Securing Your Instance

Version 2024.1
2024-07-02

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

Securing Your Instance
InterSystems IRIS Data Platform Version 2024.1 2024-07-02

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 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.