IBM Security zSecure Visual

Simplify mainframe administration through a user-friendly, Windows-based interface

In today’s rapidly-changing, interconnected environment, organizations are challenged to provide effective protection against a barrage of new, evolving and increasingly sophisticated IT threats. Inadequate IT security can result in unauthorized access to confidential information, theft of intellectual property, impaired system availability and negative publicity. Ultimately, it can cause poor business results and instability across the organization.

RACF plays a vital role in helping protect mainframes from unauthorized entry and misuse by authorized users. However, experienced RACF administrators are often scarce in IT organizations, which can make it difficult to maintain the level of security needed to protect mission-critical resources. These scarce RACF administrators are better off investing their time in risk mitigation and security assurance activities rather than in mundane security administration tasks. Additionally, the complexity and scope of protecting mainframe security resources and analyzing event logs can overwhelm even experienced security personnel.

IBM Security zSecure™ Visual, a key component of the IBM Security zSecure suite, enables efficient and effective RACF administration with a direct, easy-to-use, point-and-click graphical interface that uses fewer resources and provides richer functionality. Because it helps eliminate the need for extensive knowledge of RACF to perform many administrative functions, less-experienced personnel can use zSecure Visual and free up experienced RACF administrators to focus on higher value activities.

---

Highlights

- Enable service desk and help desk staff and line-of-business security administrators to view and manage profiles directly from an easy-to-use Microsoft Windows interface
- Minimize the need for highly specialized IBM® Resource Access Control Facility (RACF®) administration skills and leverage decentralized RACF administration, to lessen the burden on senior IT security staff
- Reduce the security risk of decentralized RACF administrators through scoped administrative rights
Decentralize RACF administration to optimize resources

Through a user-friendly Microsoft Windows interface, organizations can decentralize RACF administration, enabling tasks to be performed at the department level rather than at the corporate level. Reducing the number of administrative tasks performed by the central security group enables them to use their time more effectively. Freed from routine tasks such as password resets, experienced RACF security personnel can instead focus on activities that help improve both security and service levels.

To manage security and privacy, central security personnel can customize the administrative scope and user interface. Consequently, service desk and help desk staff or security administrators view only the profiles and actions they are allowed to administer. For example, a help desk staff member who has the right to reset passwords but no other rights will not be able to initiate commands for creating new users. With zSecure Visual, you can enable these decentralized administrators over your standard network without the cost and effort of rolling out IBM Time Sharing Option/Interactive System Productivity Facility (TSO/ISPF) and 3270 sessions to your staff.

Simplify administration to improve efficiency

zSecure Visual enables help desk staff to access RACF profiles directly from Windows, rather than having to access separate TSO/ISPF screens. With profiles accessed directly from Windows, these routine tasks can be handled easily and efficiently with only minimal training, which can help lower help desk overhead significantly.

IBM Security zSecure Visual enables service desk and help desk staff to access profiles directly from Windows, rather than having to access separate TSO/ISPF screens. This screen shot shows the results of searching system data sets for unnecessarily high universal access.

With easy access to the active, live RACF database, help desk staff can view accurate, up-to-the-minute information about users, groups and resource profiles from one or more databases. They can also easily navigate through RACF profiles and manage permits, scope and access lists. In addition, the interface can display more detailed information, such as when passwords were last changed or reset.

New users can be added to the system simply by duplicating standard user templates and entering the new user names. This feature helps reduce the risk of giving incorrect authorizations to a new user—the department can use only existing templates and assign authorizations to groups within their scope.
Optionally, departmental administrators can flag specific users for removal, so that central IT security personnel can verify and approve the removal of these users from the system. In addition, custom actions to run site-specific scripts can be made available in the user interface.

zSecure Visual enables individual users to format the product’s interface to match their own preferences, including the ability to customize display layouts and set default passwords. It can be an easy migration from homegrown tools by allowing site customization to match and enrich site-specific, user-defined displays with data, such as employee and department numbers from human resources files.

zSecure Visual 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. It allows administrators to send the same command to multiple systems with or without RACF remote sharing facility. Data encryption is used to protect the command communications.

**Empower business users to quickly identify security threats**

The security of IBM z/OS® systems with RACF relies on having products correctly configured, as well as having properly defined profiles and options in RACF. When mistakes are made, any knowledgeable programmer can bypass the access control system. The spreadsheet-like, point-and-click interface in zSecure Visual allows business managers and auditors alike to quickly view vital information about staff and resources in a read-only format, which can help reduce the requirement for ad hoc or periodic distribution of reports.

**View and manage data set and general resource profiles**

zSecure Visual allows you to generate listings of profiles with similar characteristics based on search filters or selection criteria such as resource class or group ID or combinations of these. From the listings, you can view more information on the profiles and also perform administration functions such as access control list (ACL) modification, profile copying and profile deleting. The access list display can show the ACL in two formats:

- Normal—groups and users mixed
- Effective—combining group connections and operational access to show all users that have access to the data set or resource

---

**IBM Security zSecure suite**

A summary shows the products that comprise the IBM Security zSecure suite, including IBM Security zSecure Visual.

*Product offers a subset of the capabilities provided by zSecure Audit*
Why IBM?
One of multiple IT security products in the zSecure suite, zSecure Visual offers a user-friendly mainframe administration solution, ranging from an extended delegated help desk function to a full-fledged group administration solution. The zSecure suite offers a full line of comprehensive audit and administration tools for mainframes. These tools are designed to help mainframe security personnel increase productivity and to measure and verify the effectiveness of their mainframe security and security policies.

For more information

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](http://ibm.com/security)

© Copyright IBM Corporation 2015
IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
November 2015

IBM, the IBM logo, ibm.com, zSecure, RACF, X-Force, and z/OS are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.