

# CA ACF2™ r12 for z/VM

CA ACF2™ FOR Z/VM (CA ACF2) PROVIDES INNOVATIVE, COMPREHENSIVE SECURITY FOR BUSINESS TRANSACTION ENVIRONMENTS, INCLUDING THE VM SYSTEM, VM MINIDISKS, OPENEXTENSIONS VM, CMS AND SFS FILE AND MAINFRAME LINUX — ENABLING YOUR BUSINESS TO FULLY REALIZE THE RELIABILITY, SCALABILITY AND COST-EFFECTIVENESS OF THE MAINFRAME. IN CONJUNCTION WITH CA DISTRIBUTED SECURITY SOLUTIONS, CA ACF2 HELPS SECURE YOUR ENTIRE ENTERPRISE.

## Overview

There is increased concern about the security issues that arise when establishing web links to valuable mainframe data. Many organizations are also required to comply with government regulations, including HIPAA, SOX and GLBA, as well as existing corporate policies and industry agreements. With the introduction of new technologies for the mainframe, new security concerns are rapidly developing. To stay abreast of today's challenges organizations must strengthen security, streamline administration and provide enhanced auditing capabilities.

## Benefits

CA ACF2 delivers access control software for z/VM operating systems. Basic and advanced CA ACF2 mechanisms provide the flexibility and control that you need to monitor and adjust your security policies and accommodates virtually all organizational structures. Administrative tools, extensive reporting options, online monitoring and automatic logging capabilities accompany CA ACF2, securing your environment while enabling comprehensive auditing and controlled sharing of data and resources.

## CA Advantage

CA ACF2 is just one of many products and solutions that are part of CA's Enterprise IT Management initiative (EITM), which can help you unify and simplify IT management across the entire enterprise. When combined with other CA solutions, CA ACF2 provides end-to-end controls to help you meet your business and compliance requirements. And also provides end to end security when combined with CA's distributed security solutions.

---

## Security You Can Trust

Information security is critical to achieving business efficiency and growth, superior customer service and information privacy. Today, organizations view technology as a strategic resource and seek to gain competitive advantage by providing easier, faster and more reliable access to products and services. A secure, reliable and cost-effective security infrastructure is essential for the execution of today's business strategies. Many organizations are rightly concerned about the security issues that arise when establishing web links to valuable mainframe databases. CA ACF2 addresses these concerns by enabling IT organizations to exploit the latest hardware, networking and operating system components offered for the mainframe.

CA ACF2 protects your mainframe computer systems and data by controlling access to resources. It closely maps security to how you manage your organization using a flexible configuration mechanism unique to CA that automatically associates users to one or more roles. CA ACF2 delivers flexible, streamlined administration, helping you quickly and efficiently manage users and control resources. In addition, it enables rapid, cost-effective response to changing business needs. CA ACF2 is delivered complete with flexible and powerful administrative tools, automatic logging facilities, and extensive reporting and online monitoring capabilities. Authorized individuals are provided a wide range of opportunities to analyze and evaluate computer access activities and trends. Administrators can quickly and easily set and adjust security policies to respond to rapidly changing business needs.

### Distinctive Features and Functionalities

**COMPREHENSIVE SECURITY** CA ACF2 provides comprehensive security for z/VM resources across operating systems, subsystems, OEM software and databases.

- **Operating System Release Support** CA ACF2 supports new operating system releases as they become generally available.
- **Exploitation of New Releases** CA ACF2 takes advantage of new features and functions to provide enhanced security administration and management functionality.

**INCLUSIVE USER MANAGEMENT** Individual accountability is the key to effective information security. Many government regulations and corporate policies require separation of functions or duties. CA ACF2 lets you decide what policies are relevant and implement those structures.

- **Users** CA ACF2 provides easy-to-use administration functions that adapt to your organization's structure and procedures to support compliance with regulations and laws.
- **Role-Based Security** The CA ACF2 user identification (UID) string simplifies implementation of role-based security and is flexible in order to adapt to your organization's changes.
- **Individual Accountability** Each userid is protected by a password. Consistent password policies are enforced throughout your organization, strengthening the effectiveness of passwords and increasing information security.
- **User Definition Across Products** A component of CA-CIS Services, which lets you define a new user to all system products at the same time using one set of definition panels, CA-REGISTER lets you start a single transaction to define a new user to CA ACF2, Director, IBM's Shared File system and even to user-defined subsystems.

**DATA AND RESOURCE MANAGEMENT** Your data center managers are responsible for helping to ensure the integrity of all data and programs stored on their computer systems. Any data loss can potentially translate into financial loss. (See Figure A)

- **Protection by Default** CA ACF2 safeguards against loss or abuse by protecting all data by default. When CA ACF2 is implemented correctly, no action is required to secure your data.
- **Controlled Sharing of Data** CA ACF2 requires that you grant permission to allow access to resources. This process enables you to know and control who has access to what.
- **Extended Security** Management of Shared File System (SFS) lets CMS users use CMS files that do not reside on minidisks and enables validation of VM data spaces and utilization of Control Program (CP) commands and operands.
- **External Security Manager (CA ESM)** CA ESM provides the capability to secure other products that issue RACROUTE calls. The use of CA ESM can eliminate the need for a product specific interface between another product and CA ACF2, enabling a single security environment for greater protection.

