>ACF2 Keyword additions:</i> .....	2-1
	<i>Report format modifications:</i> .....	2-2
	RBAC CONVERSION ASSISTANCE AND E-SCC .....	2-2
	PREPARING FOR THE FUTURE .....	2-2
<b>Chapter 3:</b>	<b>Event Reporting System.....</b>	<b>3-1</b>
	SUPPORT AND MAINTENANCE:.....	3-1
	BETA AND EARLY SHIP CUSTOMERS:.....	3-1
	MASTERFILE UPGRADE: .....	3-1
	PRODUCT DOCUMENTATION: .....	3-2
	PERFORMANCE IMPROVEMENTS: .....	3-2
	USABILITY: .....	3-2
	SECURITY AND CONTROL: .....	3-3
	AUTO-UPGRADE NON-ACTIVE GROUPING STRUCTURES:.....	3-3
	INTERNAL FACILITIES .....	3-3
	<i>Messages</i> .....	3-3
	<i>SHOW Command:</i> .....	3-4

---

# E-SRF Publications

Name	Contents
Installation Guide	Information about the installation and maintenance of the entire E-SRF product suite.
Release Guide and Change Summary	Contains all new features and system function changes.
General Information	An overview of E-SRF and its components.
Getting Started Guide & Utilities	Brief overview of E-SRF in general, including: a Roadmap for E-SRF, use of the sample library, and descriptions of various utilities that augment the E-SRF product
Resource Grouping Facility Guide	Provides information on how to use the EKC Grouping Facility.
<i>Access Analysis:</i> Reports Guide for ACF2	Overview of Access Analysis reports, explanation of the DataOwner and Userid/LogonidOwner reports, command syntax, utilities necessary for creating input to reports, and JCL.
<i>Access Analysis:</i> Reports Guide for RACF	Overview of Access Analysis reports, explanation of the DataOwner and Userid Owner reports, command syntax, utilities necessary for creating input to reports, and JCL.
<i>Event Reporting Facility:</i> User Guide	A "How To" guide for users of the E-SRF Event Reporting Facility.
<i>Event Reporting Facility:</i> Command Reference	Explains the Event Reporting Facility command processor, command syntax, and JCL.
<i>Event Reporting Facility:</i> Masterfile and Data Dictionary Reference	Explains the structure of the E-SRF Masterfile and describes all Masterfile fields.
<i>Event Reporting Facility:</i> Quick Reference	Brief description of datanames and commands
<i>Event Reporting Facility:</i> Messages and Codes	Provides information about the messages that may be presented by the Event Reporting Facility.
<i>Event Reporting Facility:</i> Report Overlays and Utilities Guide	An overview of the Reports and Utilities provided by the Event Reporting Facility.

# Chapter 1: E-SRF z/OS Security Reporting Release 2.3.1 Changes

This guide identifies the major enhancements incorporated into E-SRF Version 2, Release 3, Modification 1. The intent is to describe the changes that were incorporated into the product and the possible impact on your E-SRF system currently in place. The enhancements are discussed assuming you have a basic understanding of E-SRF.

If you are new E-SRF customer, this information serves as a point of interest. New customers should utilize the *User Guides* for information on the use of this product. These publications provide the best overall explanation of E-SRF functionality. The *User Guides* are organized to “bring together” E-SRF functionality and concepts and direct you to other manuals when more detailed information is required.

Version 2.3 was a major release of this product, containing enhancements that were requested by customers using the product, as well as planned enhancements needed to report on new features available in newer releases of EKC’s ETF/R and ETF/A products. This modification (V2.3.1) adds additional support for CA-ACF2 features, and support for EKC’s new Security Classification and Categorization product; E-SCC.

Major performance and usability enhancements were provided throughout the components of this product.

Please review this information to determine what, if any, impact this release may have on your operating environment. Review the product’s documentation. If you have questions or concerns about anything mentioned in this document, additional questions or comments, please contact EKC Technical Support.

The E-SRF z/OS Security Reporting Facility, with the exception of the enhancements stated in this document is functionally identical to previous releases from a user perspective. Many changes were made to accommodate new enhancements that add new functionality, but do not unduly change existing functionality. Some enhancements have no external appearance and therefore are not mentioned in this publication.

Some of the commands required to execute this product were greatly enhanced to the point where intending and renaming was required. In all of these cases, the old conventions will still work and will provide the same level of control as they did in previous releases. To take advantage of newer and extended capabilities, it is recommended that they are replaced with the newer specifications.

## Scope

Information provided in this document represents all changes that occurred from the most recent release 2.3 offering to the current product offering being release 2.3.1. If you are on a release prior to 2.3 and are interested in what changed prior to 2.3, please consult the change summaries published for all maintenance levels between the maintenance level you are currently using and this level.

---



## Chapter 2: Access Analysis Reporting Function

### **Performance Improvements**

Access Analysis reporting, by its nature, is CPU intensive. Many of the modules in this component have been extensively re-written in an effort to improve execution time, and tests in our lab have shown improvements ranging from 5 to 25% reduction. We would appreciate hearing about your run-time experiences.

