

E-SRF

**EKC Security
Reporting Facility**

Release 2.2

**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 2008
All Rights Reserved

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

Version 2, Release 2 April 2, 2008, (Revised September 2, 2008)

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

Printed in USA

Contents

Chapter 1:	E-SRF z/OS Security Reporting Release 2.2 Changes.....	1-1
	SCOPE	1-1
Chapter 2:	Access Analysis Reporting Function.....	2-1
	PERFORMANCE IMPROVEMENTS	2-1
	FUNCTIONAL IMPROVEMENTS.....	2-1
	<i>RACF Access Reporting Enhancements.....</i>	<i>2-1</i>
	<i>ACF2 Access Reporting Enhancements</i>	<i>2-1</i>
	PREPARING FOR THE FUTURE	2-2
Chapter 3:	Event Reporting System.....	3-1
	SUPPORT AND MAINTENANCE:.....	3-1
	MASTERFILE UPGRADE:	3-1
	PRODUCT DOCUMENTATION:	3-1
	PERFORMANCE IMPROVEMENTS:	3-2
	MASTERFILE "TOKEN" CLEANUP:	3-2
	REPORTING ENHANCEMENTS:	3-2
	GROUPING ENHANCEMENTS:.....	3-3
	DOMAIN AND SYSID:.....	3-4
	DICTIONARY NAMES:.....	3-4
	MASTERFILE UPDATE:.....	3-4
	<i>Heartbeat:.....</i>	<i>3-4</i>
	<i>EXCLUDE Update specification:</i>	<i>3-4</i>
	UTILITIES:.....	3-5
	<i>ESRFASCI Provide ASCII print file</i>	<i>3-5</i>
	<i>ESRFHTML Provide HTML print file</i>	<i>3-5</i>
	<i>ESRFSMFD.....</i>	<i>3-5</i>
	INTERNAL FACILITIES	3-6
	<i>ControlSets:.....</i>	<i>3-6</i>
	<i>Data Only Address Spaces:</i>	<i>3-6</i>
	<i>Messages</i>	<i>3-6</i>
	<i>SHOW Command:.....</i>	<i>3-6</i>
	<i>Table Management:.....</i>	<i>3-6</i>
	<i>License Management:</i>	<i>3-7</i>

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 2.2 Changes

This guide identifies the major enhancements incorporated into E-SRF Version 2, Release 2. 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 2.2 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 EKC’s ETF/R and ETF/A products. This release is critical to future offerings of these products.

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.

Scope

Information provided in this document represents all changes that occurred from the most recent release 2.1.0 offering to the current product offering being release 2.2.1. If you are on a release prior to 2.1.0 and are interested in what changed prior to 2.1.0, 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

RACF Access Reporting Enhancements

Access Analysis reports for RACF have been updated to include the following features:

- **INCFIRECALL** keyword option to report on access provided by ETF/R's F\$RECALL facility. ETF/R is EKC's Tools For RACF.
- **DATE** keyword option to examine access conditions that would be in effect on a date other than that of the report run, due to revoke / resume settings.
- Support for dynamic classes.

ACF2 Access Reporting Enhancements

Access Analysis reports for ACF2 have been updated to include reporting of access provided by alternate UID strings. There are two vendor sources of strings involved in this update:

- CA-ACF2 provides for multi-value fields to be included in the defined UID string. If access is not allowed by the first value, ACF2 will then use any additional values coded in the LogonID record for a user to re-process the validation, until the requested access is allowed, or the list of values is exhausted. Access provided by multi-value items after the first are flagged in Access Analysis reports with an "M-"
- ETF/A, EKC's Tools For ACF2, provides a multiple alternate UID facility allowing all 24 positions of the UID string to be used in assigning an alternative access path. MUID alternates and F\$RECALL alternates have participated in Access Analysis reporting in prior releases. There are two new categories of ETF/A alternate UIDs introduced with ETF/A 1.6.2: Group alternates and Role alternates. Group alternates provide a means of assigning a standardized UID string to a number of users by referring to the group. Role alternates provide for a parallel rule structure where access can be assigned to "roles", and the UID string values can clearly describe that role. Access provided by ETF/A alternate UIDs are flagged with A-, F- and R- respectively. Uses of the ETF/A secondary UID facility (which preceded MUID functionality) will also be marked with an "A-".