FIGURE A

CA ACF2 new rule administration panel.

#### RULE ADMINISTRATION PANEL

```
H9PA-2110 Add Access Ruleset Control Information (2.1.1) eTrust CA-ACF2
COMMAND ==>
TIME 11:41

Rulekey ==> _____
Prefix ==> _____
Owner ==> _____
Resowner ==> _____
Mode ==> _____
Userdata ==> _____

Total Rule Entries : 0

PF1=Help 2=Print 3=Quit 4=Return 5=Execute 6=
PF7= 8= 9= 10=Previous 11=Next 12=Retrieve
```

**AUDITING AND MONITORING** Several laws in many countries require organizations to establish internal controls pertaining to computerized data. CA ACF2 includes a variety of audit functions that provide the information and capabilities you need to monitor access and assess the propriety of access rights.

- **Auditing** CA ACF2 generates audit records for virtually any security related event, including start and stops of the security system, any command to modify the running security system, successful or unsuccessful user system entry or exit, failed or audited data set access, failed or audited resource access and changes to the security databases.

- **Reports** CA ACF2 provides a complete set of report generators that let you view and analyze your security event information. In addition, it allows you to limit the output of a particular report according to the privileges and restrictions of the specific user who is executing the report.

**SEPARATION OF ADMINISTRATIVE FUNCTIONS** While the implementation of security is very important, so is the responsibility for security administration. Restricting who can grant access and define your users is a cornerstone for effective security. CA ACF2 provides separation of security administration functions and duties, an additional management control that safeguards your systems and preserves the integrity of your security records.

- **Decentralized or Centralized Administration** CA ACF2 delivers several ways for you to separate security administration functions. First, it provides you with different levels of administrative authority (privileges) over your users and/or resources. In addition, it can scope or limit privileges to discrete security functions, areas or resources.
- **Changes to Security** Standard reports display updates, additions, changes or deletions of any CA ACF2 user or rule, or other security records.

**ADMINISTRATION DIVERSITY** Without proper administration, there can be no guarantee that your security is structured correctly. To help meet your business requirements and ease the administration process, CA ACF2 includes flexible and powerful administration tools. (See Figure B)

- **Command Processing** CA ACF2 allows you to administer security in multiple ways, such as CMS commands and the CA ACF2 full-screen panels.

FIGURE B

CA ACF2 new user definition panel.

USER DEFINITION PANEL

```

M9PA-1110          Define New User (1.1.1)          eTrust CA-ACF2
COMMAND ==> _____
                                                    TIME 11:30

Logonid    ==> _____      Prototype ==> _____
Name       ==> _____      Phone     ==> _____
Expiration date ==> mm/dd/yy

Password Information:
Initial password      ==> _____
Initial password verify ==> _____
Minimum days between changes ==> _____
Maximum days between changes ==> _____

Restrictions:
Source  ==> _____  Shift  ==> _____  Zone  ==> _____
Prefix ==> _____  Synerr ==> _____  Nospool ==> _____
Scplst ==> _____  Umidle ==> _____  Umidleop ==> _____

Use the 'Next' command (or PFkey) for more fields.

PF1=Help      2=Print      3=Quit      4=Return    5=Execute    6=Format
PF7=          8=          9=          10=Previous 11=Next     12=Retrieve

```

## What's New in CA ACF2 r12 for z/VM

FUNCTION/FEATURES	BENEFITS
<p><a href="#">Support for z/VM 5.3</a></p>	<p>CA ACF2 r12 includes support for z/VM Version 5 Release 3.0, including the ability to use password phrases. Password phrases are defined as being between 9 and 200 characters long, and may contain upper and lower case characters, numbers, selected special characters, and blanks. In CA ACF2, password phrases are part of the new "PWPHRASE" User Profile record. The following are user defined global controls that define what is allowed for a valid password phrase:</p> <ul style="list-style-type: none"> <li>• Minimum length</li> <li>• Maximum length</li> <li>• Minimum number of words</li> <li>• Minimum number of required alphabetic characters</li> <li>• Minimum number of required numeric characters</li> <li>• Minimum number of special characters</li> <li>• Special characters that are allowed</li> <li>• Maximum number of repeating characters</li> </ul>
<p><a href="#">LOGONID Controls</a></p>	<p>The following new logonid fields have been added to r12:</p> <p><b>CRE-TOD</b> Indicates the date and time that a logonid record was created.</p> <p><b>PSWDCVIO</b> Indicates the number of cumulative invalid password attempts for a user that occurred since the logonid record was created.</p> <p><b>PSWD-UPP</b> Specifies that the new password will be stored in upper-case.</p>
<p><a href="#">Password Controls</a></p>	<p>The following new password controls have been added to the "PSWD VMO" record:</p> <p><b>PSWDLC</b> Specifies whether CA ACF2 requires at least one lowercase (a-z) character in a new password.</p> <p><b>PSWDUC</b> Specifies whether CA ACF2 requires at least one uppercase (A-Z) character in a new password.</p> <p>In addition, the PSWDSPLT option to require a national or user-defined character between the first and last character of a new password is being changed to require a national or user-defined character anywhere in the password.</p>
<p><a href="#">LINUX Enhancement</a></p>	<p>CA ACF2 r12 supports combining values from qualified and unqualified Linux User profile records for the LINUXGRP and LINUXNAM fields. If the value in the qualified record is null, the value will be taken from the unqualified record. In addition, default Linux user and group records may now be defined. For the LINUXNAM field, if the value cannot be obtained from a qualified or unqualified record, it will be taken from the default record.</p>

