Command-Line Security Management Utilities

Version 2023.1
2024-04-15

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

Command-Line Security Management Utilities
InterSystems IRIS Data Platform Version 2023.1 2024-04-15
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

Command-Line Security Management Utilities **1**
1 About the Command-Line Utilities 1
1.1 General Notes on Prompts 1
2 ^SECURITY 2
3 ^EncryptionKey 4
4 ^DATABASE 4
5 ^%AUDIT 6

Command-Line Security Management Utilities

1 About the Command-Line Utilities

The InterSystems IRIS® Management Portal provides a browser-based interface for controlling an instance. InterSystems IRIS also has several command-line utilities that allow you to perform management activities in the Terminal. These utilities including:

- ^SECURITY — addresses the setup and maintenance of the data essential to the proper functioning of InterSystems security.
- ^EncryptionKey — supports operations for encryption key management, database encryption, and data-element encryption.
- ^DATABASE — is used to manage databases; it also allows you to set values related to InterSystems security.
- ^%AUDIT — allows the reporting of data from the logs, and the manipulation of entries in the audit logs as well as the logs themselves.

Each of the utilities is described in its own section along with its top-level functionality. In most cases, the initial menu choice leads to further requests for information until the utility has sufficient information to accomplish its task. To use any utility from the Terminal, you must be in the %SYS namespace and have at least the **%Manager** role. For example, to invoke the ^SECURITY utility, use the command:

ObjectScript

```
Do ^SECURITY
```

When the utility runs, it presents you with a list of options. Select an option by entering its number after the `Option?` prompt.

Important: It is possible to run multiple simultaneous instances of a single utility. This can result in conflicts that require resolution.

1.1 General Notes on Prompts

The following are characteristics of prompts when using the character-based utilities:

- Each option has a numeric prefix. Select an option by typing its number.
- Each option list has an item to exit the menu and return to the previous level. You may also reply to the `Option?` prompt with **Enter**. This is interpreted as if you had chosen the `Exit` option.
- For prompts that have a default value, you can choose the default by pressing **Enter**. When there is a default value, it appears after the prompt and followed by the characters `=>` as in

  ```
  Unsuccessful login attempts before locking user? 5 =>
  ```

  where the default value for this option is 5.

- Prompts with defaults of `Yes` or `No` also accept any matching partial response such as "yE" or "n"; the match is not case sensitive.
- For prompts to alter settings, the setting's current value is the default. Press **Enter** to retain that value.
- Some prompts can accept input that performs pattern matching. Typically, an asterisk (*) matches all items. Prompts may also accept comma-separated lists.

2 ^SECURITY

This utility addresses the setup and maintenance of the data essential to the proper functioning of InterSystems security.

Note: Effective with InterSystems IRIS 2021.2, exported and imported security information is versioned. In 2021.2 and all subsequent versions, you can import settings from the same or earlier version. For example, in version 2022.1 you can import settings from 2022.1 (the same version) and 2021.2 (an arbitrary earlier version). Any needed conversions occur automatically on import.

1. User setup

   Users represent actual people or other entities who are permitted access to the system. You can create, edit, delete, list, export, and import users.

2. Role setup

   InterSystems IRIS users have the ability to perform actions based on their roles. You can create, edit, delete, list, export, and import roles.

3. Service setup

   Services control predefined technologies that support connections to InterSystems IRIS. You can edit, list, export, and import services.

4. Resource setup

   Resources represent assets that require security management; a resource may represent a single asset such as a database, or it may protect multiple (usually related) assets such as a suite of applications. You can create, edit, delete, list, export, and import resources.

5. Application setup

   Application definitions represent applications, and there are several types. In each submenu, you can edit, list, export, and import each application type.

   Note: Because client applications are only available on Windows, the options associated client applications do not appear on other operating systems.

6. Auditing setup

   Auditing allows InterSystems IRIS to track security-related events. You can enable and disable auditing, view the audit database, configure audit events, and manage the audit log.

