



# About InterSystems Authorization

Version 2023.3  
2024-05-16

*About InterSystems Authorization*

InterSystems IRIS Data Platform Version 2023.3 2024-05-16

Copyright © 2024 InterSystems Corporation

All rights reserved.

InterSystems®, HealthShare Care Community®, HealthShare Unified Care Record®, IntegratedML®, InterSystems Caché®, InterSystems Ensemble®, InterSystems HealthShare®, InterSystems IRIS®, and TrakCare are registered trademarks of InterSystems Corporation. HealthShare® CMS Solution Pack™ HealthShare® Health Connect Cloud™, InterSystems IRIS for Health™, InterSystems Supply Chain Orchestrator™, and InterSystems TotalView™ For Asset Management are trademarks of InterSystems Corporation. TrakCare is a registered trademark in Australia and the European Union.

All other brand or product names used herein are trademarks or registered trademarks of their respective companies or organizations.

This document contains trade secret and confidential information which is the property of InterSystems Corporation, One Memorial Drive, Cambridge, MA 02142, or its affiliates, and is furnished for the sole purpose of the operation and maintenance of the products of InterSystems Corporation. No part of this publication is to be used for any other purpose, and this publication is not to be reproduced, copied, disclosed, transmitted, stored in a retrieval system or translated into any human or computer language, in any form, by any means, in whole or in part, without the express prior written consent of InterSystems Corporation.

The copying, use and disposition of this document and the software programs described herein is prohibited except to the limited extent set forth in the standard software license agreement(s) of InterSystems Corporation covering such programs and related documentation. InterSystems Corporation makes no representations and warranties concerning such software programs other than those set forth in such standard software license agreement(s). In addition, the liability of InterSystems Corporation for any losses or damages relating to or arising out of the use of such software programs is limited in the manner set forth in such standard software license agreement(s).

THE FOREGOING IS A GENERAL SUMMARY OF THE RESTRICTIONS AND LIMITATIONS IMPOSED BY INTERSYSTEMS CORPORATION ON THE USE OF, AND LIABILITY ARISING FROM, ITS COMPUTER SOFTWARE. FOR COMPLETE INFORMATION REFERENCE SHOULD BE MADE TO THE STANDARD SOFTWARE LICENSE AGREEMENT(S) OF INTERSYSTEMS CORPORATION, COPIES OF WHICH WILL BE MADE AVAILABLE UPON REQUEST.

InterSystems Corporation disclaims responsibility for errors which may appear in this document, and it reserves the right, in its sole discretion and without notice, to make substitutions and modifications in the products and practices described in this document.

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](mailto:support@InterSystems.com)

# Table of Contents

<b>About InterSystems Authorization</b> .....	<b>1</b>
1 Resources, Permissions, and Privileges .....	1
2 Users and Roles .....	1
3 Applications .....	2



# 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.