A number of enhancements have been made to the ACF2 Access Analysis reports to enhance selection, functionality and report readability.

- All report sections will be marked with a section number to the left of the page number to improve report clarity and documentation references.
- The **SELECT** keyword has been extended to allow multiple masked arguments for each field.
- The **INDEX** keyword can now specify up to eight masked high-level qualifiers.
- The **CLASS** keyword can now specify up to eight masked resource classes.
- The **LISTSELECT** keyword has been augmented to optionally list all participating UID strings for each user.
- The **LIDLIST** keyword has been added to allow pre-selection or exclusion of specific logonids provided in an input dataset. The remaining set of logonid records are then selected from using the standard keywords – SELECT or UGROUP. Use of this keyword will be noted in the report wrappers
- The **COMMENTS** keyword has been augmented to allow **\$USERDATA** information to be listed along with dataset / resource names.
- The **EXPFIELDS** keyword has been added to allow specified fields from the LIDREC to be appended to each export record in DIF format.
- The Access Analysis Proposed Rule Processor, which examines the access implications of a set of rule changes before they are put into production, will alternately examine ETFA Rule Test Facility rules with this release. The benefit of this method over the standard ACF2 test command is that all access implications are examined, rather than those of a specific chosen LID / UID / Resource combination.

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 2 (Release 2.2) of E-SRF Event Reporting, the latest offering of this product to date.

All enhancement and maintenance items added to previous releases have been carried forward in Release 2.2. The latest Rollup PTF (LE21071) provided for Release 2.1 has been implemented in Release 2.2. 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 2.2 (if applicable).

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

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

Masterfile Upgrade:

Release 2.2 requires your Masterfile to be at Release 02.02.01. 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 02.02.01.

Please note that Masterfile releases are based on the data format and not necessarily the software release of the product maintaining it.

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 2.2 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.

The publications have a new cleaner look. The index content has been improved to help provide quick reference to desired topics.

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 outperform its predecessor.

Release 2.2 maintains this tradition. The main areas in this release involve the management of Masterfile “tokens” (that were introduced in release 2.1), the overhead associated with inserting objects on the Masterfile and the resources consumed by the process of grouping entities on the Masterfile.

Release 2.1 provided the foundation for improved performance during the UPDATE function at the same time providing support for long resource names. Release 2.2 was built on that foundation while providing additional enhancements.

Masterfile “token” Cleanup:

Entity names carried on the Masterfile were tokenized in Release 2.1. For example, a unique token is assigned for each unique entity name. Once a token is assigned, it remained forever in the token dictionary. As entities become dormant these “orphaned” tokens remained on the Masterfile causing overhead during their maintenance. Many times the orphaned token would be used again while other times it just remained in the dictionary as an orphan. Additionally, grouping is keyed off the tokens, thus causing excessive overhead when grouping was required and orphaned tokens existed in the token dictionary.

In latter offerings of Release 2.1, an execution parameter was provided (**PARM=COMPRESS**) to “purge” orphaned tokens, compress the token dictionary and reassign all tokens across the entire Masterfile.

In Release 2.2, this parameter remains and has been documented. In addition to the parameter (*that must be manually specified*), a new facility **AUTOCOMPRESS** was added which automatically purges orphaned tokens based on a user controllable interval (*specified in days*) when the Masterfile is in UPDATE mode.

Additionally, a new warning message is posted if the number of tokens currently assigned in a token pool gets close to the maximum threshold.

Reporting Enhancements:

Provide a means to control HTML attributes.

Provide a specification: **TRUNCTAG** to eliminate the Long Names cross reference report that appears at the end of reports where entity names were too long to fully appear in the allotted space.

