



First Look: Role-Based Access Control

Version 2018.1
2018-11-30

First Look: Role-Based Access Control

InterSystems IRIS Data Platform Version 2018.1 2018-11-30

Copyright © 2018 InterSystems Corporation

All rights reserved.



InterSystems, InterSystems Caché, InterSystems Ensemble, InterSystems HealthShare, HealthShare, InterSystems TrakCare, TrakCare, InterSystems DeepSee, and DeepSee are registered trademarks of InterSystems Corporation.



InterSystems IRIS Data Platform, InterSystems IRIS, InterSystems iKnow, Zen, and Caché Server Pages are trademarks of InterSystems Corporation.

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

Table of Contents

| | |
|------------------------------------------------------------------------------|----------|
| First Look: Role-Based Access Control | 1 |
| 1 Role-Based Access Control: Why Is It Important? | 1 |
| 2 Role-Based Access Control: How It Works Within InterSystems IRIS | 1 |
| 2.1 A Brief Conceptual Overview | 1 |
| 2.2 An Example Use Case | 2 |
| 3 Role-Based Access Control: Exploring It | 3 |
| 3.1 Before You Begin | 4 |
| 3.2 Logging In and Out of the Management Portal | 4 |
| 3.3 Discovering the Resources Needed For Management Portal Page Access | 4 |
| 3.4 Creating and Assigning Your Own Manager Roles | 5 |
| 3.5 Creating Users and Assigning the New Roles | 6 |
| 3.6 Trying Out the Roles in Management Portal | 7 |
| 4 Learn More About Role-Based Access Control | 8 |

First Look: Role-Based Access Control

1 Role-Based Access Control: Why Is It Important?

When you first start working with a new database platform, one thing will likely become clear quickly: you probably do not want all of your organization's users to be able to see and change everything on the system.

InterSystems IRIS™, like all database platforms, allows you to specify carefully the actions that each user of InterSystems IRIS can perform. The mechanism we use to control user *authorization* to perform actions is called *role-based access control*.

If you're already familiar with role-based access control, the InterSystems IRIS scheme will likely resemble some of those you've worked with before. You'll find more detail about how we handle it in the next section.

If you're new to role-based access control, what this means is time savings over older access control methods that don't provide for grouping of permissions to perform system actions.

- Without role-based access control, assigning each user a permission to work with each aspect of InterSystems IRIS, one by one, could take hours or even days. Then, if a new employee needs access, you would have to repeat the process.
- Role-based access control allows you to group permissions into roles when you initially configure InterSystems IRIS. Then you can assign one or more of those ready-made roles to each of your system's users. A set of predefined roles is also available to you for use or modification.
- Further, with role-based access control, if a user needs to take on a new set of permissions, that set can be grouped into a role and that role assigned to the user. And you can always change the list of permissions within roles.

2 Role-Based Access Control: How It Works Within InterSystems IRIS

InterSystems IRIS provides a full solution for role-based access control, which we'll describe in this section. Native InterSystems role-based access control is available with every type of authentication mechanism that InterSystems IRIS supports, including LDAP, Kerberos, and OS-based. You can use LDAP instead of InterSystems IRIS for role assignment if you wish.

2.1 A Brief Conceptual Overview

Think of the information and capabilities within InterSystems IRIS as *assets* you want to protect, just as you insure assets that belong to you.

Among the items that are considered assets in InterSystems IRIS are:

- Databases, which store data and code as objects.
- Services, which control users' ability to connect to InterSystems IRIS.
- Certain administrative privileges.

- InterSystems IRIS applications, including individual pages in the *Management Portal*, which is the system administration user interface for InterSystems IRIS.

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

The resource acts as a gatekeeper for the assets it represents: it is paired with “read”, “write” (which includes read), and, in some cases, “use” (execute) *permissions* depending on the resource type. For example, only two types of permissions exist for databases: read, which allows viewing of data and execution of routines, and write, which allows modification of data.

A pairing of a resource with a permission is called a *privilege*, and privileges are grouped into *roles*.

Finally, roles are assigned to *users* within InterSystems IRIS. Each user has one or more roles assigned to them when they first authenticate with InterSystems IRIS. It’s possible to add or remove roles from a user for the duration of a session.

The exact manner in which authorization with role-based access control takes place depends on the authentication mechanism you’ve chosen. This aspect of authorization is covered fully in the online documentation.

