

CA ACF2™ r15 for z/OS



CA ACF2™ for z/OS (CA ACF2™) provides innovative, comprehensive security for your business transaction environments, including z/OS UNIX and mainframe LINUX — helping your business realize the reliability, scalability and cost-effectiveness of the mainframe. In conjunction with CA Technologies 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, PCI and GLBA, and existing corporate policies and industry agreements. With the introduction of new technologies for the mainframe, new security and compliance concerns are rapidly developing. To stay abreast of today's challenges, organizations must strengthen security, streamline administration and provide enhanced auditing and compliance capabilities.

Benefits

CA ACF2 delivers out-of-the-box access control software for z/OS operating systems, which includes interfaces for CICS, z/OS Unix (formerly known as OMVS) and IMS (and an optional add-on for DB2). CA ACF2 mechanisms provide flexibility and control to help you monitor and adjust your security policies and accommodate virtually all organizational structures. Administrative tools, extensive reporting options, online monitoring and automatic logging capabilities accompany CA ACF2 to secure your environment while enabling comprehensive auditing and controlled sharing of data and resources.

Mainframe 2.0

CA ACF2 has adopted key Mainframe 2.0 features that are designed to simplify your use of CA ACF2 can enable your staff to install, deploy and maintain it more effectively and quickly..

- CA Mainframe Software Manager: The CA Mainframe Software Manager (CA MSM) automates CA ACF2 installation, deployment and maintenance and removes SMP/E complexities.
 - The Software Acquisition Service enables you to easily move product installation packages and maintenance from CA Support Online directly to your mainframe environment and prepare them for installation.
 - The Software Installation Service standardizes CA ACF2 installation, which includes a new, streamlined Electronic Software Delivery (ESD) method that allows CA ACF2 to be installed using standard utilities. This service also provides standardized SMP/E product installation and maintenance via APARs and PTFs, and simplifies SMP/E processing through an intuitive graphical user interface and an intelligent Installation Wizard.
 - The Software Deployment Service enables you to easily deploy CA ACF2 in your mainframe environment.
 - CA MSM Consolidated Software Inventory (CSI) updates and infrastructure improvements add flexibility to CA MSM processing of CSIs and enable CA MSM to more effectively utilize CPU and system memory.
- Installation Verification Program (IVP) and Execution Verification Program (EVP): As part of qualification for inclusion in the set of mainframe products from CA Technologies that are released every May, CA ACF2 has passed stringent tests performed through the IVP and EVP to find and resolve interoperability problems prior to release. These programs are an extension of the CA Technologies ongoing interoperability certification initiative launched in May 2009.
- Best Practices Guide: This guide provides information on CA ACF2 installation, initial configuration and deployment to shorten the learning curve for staff that are responsible for the installation and management of this product.
- Health Checker: The Mainframe 2.0 Health Checker from CA Technologies provides CA ACF2 Health Checks that execute under the IBM Health Checker for z/OS.
 - The CA ACF2 Health Checker is a valuable tool to identify potential problems before they impact your availability, or worse, cause system outages. It checks the current active CA ACF2 settings and definitions for a system and compares the values to those suggested by CA Technologies or defined by you.

