IBM Security zSecure Admin

Enhance security administration, user management and compliance for IBM RACF

Highlights

- Automate administrative tasks to help increase efficiency and reduce errors
- Help identify potential problems quickly to minimize the risks of security breaches
- Administer multiple systems from a single session and perform IBM® Resource Access Control Facility (IBM RACF®) database cleanup

As the standard security system for mainframes running IBM z/OS®, RACF plays a vital role in helping to protect mainframes from unauthorized entry and misuse by authorized users. But the ultimate strength of your mainframe security system lies in the people who manage it. This makes it essential to furnish security personnel with the tools to perform their work as efficiently as possible. However, helping ensure that the RACF staff is sufficiently skilled and leveraging the power inherent in RACF can be challenging.

IBM Security zSecure™ Admin provides security personnel with tools to help unleash the potential of your mainframe system—enabling efficient and effective RACF administration while helping use fewer resources. By automating many recurring system administration functions and by enhancing the native RACF authorization and delegation capabilities, zSecure Admin can help you maximize IT resources, reduce errors, improve quality of services and demonstrate compliance.

Automate routine tasks to simplify administration

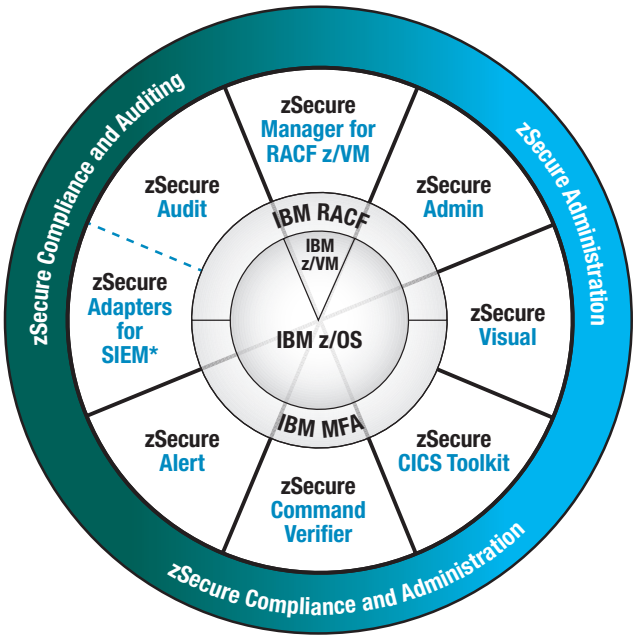
Easy to install and deploy, zSecure Admin offers robust, nonintrusive security capabilities designed to help simplify the process of managing mainframe security. The result is that complex tasks can become simple, one-step actions performed, helping to reduce the learning curve associated with RACF. Queries can be executed in seconds, and mass changes

can be implemented with little administration effort. zSecure Admin enables you to automate recurring, time-consuming security tasks such as:

- Adding or deleting userids and groups
- Defining and granting access to users and user groups
- Setting and resetting userids and passwords
- Restructuring RACF group trees and role-based access projects
- Creating and managing digital certificates
- Displaying, copying or removing all occurrences or a cross-reference of a userid or a user group
- Collecting and reporting on IBM Db2® resources and the corresponding internal and RACF security settings
- Determining the protection of member resources such as IBM Customer Information Control System (CICS®) transactions
- Managing options for pervasive encryption keys for IBM Z® and for IBM Multi-Factor Authentication for z/OS (IBM MFA)
- Feeding security event information into IBM Operations Analytics for z Systems®
- Running daily or monthly reports for functions such as identity governance

Through the ability to distribute administrative authority on a more granular level than within native RACF, security administrators can delegate the authority to perform password resets, resume a user and grant specific accesses—all without granting full administrative privileges to the distributed staff. This capability enables frequently requested user support tasks to be managed by the support staff closest to the user, frees up security personnel for mission-critical tasks, aids in reducing help desk overhead and—with segregation of duties—helps reduce the risk of security breaches by privileged users.

IBM Security zSecure suite



* Product offers a subset of the capabilities provided by zSecure Audit

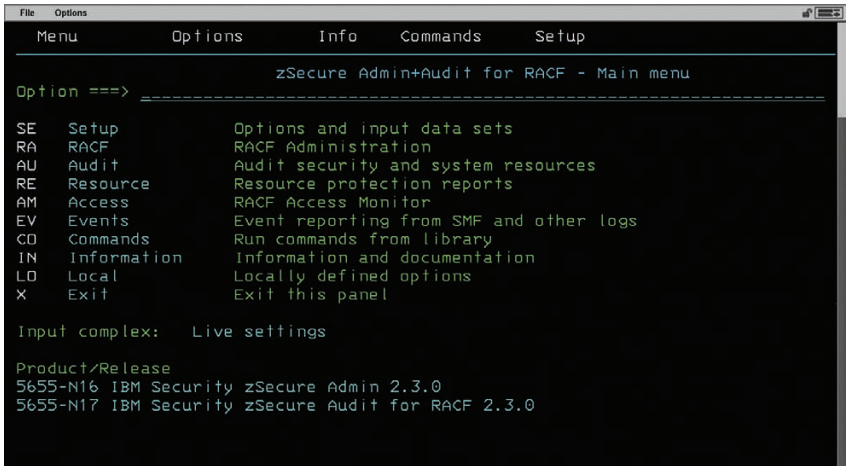
Summary of products that comprise the IBM Security zSecure suite, including IBM Security zSecure Admin

In addition, zSecure Admin allows security personnel to queue commands for execution at a later date and for a specific duration. After the time interval has expired, authorization is automatically returned to the previous state. For highly sensitive userids, you can even opt for a policy whereby two, or even three, administrators must approve a command before it is executed.

zSecure Admin offers a RACF Offline function that provides the capability to facilitate administration and audit of changes by creating a mirrored copy of the RACF database that enables RACF administrators to check and verify their configurations offline, without affecting the production database. The ability to test changes and review the results before implementing them reduces the risk of introducing errors into the production database—this is quality assurance for RACF Administration, helping you to maintain security and availability of systems and applications.