Tip: For internal test and staging systems, you may not want to bother setting up password-based authentication or different levels of role-based access control. This option is available to you if you install your instance with “minimal” security, which by default gives full administrative privileges to anyone with the Management Portal URL for the instance.

2.2 An Example Use Case

As mentioned above, individual pages in the Management Portal are assets in InterSystems IRIS that you can protect. The Management Portal allows users to view and perform operations on fundamental aspects of InterSystems IRIS, such as globals, namespaces, and even resources and roles themselves.

The screenshot below shows what the Management Portal looks and acts like when the instance’s administrator logs in with the **_SYSTEM** user account created during installation. The **_SYSTEM** user can access **System Administration > Security > Users**, which lets them view and modify any user and their roles.

You may want to restrict the role assignments of certain Management Portal users so that they can’t view or modify user accounts or any other information that is critical to security. In the next section, we’ll show you how to do that.


Menu
Home | About | Help | Logout


Welcome, **_SYSTEM**


Server: **ServerName**
Namespace: **%SYS Switch**


User: **_SYSTEM**
Licensed to: **Development**
Instance: **IRIS**


View: ☐ ☐ ☐


 Home

 Analytics

 Interoperability

 System Operation

 System Explorer

 System Administration

| | |
|-------------------|-----------------------------------|
| Configuration » | Users |
| Security » | Roles |
| Licensing » | Resources |
| Encryption » | Services |
| | Applications » |
| | SSL/TLS Configurations |
| | X.509 Credentials |
| | OAuth 2.0 » |
| | Managed File Transfer Connections |
| | System Security » |
| | Auditing » |
| | Security Advisor |
| | Mobile Phone |
| | Public Key Infrastructure |

3 Role-Based Access Control: Exploring It

The example below shows you how to set up two types of “manager” roles for use in the Management Portal. The first role will have access to pages that allow modification of security-related items such as user and role definitions. The second role will not have that access.

Then you’ll see how users with those roles interact with the Management Portal.

Important: To give you a taste of InterSystems IRIS without bogging you down in details, we’ve kept this exploration simple. For example, we’ve had you use as many default settings as possible.

When you bring InterSystems IRIS to your production systems, though, there are many things you will need to do differently, especially in regard to (but not limited to) security.

So be sure not to confuse this exploration of InterSystems IRIS with the real thing! The sources provided at the end of this document will give you a good idea of what’s involved in using InterSystems IRIS in production.

3.1 Before You Begin

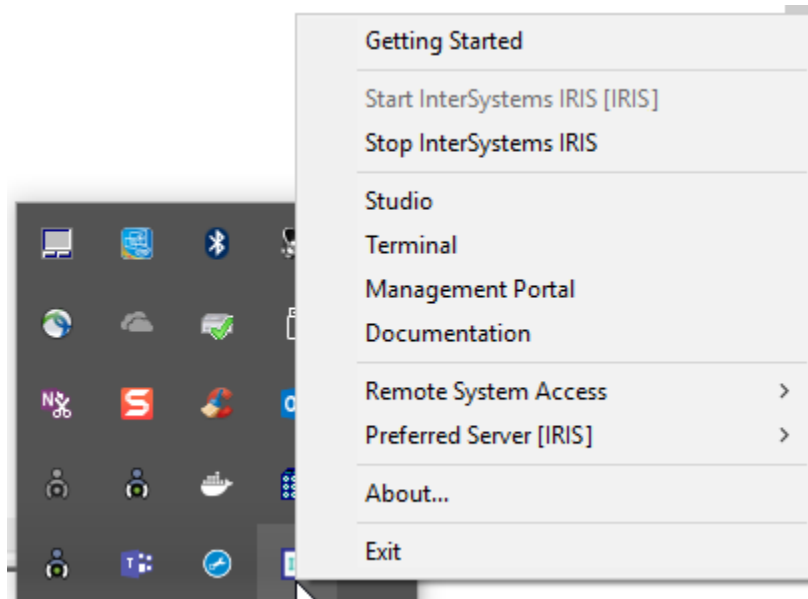
To complete the steps in this section, you will need to install and activate a license for an instance of InterSystems IRIS. When you install InterSystems IRIS, make sure to choose “Normal” security. To get a development instance of InterSystems IRIS up and running quickly, see “[Quick Start: InterSystems IRIS Installation](#)”.

You can install InterSystems IRIS on any supported operating system and use any supported browser to make and view the changes in the Management Portal.