Provide a specification: **NOOVERFLOW** to suppress detail report headings after the initial headings in a report section are published.

Make sure unnecessary blank lines do not appear on reports.

Enhance the use of alternate report output options.

The **BANNERS/NOBANNERS** specification has been removed. It has been obsolete for many years. If it is detected, you will receive a warning. The normal recommended operational mode for this specification was **NOBANNERS**.

Grouping Enhancements:

This release now insures that if a particular execution required a grouping **COLD** start, it is performed on or before the shutdown of the current execution when it was detected. This prevents security violations when running reports in subsequent executions that were not expecting to have to update the Masterfile by running a **COLD** start.

The Masterfile entities may be grouped for reporting purposes as well as providing the basis for report distribution. Event Reporting uses the EKC External Grouping Facility to provide the definitions required to establish grouping structures that meet your business needs.

The act of determining group names for individual Masterfile entities is currently the longest and most processor intense operation in current releases of Event Reporting. The design was to allow the groupings to be dynamic, allowing you the ability to change your grouping rules and have it have an immediate effect on your Event Reporting processing.

Release 2.1 took the first step in dealing with the performance issues involved in grouping by establishing a Masterfile reference cache that contains all entities and their group names. This “cache” is referred to as the *grouping structure*, is initiated on demand when the possibility for grouping exists. The structures are either **COLD** or **HOT** started. **COLD** starts were normally required whenever the data on the Masterfile changed or the grouping rules changed. What this ended up requiring was a complete regrouping (a **COLD** start) after each Masterfile Update function was executed. A **HOT** start would normally be initiated between executions as long as the grouping rule file was the same and had not changed since the last execution.

In Release 2.2, the three main areas of grouping (*RESOURCE*, *SOURCE* and *USER*) are now considered individual structures with their own startup procedures.

Whenever the Masterfile is updated, the **COLD** start requirement is no longer posted. Instead, the new **VERIFY** attribute is posted. When it is determined that grouping may be required, the structures are started based on the startup mode requested for each individual structure.

Because **COLD** is no longer required after an Update, a **HOT** start is performed, which uses the existing structures cached on the Masterfile. It is possible that additional entities were added to the Masterfile during the update. To accommodate this possibility, the new **VERIFY** attribute is set. After the conclusion of the **HOT** start, and the **VERIFY** attribute was set, any entities not currently contained in the grouping structure are automatically added making the structure up to date (as if a **COLD** start were performed).

If a **COLD** start is required, it is performed at the structure level. For example, when the token purge occurs, the Resource Entities will have to be regrouped with a **COLD** start. The Source and User groupings do not need to be regrouped and will not be unless something requested them to be. If you change your Grouping Rules or the name of the RULES file defined to the execution, all structures will be **COLD** started.

Commands have been added to manually request grouping startup modes (if required).

Please refer to the *E-SRF Event Reporting: Command Reference Guide* for more information.

DOMAIN and SYSID:

The terms “**DOMAIN**” and “**SYSID**” have taken on new meanings.

The term **DOMAIN** is no longer considered an E-SRF term. All commands that relate to **DOMAIN** will still work, but will result in a warning and depending on system options, a user specified warning return code.

The Term **SYSID** now replaces **DOMAIN**. To get rid of the warning messages, replace the term **DOMAIN** with **SYSID**.

The reason for this change was the confusion with the true meaning of **DOMAIN**. It relates more with the E-SRF term **IMAGE**. The design of this product was to accommodate event data from any security system. Currently the two systems supported are ACF2 and RACF. Support is being extended to other security systems (such as TSS and NT). Because of their requirements, and the mindset of the personnel maintaining these systems, this change had to be made.

Dictionary Names:

The field: **RC.SUBMITTR** was added to the dictionary.