7. **Note:** This option is available in legacy products, but not in InterSystems IRIS.

8. SSL configuration setup

   TLS, the successor to SSL, provides authentication and other functionality, including for use with mirroring. You can create, edit, delete, list, test, export, and import TLS configurations.

9. Mobile phone service provider setup

   To support two-factor authentication, users must register their mobile phone and service provider. You can create, edit, delete, and list mobile phone service providers.

10. OpenAM Identity Services setup

    OpenAM identity services allow InterSystems IRIS to support single-sign on (SSO). If users have already successfully authenticated, OpenAM eliminates the need to re-authenticate. Using this option, you can use the %SYS.OpenAM.IdentityServices class API to authenticate against a specified OpenAM server. You can create, edit, delete, and list OpenAM identity services.

    Note: To use OpenAM via a web policy agent, you must install and configure the web policy agent on the web server that you are using with InterSystems IRIS.

    When a user connects, the web policy agent redirects that user to the OpenAM server. The OpenAM server authenticates and directs the user to the system to which they are connecting; it also provides them with an OpenAM token in a cookie. The web policy agent recognizes the token, validates it with the OpenAM server, sets the value of the *REMOTE_USER* variable to their username, and connects to the web server. The web application can then set *$USERNAME* to the value of *REMOTE_USER*, such as through delegated authentication. Subsequent connections to any supported service validate the token, so the original authentication is persistent.

    In order to do this, you must install and configure a Web Policy Agent on the server that you are using with InterSystems IRIS.

11. Encryption key setup

    InterSystems IRIS uses keys to encrypt databases or user-specified data elements. You can create and manage keys in files, activate and deactivate keys, list keys, specify default keys, configure encryption startup options, and modify the encryption status of a database.

12. System parameter setup

    The system parameters specify system-wide security values. You can:

    - Edit system options (manage configuration security, specify the use of multiple domains, manage the default domain, manage inactive account and login limits, manage password expiration duration, manage password requirements, specify a password validation routine, manage writing to percent (%) globals, specify a required role for the system, specify the required or permitted TLS server authentication mode, and specify the default signature hash)
    - Display system options
    - Enable and disable authentication options.
    - Create, edit, delete, list, export, and import LDAP configurations.
    - Export and import all security settings, including those for SQL privileges. (See note above about exporting and importing security information.)

    Note also:

    - If you are importing security settings from a source instance configured with multiple domains to a target instance not configured to allow multiple domains *and* the source instance's default domain differs from that of the target instance, then the import does not update the target's default domain — you must explicitly set this value. To do this, use the **Default security domain** drop-down on the **System-wide Security Parameters** page (**System Administration** > **Security** > **System Security** > **System-wide Security Parameters**).
    - When importing *all* security settings, the import/export file includes web application settings; each web application has a *Path* setting. Before importing settings onto a new drive, VM, or hardware, for each web application, ensure

that the value of the *Path* setting is accurate for that environment. If the web applications associated with the Management Portal do not have correct *Path* values, the Management Portal will not display correctly.

To locate the *Path* setting for each web application in the import/export file (SecurityExport.xml), look in the *ApplicationsExport* section; in each *Applications* section, identify the application by the value of the *Name* setting; then update the value of the *Path* setting as appropriate.

13. X509 User setup

    X.509 is the standard for certificates that a public key infrastructure (PKI) uses. InterSystems IRIS uses X.509 certificates for its PKI, and each user associated with an X.509 certificate is known as an X.509 user. You can create, edit, delete, list, export, and import them.

14. KMIP server setup

    A KMIP server is a key management server that communicates using the key management interoperability protocol (KMIP). You can create, edit, delete, list, test, export, and import KMIP server configurations.

15. Exit

3 ^EncryptionKey

The **^EncryptionKey** utility is for use with managed key encryption; it supports operations for encryption key management (technology for creation and management of encryption keys and key files), database encryption, and data-element encryption.

