About InterSystems Authorization

Version 2024.1
2024-05-16

InterSystems Corporation 1 Memorial Drive Cambridge MA 02142 www.intersystems.com

About InterSystems Authorization
InterSystems IRIS Data Platform Version 2024.1 2024-05-16

For Support questions about any InterSystems products, contact:

InterSystems Worldwide Response Center (WRC)
Tel: +1-617-621-0700
Tel: +44 (0) 844 854 2917
Email: support@InterSystems.com

Table of Contents

About InterSystems Authorization

Once a user has authenticated, the next security-related question to answer is what assets that person is allowed to use, view, or alter. Assets include:

- Databases — Physical files containing data or code.
- Services — Tools for connecting to InterSystems IRIS, for example, client-server services, telnet.
- Applications — InterSystems IRIS programs, for example, Web applications.
- Administrative actions — Sets of tasks, for example, starting and stopping InterSystems IRIS or creating backups.

You probably do not want all of the users in your organization to be able to see and modify every asset on your system. The determination and control of access to assets is known as *authorization*.

Authorization manages the relationships of users and assets, which are represented within the InterSystems IRIS® data platform as *resources*. InterSystems IRIS employs *Role-Based Access Control (RBAC)* as its authorization model: a system administrator assigns a user to one or more task-based *roles*; each role is authorized to perform a particular set of activities with a particular set of resources. *Applications* can temporarily expand the roles a user has.

This page provides an overview of the RBAC authorization model implemented within InterSystems IRIS. For an interactive introduction to InterSystems RBAC, try Configuring Role-Based Access.

1 Resources, Permissions, and Privileges

The primary goal of security is the protection of *assets* — information or capabilities in one form or another. With InterSystems IRIS data platform, assets can be databases, services, applications, tools, and even administrative actions.

Each asset is represented in InterSystems IRIS by a *resource*, and a single resource can represent more than one asset.

The system administrator controls access to an asset by assigning *permissions* to a resource. Granting or revoking a permission enables or disables access to an activity which can be performed upon the asset the resource represents. For databases, the permissions are Read and Write; for most other resource types, the relevant permission is Use.

Together, a pairing of a resource and an associated permission is known as a *privilege*. This is often described using the following shorthand: `Resource-Name:Permission`. For example, a privilege granting read and write permissions on the EmployeeInfo database is represented as `%DB_EmployeeInfo:Read,Write` or `%DB_EmployeeInfo:RW`.

See Using Resources to Protect Assets and Privileges and Permissions for more details.

2 Users and Roles

Within the InterSystems role-based access control model, a user gains the ability to manipulate resources as follows:

1. *Resources* are associated with *permissions* to establish *privileges*, as described in the preceding section.
2. A set of *privileges* is assigned to a *role*.
3. *Roles* have members, such as *users*.

A *user* connects to InterSystems IRIS to perform some set of tasks. A *role* describes a set of privileges that a user holds, and thus the tasks that user may perform.

Roles provide an intermediary between users and privileges. Instead of creating as many sets of privileges as there are users, roles allow you to create sets of task-specific privileges. You can grant, alter, or remove the privileges held by a role; this automatically propagates to all the users associated with that role. Instead of managing a separate set of privileges for each and every user, you instead manage a far smaller number of roles.

For example, an application for a hospital might have roles for both a doctor making rounds (**`RoundsDoctor`**) and a doctor in the emergency room (**`ERDoctor`**), where each role would have the appropriate privileges.

An individual user can be a member of more than one role. Using the same example, the medical director for the hospital may require capabilities used by doctors across all departments. This user can be assigned both the **`RoundsDoctor`** and **`ERDoctor`** roles. Alternatively, the system administrator can create a **`MedicalDirector`** role which is itself a member of both these roles, and inherits privileges accordingly.

The native InterSystems implementation of role-based access control is available with every type of authentication mechanism that InterSystems IRIS supports, including LDAP, Kerberos, and OS-based. If you prefer, you can also choose to assign roles using LDAP or delegated authorization. See Roles and User Accounts for more details.

3 Applications

InterSystems security provides a flexible application security model. The ability to use an application is a resource, so you can restrict the use of an application to a particular set of users, or open it to all users. For users who can use an application, the security model supports a role escalation model. This means that while using an application, users can access specific resources that they could not generally access.

See Applications for more information about the multiple types of applications.