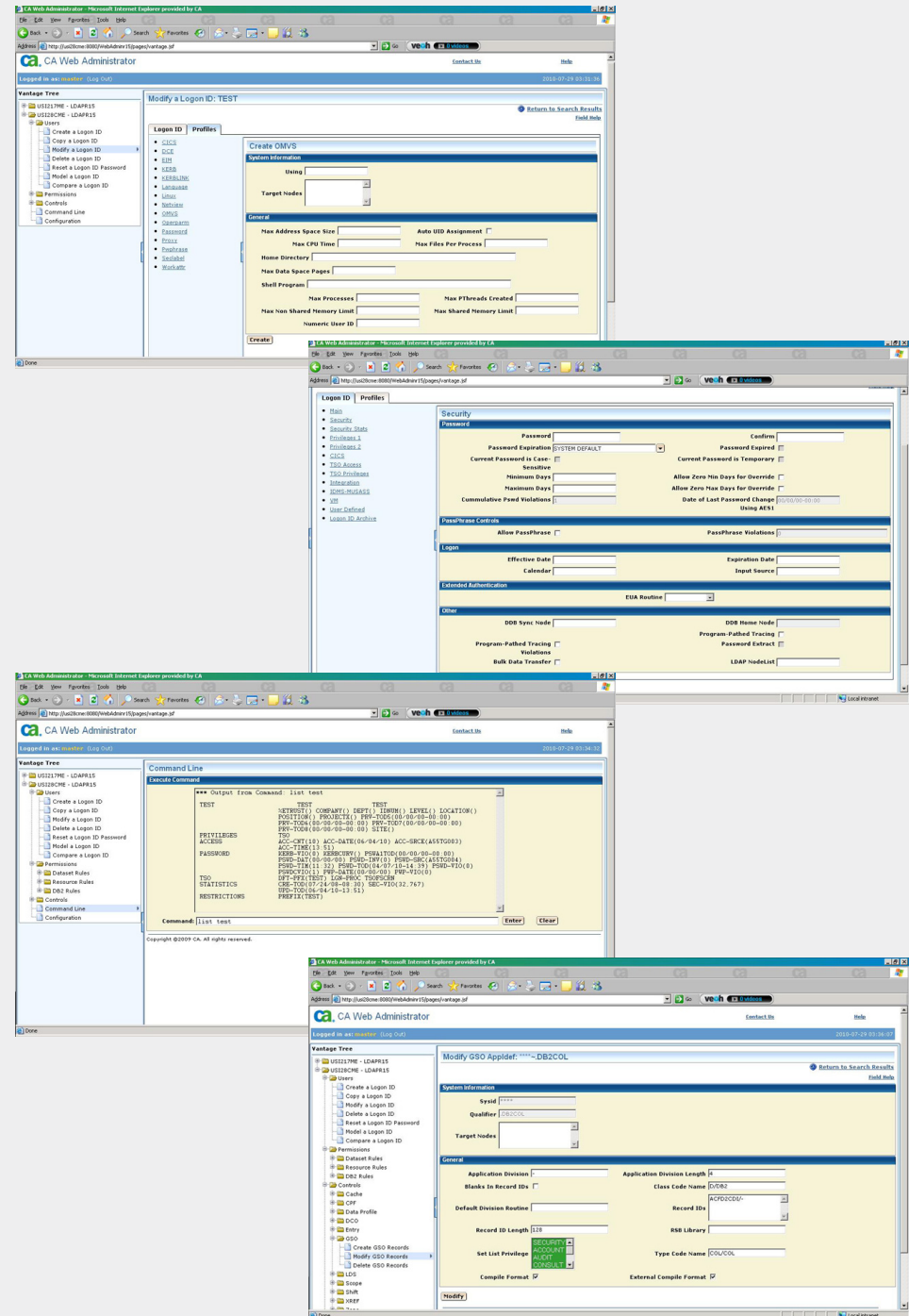
CA ACF2 Safeguards Your Data

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 helping IT organizations exploit the latest hardware, networking and operating system components offered for the mainframe. CA ACF2 is designed to protect your mainframe computer systems and data by controlling access to resources. It closely maps security to how you manage your organization by using a flexible configuration mechanism unique to CA Technologies that automatically associates users to one or more roles. CA ACF2 delivers flexible, streamlined administration, helping you to 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 with 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.

CA Web Administrator for ACF2™

Logon ID and Profile tabs in CA ACF2 using CA Web Administrator



What's New

CA ACF2 r15 for z/OS delivers and builds on product integration with CA Mainframe Software Manager (MSM) and CA Distributed Security.

Key Capabilities

Comprehensive Security CA ACF2 provides comprehensive security for z/OS resources across operating systems, subsystems, OEM software and databases.

- **Operating System Release Support** CA ACF2 support is planned for 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.

Note: CA Technologies does not provide legal advice. No software product referenced herein serves as a substitute for your compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, standard, policy, administrative order, executive order, and so on (collectively, "Laws")) referenced herein or any contract obligations with any third parties. You should consult with competent legal counsel regarding any such Laws or contract obligations.

- **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 user ID is protected by a password. Consistent password policies are enforced throughout your organization, strengthening the effectiveness of passwords and increasing information security.
- **System Entry** CA ACF2 controls entry into virtually all z/OS subsystems and VTAM/TCP/IP applications, including TSO, batch, z/OS UNIX, mainframe Linux, CICS, IMS, DB2 for z/OS and more.
- **Certificate Management** To help you reduce the administration time and effort needed to support digital certificates, CA ACF2 lets you store, generate, administer and process certificate requests. In addition, the CA Distributed Security Integration Server for z/OS (CA DSI) component added the ability to store, connect certificates to key rings and delete certificates from CA ACF2 using the provided SDK. This allows for integration with the Certificate Authority of your choice.

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.

- **Protection By Default** CA ACF2 is designed to protect all data by default when in full ABORT mode. CA ACF2 helps protect critical data sets and resources by limiting access to the appropriate people and reporting unauthorized access attempts.

