

E-SRF

**EKC Security
Reporting Facility**

Release 2.3

**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. A non-APF authorized utility, EKCRGCAT, is supplied to perform the same function, but at a considerably slower speed.
- 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 2010
All Rights Reserved

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

Version 2, Release 3 January, 2010

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

Printed in USA

Contents

Chapter 1:	E-SRF z/OS Security Reporting Release 2.3 Changes.....	1-1
	SCOPE	1-1
Chapter 2:	Access Analysis Reporting Function.....	2-1
	PERFORMANCE IMPROVEMENTS	2-1
	FUNCTIONAL IMPROVEMENTS	2-1
	ACF2 RELEASE 14 \$ROLESET SUPPORT.....	2-1
	ENHANCEMENTS IN V2.3.0.....	2-1
	<i>ACF2 Keyword additions:</i>	2-1
	PREPARING FOR THE FUTURE	2-2
Chapter 3:	Event Reporting System.....	3-1
	SUPPORT AND MAINTENANCE:.....	3-1
	MASTERFILE UPGRADE:	3-1
	PRODUCT DOCUMENTATION:.....	3-2
	PERFORMANCE IMPROVEMENTS:	3-2
	MASTERFILE TOKEN DICTIONARIES:	3-2
	REPORTING ENHANCEMENTS:	3-3
	GROUPING ENHANCEMENTS:.....	3-3
	ADDITIONAL OWNER HEADER DATA ITEM:	3-4
	INTERNAL FACILITIES	3-4
	<i>ControlSets:</i>	3-4
	<i>Messages</i>	3-4
	<i>SHOW Command:</i>	3-4
	<i>License control:</i>	3-4
	COMMAND CHANGES	3-5
	<i>Keywords:</i>	3-5
	<i>Command Changes:</i>	3-5

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/LogonidOwner 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 Changes

This guide identifies the major enhancements incorporated into E-SRF Version 2, Release 3. 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 is a major release of this product, and contains 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 release is critical to future offerings of these products.

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 2.2 offering to the current product offering being release 2.3. If you are on a release prior to 2.2 and are interested in what changed prior to 2.2, 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

ACF2 Release 14 \$ROLESET support

Our intention is for E-SRF to support ACF2 Release 14 ROLE and USER parameters in rules in this release via a PTF in early 2010. (See the CA-ACF2 for z/OS Release Notes –R14 for more information on this facility).

Enhancements in V2.3.0

The process of extensively re-engineering E-SRF Access Analysis for RACF and for ACF2, to improve performance over previous versions, has continued for V230. Run times for the various reports have improved ten fold, 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. Our clients have asked for the following enhancements, and we've listened.

ACF2 Keyword additions:

- ❑ ALLUID keyword permits report and export consolidation to one line for all access granted for common UID masks.
- ❑ BYPASSUID keyword permits unwanted access reporting to be eliminated for common UID masks.
- ❑ ONLYUID keyword permits access reporting to be limited to a set of common UID masks.
- ❑ INCPREVENT Keyword allows specified prevents to be included in the reports.
- ❑ BYACCESS Keyword provides a partial summary that groups users with common access. This mode is especially helpful in “discovering roles” that are inherent in your security definitions.
- ❑ EXPFIELDS keyword augmented to allow export of UID mask data.

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

Prior versions of Access Analysis for ACF2 stopped checking a lid on the first encountered “full” access. Version 2.3.0 lists multiple access possibilities due to Alternate UIDS.

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 (Release 2.3) 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. Release 2.3 contains all previous release maintenance up to PTF: LE22124 which was the last PTF that was implemented in Event Reporting for Release 2.2 before Release 2.3 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 (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.

Masterfile Upgrade:

Release 2.3 requires your E-SRF Event Reporting Masterfile to be at Release 02.03.01. The conversion subsystem has been enhanced to convert your current Masterfile (if you have one) from whatever release it was being maintained with to Masterfile Release 02.03.01.

If you were an early ship customer, 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 release.

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 accompanied by their associated conversions. 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 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 User Guide has reworked to in an effort to make the product easier to understand for new users. The manual consists of two logical parts. The beginning chapters discusses the topics as before except most reference to grouping and other advanced functions were removed. The latter chapters discuss how to implement and control Event Reporting grouping capability and other advanced functions.

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 continues to maintain this tradition. The main development areas in this release involved the management of Masterfile’s token dictionaries and Grouping Structures.

Release 2.2 provided the foundation for improved performance when using the grouping capabilities. Release 2.3 continues where release 2.2 left off.

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

Masterfile Token Dictionaries:

The Release 2 product offering uses tokens to represent Masterfile entities. For tokens to be useful, there must be a means of relating a token to a character string (such as a resource entity name). This task is provided with the help of token dictionaries.

In Release 2.1 and 2.2 the token dictionaries were maintained on the Masterfile by providing a single Masterfile object for each token. This approach worked well, but consumed excessive processor and syorage resources and caused delays during startup.

Release 2.3 converted the token dictionaries from individual masterfile objects to an internal structure that is far more efficient and provide a performance improvement during the establishment of these dictionaries during the execution’s startup.

Reporting Enhancements:

Added the report overlay ESRFVLHS.

