

UniKix Secure Software



Highlights:

- Offers authentication and resource-level security – providing similar functionality as IBM® RACF® security
- Leverages a LDAP or RDBMS repository
- Provides administrative and runtime services in a role-based access control model
- Includes audit logging with configurable levels of audit messages
- Enables hierarchical role structures and adaptive groupings
- Provides point-of-entry security if needed

Complete security model for mission-critical applications

Today's world demands stringent security and identification measures to protect valuable enterprise data. Organizations must be able to quickly determine which resources are to be protected, which users need access to them, and with what permissions. With UniKix™ Secure software, a comprehensive Role Based Access Control (RBAC) model can be deployed in conjunction with UniKix™ Transaction Processing Environment (TPE) software to meet the needs of businesses reliant upon high volume and secure operations.

Protecting legacy assets in open, highly-available environments

UniKix TPE software allows security configurations to be tailored to meet a variety of business requirements. Basic validation user-level security is provided through the administration of sign-on table entries, as well as through External Security Management (ESM) systems. Customizable user exits can be used to meet individual access control and audit facilities requirements, however many third-party security packages do not offer the level of granularity required for transaction processing systems.

UniKix Secure software provides a comprehensive RBAC security model for UniKix TPE software, enabling UniKix TPE to deliver security functionality beyond basic sign-on table authentication and transaction-level security. With its inclusive permissions model, multiple user profile choices, and adaptable hierarchical relationship options, UniKix Secure software delivers the detailed security protection businesses require for applications central to daily operations.

Proven security for vital resources

UniKix Secure software is implemented as an External Security Manager (ESM) and operates much like the Resource Access Control Facility (RACF) for IBM® CICS® environments traditionally deployed in mainframe data centers. In fact, UniKix Secure software was developed with mainframe access control methods in mind, smoothing the transition from a legacy environment to open systems.

With UniKix Secure software, administrators can control the resource-level security of all UniKix TPE software resources, including VSAM files, application programs, and transactions. Preset terminal security is also supported to allow terminals such as printers to run triggered transactions using a configured userid for resource permissions.

To prevent undesirable system access, UniKix Secure software uses an inclusive permissions model where all resources must be defined in a security repository and permissions must be granted for any user or role that needs to access them. If a resource is not defined in the security repository, it cannot be accessed by any user or role.

Flexible implementation framework

UniKix Secure software's RBAC security model assigns permissions to resources by using individual users and roles. Users can be assigned one or more roles, granting permission to groups of resources. A role may also be defined as a "parent" role, creating a hierarchy of relationships. Parent roles have their own permissions in addition to the access granted to any "child" or subsidiary role.

UniKix Secure software defines three types of security system users.

- The Super Administrator can create and destroy the security repository, and create the Security Administrator.
- The Security Administrator creates and maintains the Principals, as well as the Roles, Resource Domains, Resources, and associated permissions.
- UniKix Secure users are defined as Principals in the security system, but do not have administrative access to UniKix Secure software. As users attempt to access various resources, those access attempt results are stored in local cache memory to accelerate system access.