3.2 Logging In and Out of the Management Portal

To log into the Management Portal:

1. Locate the home page for the Management Portal:
 - If you installed InterSystems IRIS on Windows using the graphical installer: From the Task Bar, open the system icon tray and right-click the InterSystems IRIS icon. Then click the menu item for Management Portal.



- If you installed InterSystems IRIS via the command line: use the URL for the Management Portal that was provided by the installation script.
2. Log in with the **_SYSTEM** user name and the password you supplied for the system accounts at installation time.

To log out of the Management Portal, use the **Logout** link at the top left.


3.3 Discovering the Resources Needed For Management Portal Page Access

Access to each page in the Management Portal is protected by at least one resource. You can discover the needed resources as follows:

1. Navigate to **System Administration** > **Security** by clicking each of those words in their corresponding menu items.

Tip: In the Management Portal, menu items with child pages include a >> next to the name of the item. Pages have no such marker.

- In the **Users** menu item, click anywhere to the right of the word “Users”. This action displays the needed resource to view the **Users** page, which is `%Admin_Secure`. (All pages within the **Security** and **Encryption** submenus require use permissions (“U”) on the `%Admin_Secure` resource.)

| | | |
|-------------------|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuration » | Users | <p>Users</p>  <p>View, add, or edit user definitions.</p> <p>Go</p> <p>Add to favorites</p> <hr/> <p>System Resource(s) <code>%Admin_Secure</code></p> <p>Custom Resource -</p> <p>Assign</p> |
| Security » | Roles | |
| Licensing » | Resources | |
| Encryption » | Services | |
| | Applications » | |
| | SSL/TLS Configurations | |
| | X.509 Credentials | |
| | OAuth 2.0 » | |
| | Managed File Transfer Connections | |
| | System Security » | |
| | Auditing » | |
| | Security Advisor | |

- Navigate to **System Administration > Configuration > System Configuration**.
- Click anywhere to the right of the words “Memory and Startup.” You’ll see that the needed resource to view the page is `%Admin_Manage`.

3.4 Creating and Assigning Your Own Manager Roles

For pages within the **System Administration** menu of the Management Portal, you need roles with privileges to the `%Admin_Secure` and `%Admin_Manage` resources.

Given this structure, it’s plausible that you’d want to create roles that reflect two levels of management, one that can access all pages except for security-related pages, and the other that can perform all actions, including security-related actions. There is a predefined `%Manager` role that you can use as a template.

- Log into the Management Portal with the `_SYSTEM` account.
- Navigate to **System Administration > Security > Roles** and click **Go**. You’ll see a list of roles with which InterSystems IRIS was installed, including a `%Manager` role.
- Click the `%Manager` link. The **General** tab displays the privileges (resources paired with permissions) available to users with this role.
 - Among the privileges, you will see use permissions on `%Admin_Secure` and `%Admin_Manage`.
 - You’ll see many other privileges as well. This is because you need access to many different resources to be able to view and modify InterSystems IRIS settings. Since we know that there is only one critical resource, `%Admin_Secure`, in terms of access for security-related pages within **System Administration**, access to that resource will be the only difference between our two custom roles.
- Click **Cancel** (beneath **Edit %Manager**) to return to the main **Roles** page.

3.4.1 Creating a “Standard Manager” Role

1. On the **Roles** page, click **Create New Role**. A role definition page will appear.
2. In the **Name** field, enter “**Standard_Mgr**”.
3. In the **Copy from** dropdown, select **%Manager**. This will copy all information, including privileges, from the predefined **%Manager** role to the new one.
4. Change the description to one of your choice, such as “**Role for System Administration without security access**”.
5. Click **Save**. A **Role saved** message will appear and you’ll see the list of privileges for the new role in the **General** tab.
6. In the row for **%Admin_Secure**, click **Delete**. This removes the privilege from the role.
7. Click **Save** again to save changes.

3.4.2 Creating a “Security Manager” Role


1. On the **Roles** page, click **Create New Role**. A role definition page will appear.
2. In the **Name** field, enter “**Security_Mgr**”.
3. In the **Copy from** dropdown, select **%Manager**. This will copy all information, including privileges, from the predefined **%Manager** role to the new one.
4. Change the description to one of your choice, such as “**Role for System Administration with security access**”.
5. Click **Save**. A **Role saved** message will appear and you’ll see the list of privileges for the new role in the **General** tab.

3.5 Creating Users and Assigning the New Roles

To see the roles in action, you’ll need to create two users, one for each of your new roles.