- **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.

- **Data Classification** There is an increasing number of regulations pertaining to the secure access of data. The Health Insurance Portability and Accountability Act (HIPAA) dictates the type of data that must be kept confidential for patients. The Family Educational Rights and Privacy Act (FERPA) describes the data that can be accessed from a student's educational records. There are also many other regulations (SOX, FISMA, FFIEC, etc.) that can pertain to secure data. CA ACF2 provides tracking records that help determine what data (files, data sets and resources) pertain to which regulation.

Auditing And Monitoring Several laws, and industry-wide regulations in many countries require organizations to establish internal controls pertaining to computerized data. CA ACF2 includes a variety of audit functions that provide information and capabilities to help you monitor access and assess the propriety of access rights.

- **Auditing** CA ACF2 generates audit records for virtually any security related event. These include: starts 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, changes to the security databases and any security-related z/OS UNIX events. In addition, CA ACF2 provides an ACCESS command to facilitate the requirement to quickly review access to data or resources.

- **Reports** CA ACF2 provides a comprehensive set of reports 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 and an additional management control that safeguards your systems. CA ACF2 also helps preserve the integrity of your security records.

- **Decentralized Or Centralized Administration** CA ACF2 delivers several ways for you to separate security administration functions. It provides you with different levels of administrative authority (privileges) over your users and 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.

- **Command Processing** CA ACF2 allows you to administer security in multiple ways, such as TSO, batch, CICS, IMS, CA Identity Manager and CA Web Administrator for ACF2™.

- **Multiple Image Security Administration** In an environment with multiple system images, you can send CA ACF2 commands from one node to single or multiple nodes. This is accomplished through the CA ACF2 Command Propagation Facility (CPF).

Security Information Sharing To reduce security administration, human error and costs, security information must be shared across a networked environment. CA ACF2 works with other solutions to provide comprehensive information security across your network.

- **CA LDAP Server for z/OS (CA LDAP Server)** This component provides a single interface for applications to request security services, including adding, updating and retrieving information. It can be used to securely perform user authentication on behalf of business applications running on z/OS and other platforms connected through TCP/IP. You can leverage the existing information stored in your z/OS security solution and achieve mainframe-strength user authentication for applications throughout the enterprise by connecting to CA ACF2 through the CA LDAP Server.

- **LDAP Directory Services (LDS)** LDS provides flexible sharing of CA ACF2 administrative changes to remote security repositories residing on distributed platforms.

- **CA Distributed Security Integration (CA DSI)** While the CA LDAP Server provides an interface to security services, it is limited to what the LDAP protocol supports. The CA DSI Server was created to provide the following additional functionality while restricting access using native security scoping: .

- CERT2UID – Maps a digital certificate to a user ID using the External Security Manager (ESMs). The digital certificate must reside in the ESM for this function to succeed.
- DATAPUT – Adds a certificate to the database and connects it to a key ring. If the specified key ring does not exist, an attempt is made to create the key ring.
- DATAREMOVE – Removes a certificate from a key ring. You can also indicate that the certificate should be removed from the database. For it to be deleted from the database, it cannot be connected to any other key rings.
- DELETERING – Deletes a key ring.
- GETPNL – Retrieves the groups associated with a LID. (This is CA ACF2 specific.).
- GETVER – Gets the product name and version of the ESM that is currently running.
- MAPUID – Maps a long user name to a short name or a short name to a long name using the ESMs.
- NEWRING – Creates a new key ring.
- PASSCHK – Performs user ID and password authentication to the ESM.
- PURGERING – Removes all certificates from an existing key ring.
- RESCHK – Performs a resource authorization check to the ESM.

- XEQCMD – Issues native commands to the ESM using the same native syntax as TSO or batch.

▪ **LINUX On System z Support** CA Pluggable Authentication Module (CA PAM) allows CA ACF2 to act as an authentication server for one or more Linux systems, eliminating the need for redundant security administration to define users on a system-by-system basis. CA PAM Client for Linux for System z can authenticate to CA ACF2 for z/OS or z/VM.

▪ **IBM Policy Director (PDAS)** CA ACF2 utilizes the common SAF interface to support customers' usage of IBM Policy Director.

▪ **CA Web Administrator For ACF2** CA ACF2 customers have had limited, text based, options for maintaining their z/OS security information. With the retirement of knowledgeable security administrators, customers are trying to maintain their systems using less experienced and non-mainframe personnel. Something is needed to help these new administrators accomplish what is needed in a faster and easier manner than reading the 1,000 page administrator guide and trying to determine the correct command syntax. The CA Web Administrator for ACF2 provides an internet browser-based GUI interface to help these new administrators. The CA Web Administrator for ACF2 is designed to provide a comprehensive administration solution for CA ACF2 using a browser-based GUI.