### **Functional Improvements**

#### **CA-ACF2 Release 14 \$ROLESET support**

E-SRF V2.3.1 supports analysis of access via CA-ACF2 Release 14 ROLE and USER parameters in rules. (See the CA-ACF2 for z/OS Release Notes –R14 for more information on this facility).

#### **CA-ACF2 for DB2 support**

E-SRF V2.3.1 supports analysis of access to DB2 resources based on CA-ACF2 security option for DB2 controls. (See the CA-ACF2 for z/OS Release Notes –R14 for more information on this facility).

#### **RACF Conditional Access support**

E-SRF V2.3.1 support adds JESINPUT, SYSID and SERVAUTH conditional access types.

### **Enhancements in V2.3.1**

The process of extensively re-engineering E-SRF Access Analysis for RACF and for ACF2, to improve performance over previous versions, has continued for V2.3.1. Run times for the various reports have improved, and general storage and processing improvements make it possible to run much larger selections of data.

Several new Keywords have been added, and several existing keywords have been augmented to provide additional reporting and selection options.

#### **ACF2 Keyword additions:**

- ❑ ALTUID(MAX) keyword permits reporting of access possibilities beyond a single access path in a multiple UID or mixed roleset and UID access environment. This will demonstrate that even if the primary rule path is removed, access is still available.
  - ❑ The LISTSELECT keyword has been augmented with the ROLE operand to allow listing of all available UID and ROLE access paths for each of the selected users.
  - ❑ EXPFIELDS keyword augmented to allow export of DB2 Service data.
-

- BYACCESS with EXPORT(ENV) has been added to communicate the groupings inherent in your security environment to the E-SCC product for further analysis and RBAC generation.

In a multiple UID, or mixed ROLE / UID environment, a specific prevent is only a “not yet”. In this release of E-SRF, the “prevent overcome” summary flag indicates accesses in which a specific prevent rule, such as USER(LID001) PREVENT, has been overcome by an alternate uid string (either a CA/ACF2 multi-value field or an ETF/A alternate).

### **Report format modifications:**

The detail level report formats have been modified to incorporate the new information required to describe the access environment. New information for ROLE and USER specifications is available in all reports for CA-ACF2 \$ROLESET access descriptions.

Additional information is also available in the detail level Resources reports for DB2 column restrictions and service definitions for users of the CA-ACF2 security option for DB2.

### **RBAC conversion assistance and E-SCC**

The BYACCESS report format for both RACF and ACF2 Access Analysis, introduced in V2.3.0, has been further developed to work with the EKC Security Classification and Categorization product (E-SCC). With E-SCC, you can view your Access Analysis results in a PC application.

For CA-ACF2 users, E-SCC can produce CA-ACF2 command streams to:

- Build XROL groups and entries for your users based on their access analysis groupings.
- Build \$ROLESET rules to replicate your rule environment in an RBAC mode.

Access Analysis can in turn, produce reports on the E-SCC generated environment before anything is committed using the proposed rule processor.

While this is not a full conversion product set (there will still be a few details to work through), it does give you a starting place, and a view of where you are going with role based access controls.

### **Preparing for the Future**

In addition to the functional changes listed above, the Access Analysis components have been redesigned to provide a flexible platform for the next release. We intend to provide additional features, and product integration with the Event Component, so that on one report a data owner can see both who does have access to area resources, as well as the loggings and violations for those resources.

---



## Chapter 3: Event Reporting System

### **Support and Maintenance:**

EKC welcomes you to Version 2, Release 3, Modification 1 (Release 2.3.1) of E-SRF Event Reporting, representing the latest offering of this product to date.

All enhancement and maintenance items added to previous releases have been carried forward in Release 2.3.1. Release 2.3.1 contains all previous release maintenance up to PTF: LE22023 which was the last PTF that was implemented in Event Reporting for Release 2.3 before Release 2.3.1 became generally available. Any subsequent maintenance provided during the “end of life” support period for previous releases as well as new maintenance items will be carried forward in Release 2.3.1 (*if applicable*) as maintenance service.

Future maintenance for this product should be applied when made available.

This offering should be considered a replacement for the software and product documentation that may exist for any previous product release you may have.

This version will run on a mainframe computer under the zOS operating system. Event Reporting may also be executed on OS/390 release 2.10.

Please insure you apply your Site License enabling PTFs when installing this release. These PTFs were provided with your installation materials.

### **Beta and Early Ship Customers:**

Beta and Early Ship (ESP) releases do not raise the Masterfile release level if errors were found that caused the Masterfile data to be incorrect or the Masterfile’s format was changed. The Masterfile release remains the same and no automatic conversion is provided across these early release offerings. This means your Masterfile may not be in-sync with the Generally Available software you are replacing your early release offering with.