Grouping Enhancements:

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 maintain up to sixteen individual Grouping Structures. Previous releases maintained a single Grouping Structure. When Event Reporting starts up, the named default Grouping Structure is activated. You now have the ability to subsequently activate any other defined Grouping Structure as may be needed to address your reporting requirements.

When a new Masterfile is created, the shell of the first Grouping Structure is placed on the Masterfile and named DEFAULT. This structure is declared as the *default* Grouping Structure. The rule object data set associated with this structure is declared as RULES and is referenced via the RULES DD name.

If you are converting from a previous release's Masterfile, the existing Grouping Structure is converted and installed on the Masterfile as DEFAULT. Everything will function as it did in the prior release, except you now have the ability to define and activate fifteen additional structures if you need to do so (one structure at a time).

A new command: GROUPING was added that is used to activate and maintain control over your Grouping Structures and group control functions. Use of the old commands will still function, but will process against the default Grouping Structure.

If you want to continue to run with a single Grouping Structure, everything you did in your previous release will work unchanged. It is recommended that you read the information about grouping in the User's Guide if you want to exploit the new features of grouping.

The RULES dataset DD is no longer required as part of your JCL and should not be there. Each Grouping Structure is defined on the Masterfile and part of that definition is the rule object data set DD name and DS name. The file is dynamically allocated when a Grouping Structure is activated.

If a DD for the particular Grouping Structure's rules object data set is found in the JCL, the DS name will replace the definition contained on the Masterfile and the JES allocation will be used.

If the rules object data set is not defined in the Grouping Structure Masterfile definition and is not in the JCL, the structure is marked non-usable and subsequent calls against it are ignored. A group name resolution against any entity, even if it exists in the current structure will result in the group name \$ESRF(NOT_AVAIL). This is because without the rules object data set, there is no way insure the structure is accurate and impossible to update when new entities are presented for grouping.

Improvements to the Group Structure startup and subsequent access have been made.

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*.

Additional Owner Header data item:

The OA.MAIL item was added to the Owner Header. This 48 character field is intended to be used to maintain e-mail addresses of the owner that will be used to route reports through e-mail.

The ability to route reports through e-mail will be released as subsequent maintenance to this product release.

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.

ControlSets:

An internal facility to store mapped and unmapped data structures was introduced in Release 2.2. Its purpose is to provide a place to “quick-cell” data between E-SRF executions. This enhancement has no user involvement, other than its presence makes adding new functionality easier and more reliable. The only user involvement would be the possibility of messages relating to ControlSets on the SYSPRINT Control Report.

The use of controlsets were extended in release 2.3 to maintain more of the system data needed to enhance the product in this and future releases.

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.

The messages originating from group control exceeded its assigned range. The messages E300-325 were moved to the E800-849 range. Some messages were eliminated while others were added. If you have programs that look for Event Reporting messages on the Control Report, please review them and make whatever changes necessary to insure continued functionality. The Event Reporting Messages and Codes manual fully documents all messages that originate from this product.

SHOW Command:

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

License control:

If the EKC site ID module is not available, the EKC E-SRF site ID module will be used for both site ID keys.

Command Changes

Changes to the Event Reporting command syntax were made in this release.

Keywords:

Command syntax was improved by allowing you to specify the characters of a keyword that are required to uniquely identify a keyword from the list of available keywords for a specific specification.

For example, the following fully spelled out command:

GROUPING ALTERSTRUCTURE(AUDIT)

May be specified the following way:

GRP AST(AUDIT)

The Command Reference was enhanced to show the fully spelled out command names. The short names documented and used in previous releases will map into the longer names and should be continued to be used. The long names are provided so you know the full name of each keyword allowing you to abbreviate your specifications as you desire. There are two rules, first keyword must always start with its first character and the remaining characters must be specific enough to make the specification unique against the list of choices available for the particular specification. More information about this topic may be found in the: *E-SRF Event Reporting Command Reference*.

Command Changes:

As previously stated, some commands were depreciated, renamed and/or relocated in this release.

The legacy forms of these commands will continue to function unless their function was removed. However they are no longer documented and may be limited to the capability that existed at the time they were considered current.

It is recommended that the newer commands be used.

The following is a list of the depreciated commands and how they are now implemented:

JCL parm:

SIP: Keyword was added for \$SIP debugging.

Major Commands:

CACHE : Additional options were added.

GROUPING: Was added in Release 2.3 to maintain control over grouping functions. Specifications from **OPTION** and **SET** were ported to this command. Additional grouping specifications were provided in this command to control new features contained in this release. The previous grouping commands will still work in a limited fashion. If the new grouping features are not used, the system will operate the same as it did in the previous release. It is recommended that the **GROUPING** command be reviewed in the: *E-SRF*

Event Reporting Command Reference to get an understanding of the new grouping features and whether or not they may be useful in your environment.

INSERT (or **ADD**): Class name was added to identify GROUP and OWNER structure classes. If omitted when needed, DEFAULT will be assumed.

OPTION: Specifications relating to grouping were moved to the GROUPING command.

REMOVE (or **DELETE**): Class name was added to identify GROUP and OWNER structure classes. If omitted when needed, DEFAULT will be assumed.

SET: Specifications relating to grouping were moved to the GROUPING command.

SHOW: The GROUPING keyword was added to provide a display of your current grouping environment.