The fields: **xx.MACHINE**, **xx.LPAR** and **xx.SYSID** were added as alias to: **xx.SYSTEM** and have the same meaning of the previous field: **xx.DOMAIN**

The field: **xx.DOMAIN** was retained for compatability but is now considered an obsolete field. The use of this field will provide the same results as using **xx.SYSID**.

Masterfile Update:

Heartbeat:

Heartbeat is a feature provided by later releases of ETF/A and ETF/R. Its purpose was to create journal records that may be used to verify the journal records provided by the security system were intact.

A Heartbeat record is produced at controlled intervals. It will contain information about the security journal records written within the interval. This data may be compared by specially developed programs that capable of re-computing the same information using the records that are available to it. If the data is the same, the Heartbeat “*passes*”. If it does not, the Heartbeat “*fails*”. This release has been enhanced to provide this verification and publish warnings when Heartbeat intervals fail.

EXCLUDE Update specification:

The EXCLUDE Update Specification has been formalized and documented in this release.

Utilities:

Renamed the *Report Overlays Guide* to the *Report Overlays and Utilities Guide*. Provided documentation on the three optional Event Reporting utility programs provided for use by customers..

Changes have been made to these programs in this release. Because these programs were never documented in prior releases, no mention of these changes will appear in this document. If you have used these programs before, please refer to the Report Overlays and Utilities Guide to make sure you have an understanding of how these programs function.

ESRFASCI Provide ASCII print file

A utility to convert a standard mainframe print image file to normal ASCII print image file suitable to be downloaded as a binary file to a PC. The output is similar to the output produced by using the **CTLCHAR (ASCII)** specification in the **RUN** command.

This utility may be used to convert print files (such as the ones produced by Access Analysis) to a file that can be downloaded (*in binary format*) to a PC and printed using a normal PCL printer.

ESRFHTML Provide HTML print file

A utility to convert a standard mainframe print image file to HTML. The output is similar to the output produced by using the **CTLCHAR (HTML)** specification in the **RUN** command.

This utility may be used to convert print files (such as the ones produced by Access Analysis) to HTML so they can be viewed by a normal web browser. The conversion is in EBCDIC so you will need **ASCII/CRLF** when downloading to a PC.

ESRFSMFD

A utility to print SMF records in various formats.

This program was initially provided to be used for E-SRF Event Reporting problem determination but has been extended to cover a range of other applications.

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.

Data Only Address Spaces:

This product uses data-only address spaces to maintain some of its data structures. Because this product runs as a NON-APF (*not APF authorized*) product, certain installations may place limits on how many and how large a Data-Only Address Space can be. Previous releases provided a means to disable the use of Data-Only Address Spaces. In this release, you now have additional control over how large these Data-Only Address Spaces can be.

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:

A new command was added that posts basic information about current execution and the configuration you have established on the control report. The information presented is similar to what the ESRFSHOW report produces except in condensed form and appears on the SYSPRINT Control Report.

This is useful when attempting problem determination and need to see what is occurring between commands. This is not a command required for normal report production.

Table Management:

Table management is the heart of how this product manages its data structures. One of the longest instruction paths in this process is the routine to insert a new object into a table. A new algorithm was developed which will provide exceptional performance in this area. It has been partially exploited in this release and will be fully exploited after more field evaluation has been reviewed.

License Management:

A “License Management” provision has been incorporated into the Event Reporting to accommodate the needs of product leasing and large outsourcing organizations that want to license this product for a subset of their processing workload.

An enabling PTF must be received and applied to your system (*normally during installation*) for this product to function (in UPDATE mode). The vast majority of the user community running this product has a perpetual license that means once the enabling PTF is applied, no other concern for this issue remains.

The criteria are Customer ID and the scope of the product. There are no licensing issues relating to the processor hosting the product execution.

Customers who currently lease this product, or have tailored versions specific to their requirements will have more concern with this requirement. Previous product customization to maintain licensing compliance was not carried forward into release 2.2. This customization must be provided in the Licensing Enabling PTF.

If you feel you may have an issue with this, please feel free to contact EKC technical Support for assistance.