If you were an early ship customer running a BETA or ESP version of release Release 2.3.1, it may be possible that you may have to cold-start your Masterfile. Please contact EKC Product Development for information regarding the status of your Early Ship Masterfile level and the level that is expected for the Generally Available software release.

In most cases, a COLD start will NOT be required.

### **Masterfile Upgrade:**

Release 2.3.1 requires your E-SRF Event Reporting Masterfile to be at Release 02.03.01 which is the same level as Release 2.3. If you are converting from Release 2.3, there will be no conversion. If you are converting from a release prior to Release 2.3, a conversion will be required and will be performed the first time you execute your new software against your existing Masterfile. Please insure your job is properly conditioned to allow the conversion.

Please note that Masterfile releases are based on data format and not necessarily the software release of the product maintaining it. The same product release may cause subsequent Masterfile level upgrades during the life of the release. If maintenance to this product

---

requires a Masterfile level conversion, you will be informed. As discussed in the product documentation, conversions are automatic, but you have to allow them to proceed.

As indicated in the product documentation, this product maintains full compatibility to older Masterfile releases created by any previous software release.

Please note: Although you are able to convert any *previous* Masterfile to the release required by the *current* software release, *you cannot convert a newer Masterfile back to a previous software release.*

As with any data processing application, make sure you back up your Masterfile prior to allowing this release to convert your Masterfile. As with all previous Masterfile conversions, once your Masterfile has been converted, it cannot be processed with prior releases of this product. If you want to run the older release the same time, you will need to maintain the older Masterfile as well as the converted Masterfile.

### **Product Documentation:**

The documentation provided in Release 2.3.1 continues the effort started in release 2.2 and again represents a major overhaul. The individual publications continue to contain information relating to their purpose, but have been reviewed and edited in an effort to make them easier to understand.

Documentation was added for additional Event Reporting utility programs in the E-SRF Report Overlays and Utilities Guide.

The Masterfile and Data Dictionary was reworked in an effort to make the product easier to understand for new users.

The Event Reporting class for this release is being developed using the User Guide as a “textbook” and should be available soon.

This effort has been ongoing for the past several releases and will continue into future releases. An effort is also underway to reduce the size of the publications while providing the information that may be required to successfully deploy and maintain this product.

### **Performance Improvements:**

An initial design objective that continues to remain with this product is that each new release must contain more functionality and will outperform its predecessor.

Release 2.3.1 continues to maintain this tradition. Various components within this product have had performance improvements that may be measurable in certain environments depending on the size of your Masterfile and the type of data stored on it.

Numerous other performance enhancements were provided throughout all components of the product.

### **Usability:**

The command processor was further enhanced to process keywords (both major and minor) using the fully spelled out representations as well as any abbreviation that does not make the keyword ambiguous with other related keywords. This effort was started in Release 2.3 and was completed in this release.

---

The Command Guide and the Quick Reference publications have been enhanced to show the fully spelled out keyword representations. Please refer to the Command Guide for the rules to properly specify keyword representations in an abbreviated form.

## **Security and Control:**

An optional Security Authorization facility (SAF) interface has been incorporated in Release 2.3.1 which optionally allows you to maintain control over every command that may be executed by the command processor.

You can optionally define entity names in your security system to secure the use of any command using the fully spelled out keyword representations. The interface is fairly easy to implement and is fully documented in the Uerr Guide.

## **Auto-Upgrade non-active Grouping Structures:**

Grouping is a very powerful capability in Event Reporting and has been improved in every release of this product.

This release now provides the ability to optionally upgrade defined Grouping Structures that are not currently “active” when the grouping environment changes (possibly due to a Masterfile Update Function) during the execution’s termination.

In previous releases, only the current active Grouping Structure was automatically upgraded (if required) prior to the execution’s termination. This left other structures that may be defined on your Masterfile to remain in a state where an upgrade would be forced on first reference. This design was dictated by an effort to improve execution performance as many Grouping Structures are not frequently used, or may not be used at all. Although this is how the product was designed, this operational mode caused security violation problems when a user attempted to run reports using a structure left in this state when their access to the Masterfile was Read-Only. The structure would have to be upgraded which updates the Masterfile.

To address this problem an attribute was added to the structure definition that would “force upgrade” particular Grouping Structures during the execution’s termination making these structures behave as if they were the current active structure.

To find out how grouping works in this release, please refer to the: *E-SRF Event Reporting User Guide*, *E-SRF Event Reporting Command Reference* and the: *E-SRF Event Reporting Masterfile and Dictionary Reference*.

## **Internal Facilities**

Many enhancements were provided to accommodate “*under-the-hood*” requirements that users would normally not need to know about, but provide the framework for this product to perform its functions. Most of these enhancements are not mentioned unless they are a point of interest or could have an effect on how this product runs on your hardware.

## **Messages**

Additional messages have been added to this product for functions requiring them. These messages are documented in the: *E-SRF Event Reporting Messages and Codes Reference* manual.

---

## **SHOW Command:**

The SHOW command (and the ESRFSHOW report overlay) have been enhanced to accommodate new features.