The CA Web Administrator:

- Provides the ability to communicate with CA ACF2 through the CA LDAP Server.
- Enables administration to be performed in real time against live CA ACF2 data.
- Provides the ability to administer CA ACF2 anywhere that you have an accessible browser, using SSL for security.
- Allows administrators to input native commands directly from the GUI and receive output if desired.
- Restricts data access using native security scoping.
- Provides the ability to issue console commands during pre- and post-processing of any record.
- Simplifies administration so there is no need to memorize native commands or hundreds of fields.
- Lowers the learning curve for new administrators.
- Allows activity to be logged for auditing purposes, via native SMF records.

What's New with CA ACF2 r15 for z/OS

function/features	benefits
CA Mainframe Software Manager	CA MSM simplifies and unifies the management of CA Technologies mainframe products on z/OS systems and is an integral component of the MF 2.0 solutions for the z/OS operating system. As z/OS products adopt the services provided by CA MSM, you can acquire, install, and maintain them in a common way. These services enable you to manage your software easily, based on industry accepted best practices such as SMP/E, FTP, USS and Java.
New Utility and Documentation for Enhanced Role-based Security	Help with administration of roles. 1) Ability to identify all users assigned to a role 2) The cleanup of users within roles 3) A migration path to assist in moving from the old "UID string rules" to the new role-based security rule sets
Enhanced usability for Digital Certificates	Easier administration. 1) A RENEW command to simplify the administration of renewing certificates that are defined on the ACF2 database 2) Expanded size limits of the IDN/SDN extensions 3) Certificate Utility now displays all Certificate extensions 4) Expanded key ring size to hold more certificates 5) Prompting for passwords, removes the need to include clear-text passwords on commands 6) Warnings before certificates expire to prevent service interruptions
Restricted Administrative Privileges	The ability to create "limited" security officers. For example, 'helpdesk' personnel can be created who only administer password resets and password-related fields, or users who are only authorized to issue digital certificate related commands.
User Comparison	The ability to compare two Logonid records and associated user profile records.
IMS Support	A single CA ACF2 IMS r15 function is now used for all supported IMS releases, thereby streamlining installation and maintenance.
User Modeling	The ability to automatically model one user to create another; including user profile information and roles. This can be extremely useful when users switch roles or new users are created.
Virtual Storage Constraint Relief	Improved storage utilization and increased performance through exploitation of above-the-bar 64-bit storage.
AUTOERAS Enhancements	Additional AUTOERAS record fields provide more granular controls over AUTOERAS Erase-On-Scratch (EOS) processing.
TSO Enhancements	Use of screen scraper technology is simplified by the new NOBYPPAUSE TSO record option which removes the wait that occurs when CA ACF2 messages are displayed. Additionally, a new TSO record option, LOGHERE, controls whether an existing TSO user's session can be pre-empted by that same user at a different terminal.
Serviceability	Additional diagnostic capabilities help CA Support identify product release and maintenance status.

The CA Technologies Advantage

Mainframe Security products from CA Technologies are integrated components of the comprehensive Security Management solution set that enables customers to easily manage and protect IT assets across all platforms and environments. By leveraging this end-to-end Security 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. This solution 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 lifecycle and service management, along with IT security and identity and access management capabilities. CA Mainframe Security helps provide a consistent and secure platform across your entire IT environment, including emerging technologies that you might adopt in the near future.

CA Technologies has been a leader in IT management for over 30 years, has over 1000 security customers, and is committed to continuing to bring innovative security capabilities to them. We have a very large and dedicated group of security experts who know how to make security deployments successful, and help our customers achieve very quick time-to-value.

Next steps

If you're finding that:

- You need to strengthen security...
- You are struggling with the costs and effort required for compliance with relevant industry and regulatory requirements...
- Budgetary pressures are demanding greater efficiencies in your administrative functions...
- You are concerned about potential risks and need to enhance auditing capabilities...
- You need to be able to offer more rapid development of services and business applications, but cannot rewrite all your code as part of moving to SOA...

...then take a look at CA ACF2 r15 for z/OS. When combined with other CA Technologies solutions, CA ACF2 provides end-to-end controls to help your organization address business and compliance requirements across the enterprise. Visit us at ca.com/mainframe/security today.

Copyright ©2010 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. This document is for your informational purposes only. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document "as is" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or non-infringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill or lost data, even if CA is expressly advised in advance of the possibility of such damages.

2839_0910