



Securing Your Instance

Version 2024.1
2024-05-16

Securing Your Instance

InterSystems IRIS Data Platform Version 2024.1 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

Table of Contents

Securing Your Instance	1
1 Security Strategy	1

Securing Your Instance

1 Security Strategy

The best time to start planning for securing your InterSystems IRIS® instance occurs before you perform the initial installation. The section [Prepare for InterSystems Security](#) describes some issues you should consider prior to installing InterSystems IRIS® instance. In general, for production systems, InterSystems recommends that you start with the highest possible level of security and then grant privileges only as required. A good place to start is by performing an installation with the initial security setting of Locked Down and then fine tuning from there.

Once you have installed InterSystems IRIS, or if you have already installed your instance, see [Tighten Security for an Instance](#) for guidance on ways you can restrict access to the instance and reduce the surface of attack. If you have performed the installation using the Locked Down initial security setting, some of the steps outlined here have already been done for you. However, you should still review its contents to learn additional steps you can take to tighten your instance.

The InterSystems IRIS Management Portal includes the [Security Advisor](#), which provides a list of areas that should be examined for your instance to see if they should be tightened further. For each such area, the Security Advisor provides a handy link to the appropriate page in the Management Portal so that the related setting can be adjusted, if needed.

Of course, running a secure system requires the hardening of attack surfaces apart from the InterSystems IRIS executable. InterSystems IRIS also uses other processes and resources that could be targets for malicious behavior. The section [Secure InterSystems Processes and Operating-System Resources](#) discusses these topics and provides guidelines for you to follow.

Lastly, the [Checklist for Hardening Your Deployment](#) is divided into a number of broader security categories, such as network, operating system, or web server, and provides a checklist for each category that your organization can use to harden your deployment as a whole.