FUNCTION/FEATURES	BENEFITS
<a href="#">Changes to RULELONG Processing for CMS Databases</a>	<p>Prior to r12, RULELONG was only available if CA ACF2 VSAM databases were being used, since the CA ACF2 CMS database structure only supports records up to 4096 bytes long. This also meant that VSAM databases needed to be used for any new features, such as ACTIVE date, which require the RULELONG option.</p> <p>While the CMS database structure is still limited to 4096 byte records, the ability to use RULELONG with CMS databases has been added to r12, to enable ACTIVE date and any future rule features to be used with CMS databases. Because the RULELONG rule format takes up more space, the Dynamic Compile feature (COMPDYN) has also been added to r12. COMPDYN allows rules to be compiled with the standard compiler, only switching to the RULELONG compiler if necessary to support a new option that requires RULELONG.</p>
<a href="#">Database Synchronization Component</a>	<p>In the past, database sync was used to synchronize CA ACF2 databases between z/VM and z/OS systems. In r12, Database Synchronization has been modified to allow synchronization to occur between two VM systems.</p>
<a href="#">ACFFS Enhancements</a>	<p>The following support for ACFFS has been added:</p> <ul style="list-style-type: none"> <li>• Support has been added to ACFFS rule panels for ACTIVE date (requires RULELONG).</li> <li>• Support has been added to ACFFS for Control VMO records. This includes the ability to add, display, change, and delete VMO records. Individual VMO records can be selected from a list of existing VMO records based on masking of the SYSID and RECID values. Each VMO record has a separate set of panels specifically designed for that record. HELP files are included both at the panel level and field level.</li> <li>• Support has been added to ACFFS for SHOW commands. Each SHOW command will be able to be selected from a menu, and the output displayed in a panel with the ability to locate text, scroll forwards or backwards, or print all of the output from the SHOW command to the virtual printer.</li> </ul>

## CA ACF2 enables you to strengthen security, streamline administration and provides enhanced auditing capabilities

CA ACF2 protects your mainframe computer systems and data by controlling access to resources. It closely maps security to how you manage your organization using a flexible configuration mechanism unique to CA that automatically associates users to one or more roles. CA ACF2 delivers flexible, streamlined administration, helping you quickly and efficiently manage users and control resources. In addition, it enables rapid, cost-effective response to changing business needs.

CA ACF2 enables you to strengthen security, simplify administration and provides enhanced auditing capabilities so that you: efficiently manage user identities and access to assets, proactively monitor accesses and reports, enforce business policies, comply with regulations and achieve end to end security management. CA ACF2 allows your organization to securely take advantage of the latest hardware, networking and operating system components offered for the mainframe. When combined with other CA solutions, CA ACF2 provides end-to-end controls to help you meet your business and compliance requirements.

---

## CA Advantage

CA's Mainframe Identity and Access Management products are integrated components of CA's comprehensive portfolio of Identity and Access Management solution, enabling customers to easily manage and protect IT assets across all platforms and environments. By leveraging CA's end-to-end Identity & Access Management solution, organizations can centralize user identity administration, provisioning and access management across the enterprise to improve IT efficiency, reduce IT costs and enhance user productivity. It also enables security administrators to view consolidated cross-platform security events for enhanced auditing and compliance and faster response to security risks and incidents.

To optimize the performance, reliability and efficiency of your overall IT environment, you need to tightly integrate the control and management of distinct functions, such as operations, storage, and life cycle and service management, along with IT security and identity and access management capabilities. CA's vision for enabling this higher level of management control is Enterprise IT Management (EITM).

EITM is a dynamic, secure approach that integrates and automates the management of information technology applications, databases, networks, security, storage and systems across departments and disciplines to maximize the full potential of each. CA's comprehensive portfolio of modular IT management solutions helps the enterprise unify, simplify and secure IT to better manage risk, costs and service, and ensure that IT meets the business needs of the enterprise.

CA Technology Services™ and our partners can help you assess your current IT situation, define your goals and implement solutions to gain measurable results. To keep your CA solutions operating at peak performance, CA support delivers unparalleled technical and customer support worldwide, and we offer training and certification through CA Education.

---

## Next Steps

CA ACF2 delivers flexible, streamlined administration, helping you quickly and efficiently manage users and control resources.

---

To learn more about CA ACF2, visit us at [ca.com/iam](http://ca.com/iam).