The RACF Offline function can be used in a variety of circumstances, such as combining workloads from newly acquired companies or providing a simulated RACF environment to aid in release-to-release RACF migrations. In addition, RACF Offline can be used for required testing of strong password encryption or any new function or new combination of products without impacting the normal production workload or running the risk of unexpected security results. Customers can use RACF Offline to test major policy changes or additions before implementing them into production to help lower risk of implementations for new policies, reduce human error and minimize possible security outages related to the proposed changes.

zSecure Admin can administer multiple systems with a single application interface for fast live data access on all of the selected systems in the enterprise to keep their security synchronized. Administrators can send the same command to multiple systems with or without RACF remote sharing facility. Data encryption protects the cross system communications.



zSecure Admin makes RACF administration faster and easier. It provides quick access to frequently used functions and extensive reporting capabilities, enriched with context-aware actions that help you to easily organize your database.

RACF database usage reporting and database cleanup

The Access Monitor capabilities of zSecure Admin can report on actual usage of profiles and authorizations and relate that information to the information defined in the current RACF database. This helps security personnel to:

- Understand how profiles and authorizations are being used in production, while also providing user-to-resource relationships
- Identify unused or obsolete profiles and authorizations in access control lists, as well as potential identity governance issues due to over-entitlement
- Determine how RACF database changes will affect users prior to implementing them

RACF database cleanup can analyze profiles, permits and connects, and then automatically generate the commands necessary to clean up the RACF database by removing unused or obsolete information. Security personnel can review these commands prior to execution to confirm that cleanup actions will not affect definitions that must be retained. Data collection and analysis is optimized to improve data consolidation, using less memory and CPU, and reducing elapsed time.

Identify and analyze problems to minimize threats

zSecure Admin can help you quickly identify problems in RACF, such as missing or inconsistent definitions, enabling you to fix or prevent mistakes before they become a threat to security and compliance. You can also monitor privileged users to help ensure that old accounts are properly deleted and that products have been integrated appropriately—helping avoid vulnerabilities and entitlements creep with identity governance.

Furthermore, zSecure Admin integrates smoothly with IBM Security zSecure Audit for end-to-end monitoring and remediation. While zSecure Audit enables you to efficiently measure and verify the effectiveness of your mainframe security and security policies, zSecure Admin enables you to take the appropriate steps to remediate problems in an efficient, cost-effective manner.

Because zSecure Admin displays data from the active (live) RACF database, you can view up-to-date data, including any recent administrative changes.

The security personnel can also immediately verify the effect of the changes, without having to wait for a refresh of the extract file or unloaded RACF database.

In addition, you can request information about individual definitions in RACF or unload all RACF profiles to an external database, such as Db2, for offline analysis and reporting.

zSecure Admin also integrates with IBM Operations Analytics for z Systems to provide a dashboard containing a graphical overview of RACF events, based on detailed information collected by the Access Monitor component of zSecure Admin.

Merge databases quickly and efficiently

In today's ever-changing business world—where mergers and acquisitions are a frequent fact of life—flexibility is essential, especially where database management is concerned. zSecure Admin helps ease the burden of consolidation efforts by enabling you to:

- Compare profiles
- Efficiently merge security rules from different databases
- Copy or move users, groups, resources, applications or whole databases between systems
- Rename IDs within the same database

In addition, when merging profiles from different databases, zSecure Admin performs extensive consistency checks and reports potential conflicts before generating commands.

Store non-RACF data to reduce organizational costs

zSecure Admin enables you to store non-security information in the RACF database, such as telephone numbers, accounting codes and email addresses. It also supports installation data fields, custom fields and USRDATA and allows you to view and update this information. Access controls help keep the information safe and confidential.

You can also include information from external files in your RACF profile displays and reports. For example, you can match human resource information with user profiles to include the human resource information in the RACF profile displays and reports.

Why IBM?

Based on more than 25 years of experience in security audit and compliance, zSecure Admin offers an industry-leading solution to help organizations harness the power of the RACF security environment. zSecure Admin integrates seamlessly with the complete IBM Security zSecure suite of enterprise-wide security information and event management and auditing solutions, providing a comprehensive, end-to-end workbench for RACF security management. To further reduce the administrative load for scarce native-RACF resources, IBM Security zSecure CICS Toolkit—a key component of the zSecure suite designed for easy integration with zSecure Admin—enables mainframe administration tasks to be performed from a CICS environment, while IBM Security zSecure Visual provides a Microsoft Windows graphical user interface ideal for decentralized RACF administration.

For more information

To learn more about IBM Security zSecure Admin, please contact your IBM representative or IBM Business Partner, or visit the following website:
ibm.com/us-en/marketplace/zsecure-admin

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

For more information on IBM security, please visit:
ibm.com/security

IBM Security
New Orchard Rd
Armonk, NY 10504

Produced in the United States of America
September 2017

WGD03086-USEN-01