1. Create new encryption key and key file

   Allows you to create a new database-encryption key, which it stores in a key file.

2. Manage existing encryption key file

   Allows you to list administrators associated with a key file, add an administrator to a key file, remove an administrator from a key file, and convert a version 1.0 key file to a version 2.0 key file.

3. Database encryption

   Allows you to perform encryption management operations, activate a database encryption key, display the unique identifier for a currently activated database encryption key (if there is one), deactivate the activated database encryption key, and configure InterSystems IRIS startup options related to database encryption. Encryption management operations are for converting an unencrypted database to be encrypted, converting an encrypted database to be unencrypted, and converting an encrypted database to use a new key; for more information, see "Modify Database Encryption Using ^EncryptionKey."

4. Data element encryption for applications

   Allows you to activate a data-element encryption key, list the unique identifier for any currently activated data-element encryption keys (if there are any), and deactivate the activated data-element encryption key.

4 ^DATABASE

The **^DATABASE** utility is used to manage databases; it also allows you to set values related to InterSystems security.

1. Create a database

Allows you to create a new database.

2. Edit a database

   Allows you to change the characteristics of an existing database, for example, by adding additional volumes.

3. List databases

   Displays the characteristics of one or more databases.

4. Delete a database

   Allows you to delete an InterSystems IRIS database. This action is irreversible.

5. Mount a database

   Makes a database ready for use by InterSystems IRIS. Databases must be mounted to InterSystems IRIS in order to be usable. Databases can be set to be automatically mounted at startup.

   Note: You can use the **Mount a database** option to mount any IRIS.DAT file accessible to the instance by specifying the directory containing it. However, if you do this with a database that was deleted from, or was never added to, the Management Portal database configuration (see Configuring Databases in the "Configuring InterSystems IRIS" chapter of the *System Administration Guide*), the database is not added to the Management Portal configuration and is therefore unavailable for portal database operations and for some utilities, for example **^Integrity** (see Checking Database Integrity Using the ^Integrity Utility in the "Introduction to Data Integrity" chapter of the *Data Integrity Guide*).

6. Dismount a database

   Permits you to quiesce a database and remove it from use by InterSystems IRIS.

7. Compact globals in a database

   Reorganizes the data inside *IRIS.DAT*. Note that this option does not reduce the size of the database file; to reduce the size of the database, see option 13.

8. Show free space for a database

   Displays the available space for a database. This is calculated as the difference between its current contents and its current declared size.

9. Show details for a database

   Displays detailed information on a specified database including location, size, status, and other controlling parameters.

10. Recreate a database

    Creates a new, empty database based on the parameters of an existing database. You can specify the size of the new database, where the size of the original database is the default.

11. Manage database encryption

    Removes all the logical data from a database while preserving the properties of the database for reuse.

12. Return unused space for a database

    Frees either a specified amount of or all available extra space associated with a database, reducing it from its current size to its smallest possible size.

13. Compact free space in a database

    Specifies the desired amount of free space (unused space) that is in a database after the end of the database's data. You can also eliminate this free space using the Return unused space for a database option (#12).

14. Defragment a database

Defragments a database, which organizes its data more efficiently. Defragmentation may leave free space in a database (see options #12 and #13).

15. Show background database tasks

    Displays a list of background tasks that are running or that have run since startup. You can also use this option to re-enter the monitor screen, where you can cancel a currently running task as well as purge the history of completed tasks. (Note that the tasks listed here are not the same as those listed as scheduled tasks in the Task Manager.)

5 ^%AUDIT

This utility allows the reporting of data from the logs, and the manipulation of entries in the audit logs as well as the logs themselves.

1. Audit reports

   Permits you to specify selection criteria (date ranges, events, affected users, and so on) and display characteristics, then extracts the data from the audit log and formats it for presentation.

2. Manage audit logs

   Allows the extraction of log entries to another namespace, the export and import of audit log data to and from external files, and maintenance activities against the audit log itself.

3. Exit