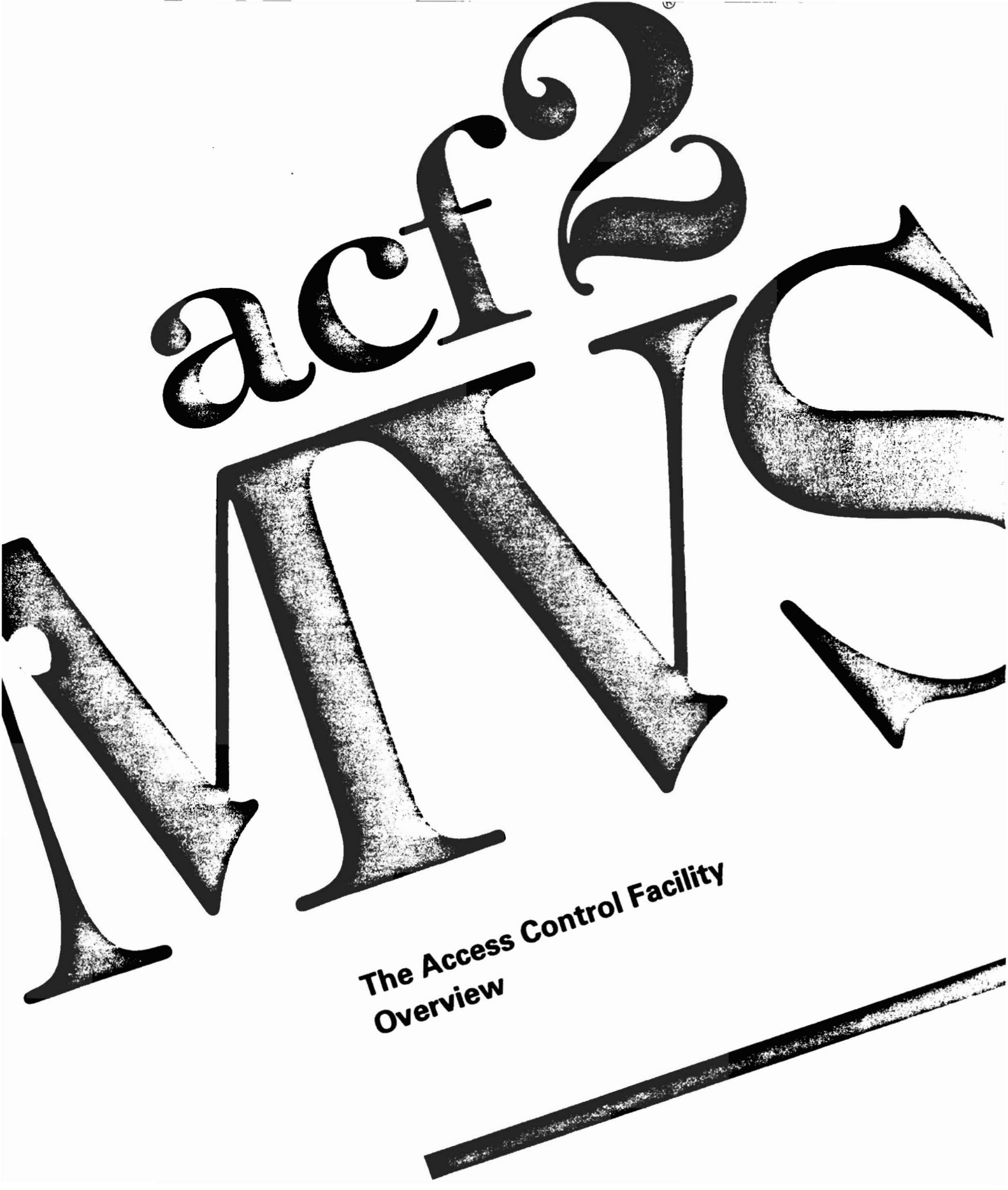
acf2®
MVS
The Access Control Facility
Overview

acf2™

The Access Control Facility

OVERVIEW

for

for acf2/MVS Release 4.0 Installations

Base Manual Dated: January 15, 1985

Doc. Nr. ABG0001-02

Printed in U.S.A.

ACF2 is a proprietary product developed and maintained by:

SKK, Inc.
10400 West Higgins Road
Rosemont, Illinois 60018-9990

Business Office: (312) 635-1040
Product Support: (312) 635-3000
TELEX: 206-186 (SKK ROSM)

A 24 hour answering service on (312) 825-5150 is available
for emergency assistance outside of normal business hours.

THE ACCESS CONTROL FACILITY: DEFINITION

acf2/MVS - the Access Control Facility, is a security extension to the IBM MVS Operating System. Security requirements are complex and diverse in today's fast-growing data processing community and no installation can afford to have less than state-of-the-art data access protection.