1. Log into the Management Portal with the **_SYSTEM** account.
2. Navigate to **System Administration > Security > Users** and click **Go**. You’ll see a list of user definitions with which InterSystems IRIS was installed.

3.5.1 Creating a “Standard Manager” User

1. On the main **Users** page, click **Create New User**. A user definition page will appear.
2. In the **Name** field, enter “**Std_Mgr**”. (The name of the user cannot match the name of the role.)
3. In the **Password** and **Password (confirm)** fields, enter a password of your choice.
4. Click **Save**. A **User saved** message will appear.
5. Click the **Roles** tab. Scroll through the **Available** list on the left and highlight **Standard_Mgr**.
6. Click the right-pointing arrow  to add the role to the **Selected** list. Then click **Assign**.
7. Click **Cancel** to return to the main **Users** page.

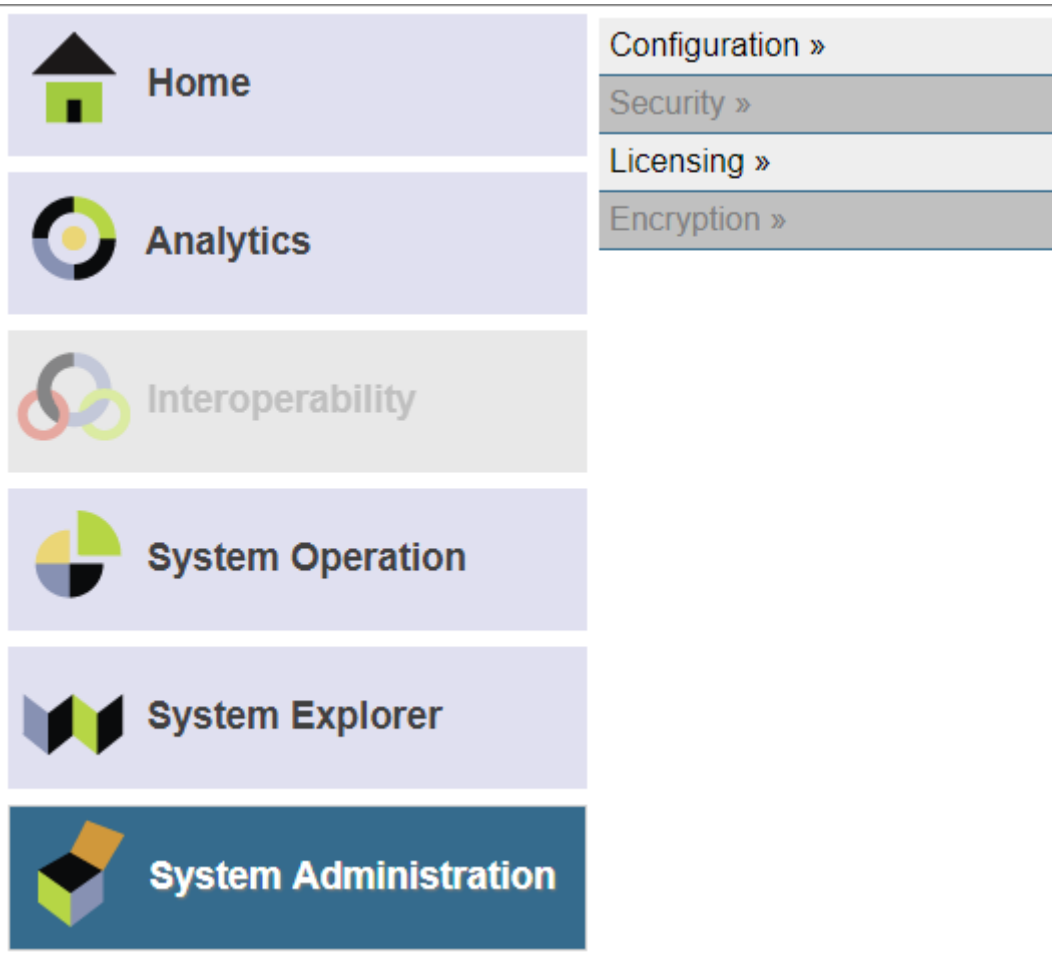
3.5.2 Creating a “Security Manager” User