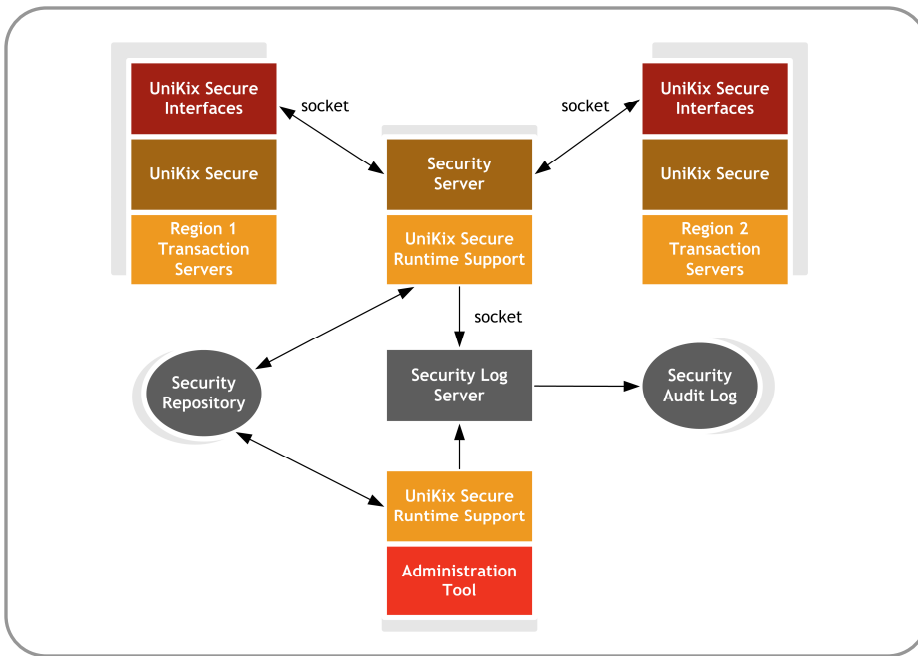
For reporting purposes, UniKix Secure software generates and logs audit messages to record security events. These events are time-stamped and categorized by severity level depending upon significance and remedy action required.

Primary UniKix Secure software components

UniKix Secure software is composed of the following items:

- A Security Repository, implemented as a third-party RDBMS or LDAP, containing the definitions of Principals, Roles, Resources Domains, and Resources
- An Administration Tool Set, used to initialize and maintain the security repository
- A Security Server, which manages interactions for authentication and authorization between UniKix TPE software regions and the security repository
- UniKix Secure software runtime support, a set of services that allows the security server and administration tools to communicate with the security repository
- UniKix Secure software interfaces to the Security Server, used by UniKix TPE region transaction servers to communicate with the Security Server
- A Security Log Server, which collects audit messages generated by UniKix Secure software runtime services, and writes them to a Security Audit Log file

The Transaction Server communicates via TCP/IP sockets with the Security Server to validate access requests. The Security Server verifies or denies access based on the security configuration in the Security Repository.



Access control through UniKix Secure technology provides resource-level security of all UniKix TPE software resources, including VSAM files, application programs, terminals, as well as transactions.

Administration tools are used to create and maintain the security configuration in the Security Repository.

Comprehensive legacy investment and modernization solutions

UniKix Secure software enables comprehensive, secure processing of mainframe applications on open systems. When considering a migration project, both the path to obtain the desired target environment and the destination are equally as important. With UniKix Secure software, mainframe application investments can be safely leveraged on open systems, resulting in a highly manageable and well-supported platform moving forward.

UniKix Secure software is part of a larger suite of migration and modernization offerings from Clerity that look to enhance, extend, and transform legacy assets. Clerity recognizes that companies have significant investments in core applications and procedures and provides a wealth of low risk, high value solutions and technology to reduce IT costs without sacrificing current functionality and service level agreements.

Find more details about these solutions at www.clerity.com.

About Clerity

Clerity is a leading full-service provider of legacy migration, modernization, and optimization solutions. Drawing from over 16 years of experience, Clerity recognizes that companies have significant investments in core applications and procedures and provides a wealth of low risk, high value tools, technology, and services to reduce IT costs without sacrificing current functionality and service level agreements. Headquartered in Chicago, Illinois with offices worldwide, Clerity has customers in all in major countries, including some of the largest financial services ISVs and Fortune-class end users.

Learn how Clerity can provide an evolutionary path forward for your application and data environments at www.clerity.com.



9930 Derby Lane, Suite 202 • Westchester, IL 60154
Phone 1-888-2-REHOST (or 1-630-981-6100)

© 2010 Clerity Solutions, Inc. All rights reserved. Clerity and UniKix are trademarks, or registered trademarks, of Clerity Solutions, Inc. in the United States and other countries.

IBM, CICS, and RACF are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. All other marks are the property of their respective owners.