ACF2 provides this protection in a way no other available product does:

> ALL DATA IS PROTECTED BY DEFAULT on a system with ACF2 and is automatically protected from access by other than the owner unless pre-authorized by a security officer or by the owner.

In order to permit access (and thus the sharing of data), an ACF2 rule which specifically permits access must be entered in the ACF2 database. Thus, ACF2 surpasses mere protection of data and provides for the controlled sharing of data.

In ACF2, an algorithmic methodology is used to determine whether access to data by a specific user should be allowed. This method is flexible while totally efficient. It is also easy to use and understand. A data processing installation need not be concerned with non-technical users suddenly becoming burdened with a complicated system.

Also, ACF2 administration can be either centralized or decentralized, regardless of whether authorization responsibilities are centralized or decentralized. Thus, total computer security can be accomplished in a smooth and efficient way which best fits each installation.

ACF2: THE STRUCTURE

The Databases: ACF2 uses three databases:

* The Logonid database contains a record for each individual authorized to use the system.
* The Rule database contains access rules specifying who can access data, and under what conditions that access will be allowed.
* The Information Storage database contains global system options, generalized resource rules, and additional system data.

All three datasets are managed through VSAM, IBM's most advanced access method.

The "Logonid" Record: Fields of the Logonid record establish a profile of a user's identity and his privileges. Thus, an installation can restrict which individuals are able to perform various security-related functions such as:

* define new users to the system.
* control dataset access.
* issue operator commands.
* submit jobs from time sharing.
* use bypass label processing for tapes.
* issue mount requests from time sharing.
* use each subsystem, such as TSO, IDMS, IMS, CICS, etc.
* use various input devices, such as selected terminals, card readers, etc.
* access the system only at a pre-determined time, day, or shift.

THE GLOBAL SYSTEM OPTIONS

The Global System Options (GSO) distributed with the ACF2 package define most the system-wide options and default values that a site may use. GSO records are stored on the ACF2 Information Storage Database where they can be easily modified and dynamically activated to meet the specific needs and access scope of any data processing center.

The sophisticated structure of the Logonid and rule records, as well as the advanced facilities and numerous options of the ACF2 system, distinguish it from any other security package.

ACF2: THE CONTROLS

ACF2 System Controls

Users of an ACF2 system have a Logonid record with which a password is associated. Before performing any further processing, ACF2 irreversibly scrambles (one-way encrypts) the password, ensuring it cannot be deciphered. A non-encrypted password is never placed in storage, listed on a printout, or displayed by ACF2.

Several password control options are available to an installation, such as:

* limiting the number of times in one day that an incorrect password can be entered for a particular Logonid record before that Logonid is deactivated.

* determining the minimum number of characters allowed for a password.

* setting the maximum number of days allowed before a password must be changed.

Most production jobs need no passwords for submission in order to maintain security. These production jobs are submitted to the system through a pre-defined controlled path, eliminating the need for password checking and thus for password maintenance of production jobs.

An extra level of protection can be obtained by restricting the user's points of access to the system. For example, a user may be allowed to access the system only from a given combination of interactive terminals, remote terminals, and/or card readers.

"DEFAULT" is the Difference

Data protection by default makes ACF2 the unique security system that distinguishes it from all others. Absolutely no action need be taken to protect data -- only action to allow access is required. Every user must be identified, and all user accesses must be pre-authorized. Access rules are compiled, stored in the rule database, and referenced only when needed.

A Finer Degree of Control

An access rule set can further define the specific environment that must exist before a user (other than the owner) can access a dataset. For example, a rule can specify the input source of the job (terminal, reader, etc.), the program being used, and/or the specific library from which the program was executed.

Additionally, ACF2 can limit a user's system access capability to a specific pre-determined time period (e.g., shift of the working day).

Another powerful ACF2 feature is the ability to stipulate execute-only access authorization to program libraries, prohibiting reading or copying of powerful or proprietary software while still allowing them to be used (executed).

The Goal is Protection

As well as providing dataset and program protection, ACF2 safeguards billing account numbers, TSO procedures, tape and disk volumes, etc. ACF2 interfaces are also available for commonly used online interactive systems, such as IDMS, IMS, and CICS. Using these interfaces, the installation can protect resources such as CICS transactions, files, and programs; IDMS tasks, data areas, subschemas, and programs; and IMS transactions.

ACF2: CUSTOMER AIDS

The ACF2 package provides aids for all facets of system implementation and maintenance.

Transition Aids

The transition from a "no security" environment to a fully protected one can be made gradually under ACF2. Facilities are provided to help an installation phase in full protection without having an impact on normal protection processing by use of phased MODES:

* "Quiet" mode, the first in the series, performs user identification only. Dataset access and resource rule validations are not enabled.