1. On the main **Users** page, click **Create New User**. A user definition page will appear.

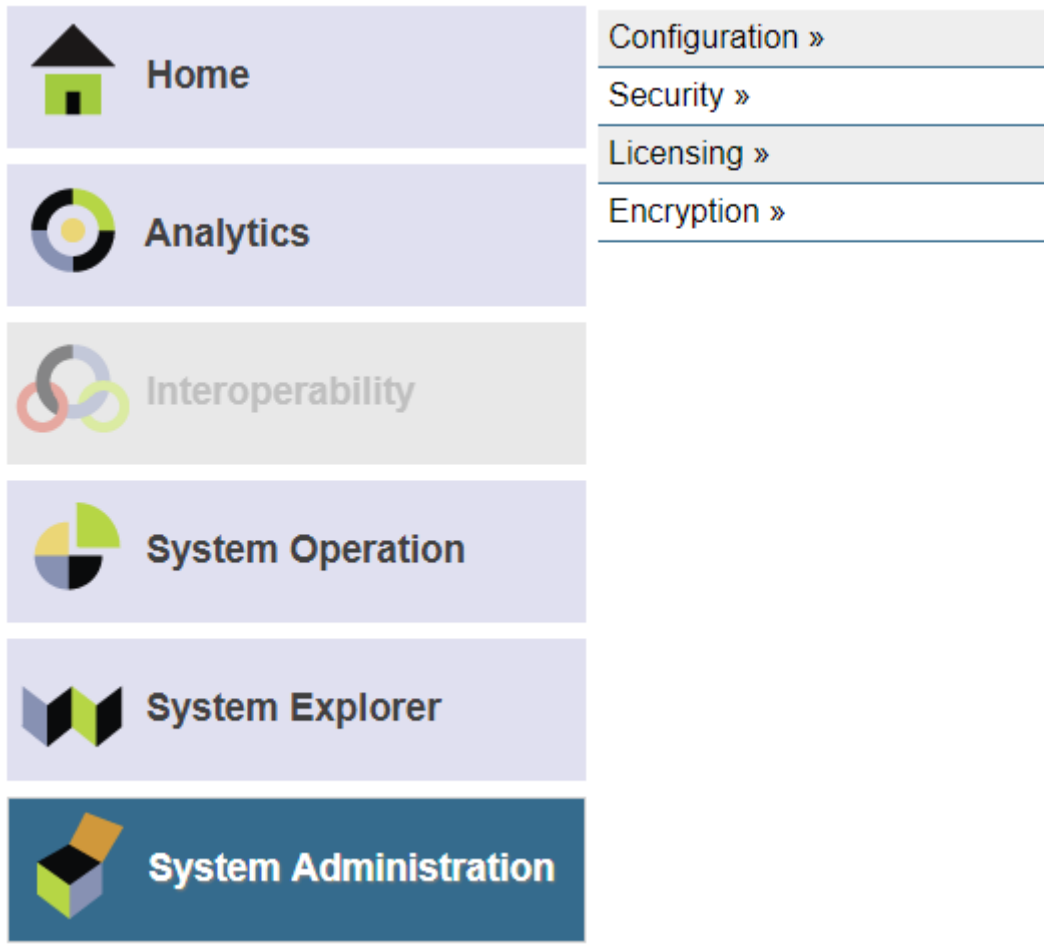
2. In the **Name** field, enter “**Sec_Mgr**”.
3. In the **Password** and **Password (confirm)** fields, enter a password of your choice.
4. Click **Save**. A **User saved** message will appear.
5. Click the **Roles** tab. Scroll through the **Available** list on the left and highlight **Security_Mgr**.
6. Click the right-pointing arrow to add the role to the **Selected** list. Then click **Assign**.
7. Click **Cancel** to return to the main **Users** page.

3.6 Trying Out the Roles in Management Portal

1. Log into the Management Portal as the **std_Mgr** user. You’ll see that security-related menu options are grayed out, as expected. The **Interoperability** menu option is also grayed out because the predefined **%Manager** role from which the two custom roles were copied does not have the privileges necessary for those pages.



2. Log out, and log back in as the **Sec_Mgr** user. This user, as you’ll see, has full access to the pages in the **System Administration > Security** and **System Administration > Encryption** submenus.



4 Learn More About Role-Based Access Control

To learn more about role-based access control and the InterSystems IRIS security model, see:

- “[Authorization: Controlling User Access](#)” section of the *InterSystems IRIS Security Administration Guide*
- “[InterSystems IRIS Security](#)” and “[Namespaces and Databases](#)” sections of the *InterSystems IRIS Programming Orientation Guide* — provides information about role-based access control for application developers.
- “Authorization” section of the *Security Tutorial* — step by step instructions for creating users, roles, and privileges.