* "Log" mode, the next in the series of transition steps, records access violations, formats them, and makes them available for analysis and to start building rules.

* "Warn" mode allows ACF2 to issue warning messages to the user in addition to recording violations, further enabling users and the installation's Security Officer to analyze access needs and to refine rules.

* "Abort" mode, the final phase, is one of full security, where access rules control data sharing and violation attempts are aborted and logged.

* "Rule" mode, allows the installation to phase in ACF2 protection on an individual basis for each dataset. For example, critical and sensitive datasets can be immediately protected by ACF2 in abort mode while less sensitive datasets can be placed in either warn, log, or quiet mode.

These transition modes can be applied to individual users or to datasets and other resources at different stages, thus allowing critical data to be fully protected immediately while less critical areas are phased in later. ACF2 will also co-exist with existing facilities, such as OS Password Protection or Expiration Date Protection, during the transition to full security.

Ease of Installation and Maintenance

ACF2 applies IBM standards for both installation and maintenance procedures and uses SMP (the IBM System Maintenance Program). ACF2 is supported by the designers and the developers of the system and is distributed with the following documentation:

* ACF2 Administrator's Guide
* ACF2 Auditor's Guide
* ACF2 CICS Support Manual
* ACF2 Composite Index
* ACF2 General Information Manual
* ACF2 Implementation Planning Guide
* ACF2 IDMS Support Manual
* ACF2 IMS Support Manual
* ACF2 Messages Manual
* ACF2 Other Products Manual
* ACF2 Overview
* ACF2 Reference Card
* ACF2 System Programmer's Guide
* ACF2 Utilities Manual

Backup and Recovery

ACF2 logs all changes to its databases and performs automatic daily backups. The ACF2 recovery utility can quickly provide a completely current ACF2 database in the event of destruction. Critical jobs can be allowed to run during the recovery process.

ACF2: THE EXTRAS

Tape Management System Interface

ACF2 provides optional tape dataset access control to insure equivalent protection of tape, disk, and mass storage data. Some tape management systems, such as UCC-1 and TLMS2, allow full standard dataset name matching with ACF2 without the use of local exits.

If a site does not have a tape management system or has one which does not retain full tape dataset descriptions, an installation may wish to use the ACF2 Pseudo Dataset Name Generator exit to more fully interface with the tape management system.

SMF Recording and Report Generators

ACF2 provides complete audit trails and event loggings via the standard system SMF recording facilities. Additionally, ACF2 monitors information and formats the data to provide automatic audit trails. The ACF2 package includes nine daily report generators and various "as required" utilities and reports for formatting and analyzing data. These include:

* The Invalid Password and Authority Usage report highlights each system access (Job submission or Logon/Signon attempt) denied by ACF2, along with the reason for the denial.

* The Restricted Logonid Job Log report logs each use of a restricted production Logonid, the job name, the time, and the source of submission.

* The Logonid, Rule, and Information Storage Modification Logs show each time a Logonid Record, Access Rule Set, or Information Storage entry was modified and which user was responsible for making the change.

* The Dataset Violations and Loggings report displays complete information about attempted invalid dataset accesses or accesses to critical datasets which ACF2 has been instructed to log. Also included are log records for usages of critical programs, and "trace" records for selected users.

* The Generalized Resource Violations and Loggings report displays complete information about invalid resource usage or accesses to critical resources which ACF2 has been instructed to log.

* The optional TSO (MVS) Command Record Log report contains usage statistics and command input for each TSO command issued.

ACF2 also provides various utilities which can be used as needed to identify other security-related information of concern to auditors and security administrators. These include:

* The Access Index report is an historical log of dataset access rules.

* The Dataset Cross Reference report specifies which users have access to which datasets, currently or at previous times.

* The Selected Logonid report is a listing of all Logonid records matching any selection criteria

specified by the user. For example, all users who have not changed their passwords in the last 30 days or all users with a particular group of attributes could be displayed.

* The Environment Report shows all security related environmental changes made to the ACF2 system. For example, this report details each time a global system option (GSO) is dynamically activated, each time the system operator issues a modify command to perform an ACF2 function, and the date and time of all system restarts (IPLs).

Support Activities

The ACF2 package is also supported by a full-time team of technicians and writers. The wide range of support includes (some at additional cost):

* Sponsorship of annual user's conference.
* Bimonthly newsletter.
* 24 hour technical support facility.
* Inhouse multi-CPU data center for maintenance and development.
* Regular program of product updates.
* Full time staffs devoted to documentation and user services.
* Regularly scheduled training classes and on-site training available via a full time customer training staff.
* Sales and support offices and representatives around the world.
* Computer security consulting services.
* Annual Users' Conferences in the U.S. and Europe.