Introducing InterSystems Security

Version 2023.1
2024-07-11

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

Introducing InterSystems Security
InterSystems IRIS Data Platform Version 2023.1 2024-07-11

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

Introducing InterSystems Security **1**

1 Authentication: Establishing Identity 2
2 Authorization: Controlling User Access 2
3 LDAP: A Pervasive Authentication and Authorization Tool 3
4 TLS: Industry-Standard Protection for Data in Transit 3
5 SQL Security: Protecting Relational Access 4
6 Encryption: Protecting Data at Rest 4
7 System Security: Hardening an Instance 4
8 Auditing: Knowing What Happened 4
9 Public Key Infrastructure (PKI): Using with Certificates and Private Keys 5

List of Figures

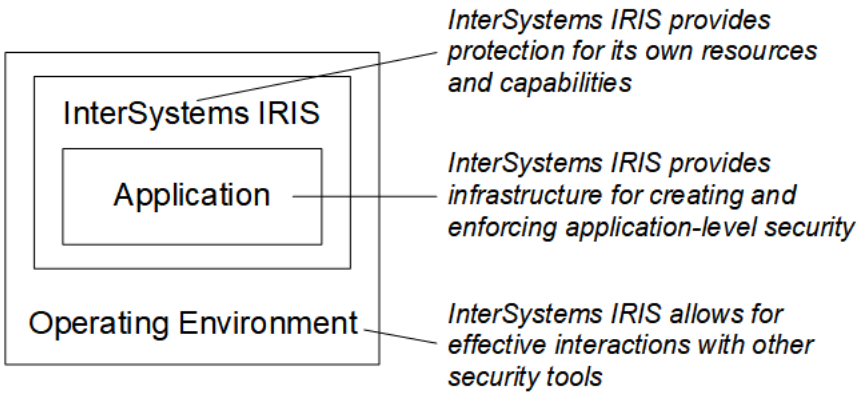
Figure 1: InterSystems Security and Different Levels of the Computing Environment 1
Figure 2: InterSystems IRIS Auditing System 5

Introducing InterSystems Security

InterSystems IRIS® data platform provides a simple, unified security architecture with the following features:

- It provides a security infrastructure that makes it easy for developers to build strong, high-performance security features into applications.
- It places a minimal burden on performance and operations.
- It ensures that InterSystems IRIS can operate effectively as part of a secure environment and that other applications and InterSystems IRIS can seamlessly work together.
- It provides infrastructure for policy management and enforcement.

Figure 1: InterSystems Security and Different Levels of the Computing Environment



InterSystems security has a number of major features and supports popular technologies:

- Authentication verifies the identity of all users.
- Authorization ensures that users can access the resources that they need, and no others.
- LDAP (the Lightweight Directory Access Protocol) is a popular tool that supports both authentication and authorization.
- TLS (the Transport Layer Security protocol) creates protected channels for communications and data transmission.
- SQL security controls access when working with data as relational tables.
- Encryption protects stored data from unauthorized access.
- System security provides tools to protect and harden instance-level security.
- Auditing keeps a log of predefined system and application-specific events.
- PKI (the public-key infrastructure) manages keys and certificates for use in secure communications.

You can use InterSystems IRIS along with other security products and tools (such as firewalls and the security features of operating systems) as part of a comprehensive solution to secure your computing environment. This is why the security features in InterSystems IRIS are designed to successfully interoperate with those of other products.

InterSystems also recommends that you establish clear, effective, and properly enforced security policies. With technology, policy, and enforcement, you can create a secure and productive environment.

1 Authentication: Establishing Identity

Authentication is how InterSystems IRIS verifies the identity of each user. Trustworthy authentication is the basis for all security, because authorization and all other features depend on it.

InterSystems IRIS has a number of available authentication mechanisms:

- Kerberos — The most secure means of authentication. The Kerberos Authentication System provides mathematically proven strong authentication over a network.
- Operating-system–based — OS-based authentication uses the operating system's identity for each user to identify that user for InterSystems IRIS purposes.
- LDAP — With the Lightweight Directory Access Protocol (LDAP), InterSystems IRIS authenticates the user based on information in a central repository, known as the LDAP server.
- Instance authentication — With Instance authentication, InterSystems IRIS prompts the user for a password and compares a hash of the provided password against a value it has stored.
- Delegated authentication — Delegated authentication provides a means for creating customized authentication mechanisms. The application developer entirely controls the content of delegated authentication code.

InterSystems IRIS also supports two forms of two-factor authentication:

- Sending a security code to the end-user's phone.
- Using an application on the end-user's phone to create a time-based one-time password (TOTP).

For situations with strongly protected perimeters or in which neither the application nor its data are an attractive target for attackers, you can configure InterSystems IRIS to accept user connections without authentication.

2 Authorization: Controlling User Access

Once a user is authenticated, the next security-related question to answer is what that person is allowed to use, view, or alter. This determination and control of access is known as authorization. Authorization manages the relationships of users with resources, which are the entities being protected. Resources are as diverse as databases, InterSystems services (such as for controlling web access), and user-created applications.

With InterSystems IRIS authorization:

- Each user has one or more roles.
- Each role provides one or more privileges, each of which is permission to perform a particular activity with a particular resource.
- There are tools to manage users, roles, and other security entities.

InterSystems IRIS supports both internal and external tools that allow you to assign roles to users. InterSystems IRIS then uses these assignments to determine each user's authorized activities. These tools are known as *role-assignment mechanisms*. The role-assignment mechanisms are:

- InterSystems authorization — Role assignment occurs within InterSystems IRIS. Available for use with the Kerberos, OS-based, and Instance authentication mechanisms.
- LDAP — An LDAP (Lightweight Directory Access Protocol) server performs role assignment. Available for use with the OS-based and LDAP authentication mechanisms.

- Delegated authorization — Role assignment occurs in user-supplied code that exclusively handles authorization activities. Available for use with the Kerberos and OS-based authentication mechanisms.
- Delegated authentication — Role assignment occurs as part of user-supplied code also handles authentication activities. Available for use within the delegated authentication mechanism only.

For all role-assignment mechanisms, role *management* — that is, associating particular privileges with particular roles — occurs within InterSystems IRIS.

3 LDAP: A Pervasive Authentication and Authorization Tool

LDAP, the Lightweight Directory Access Protocol, is a prevalent, industry-standard protocol that supports authentication and authorization activities. On Windows, it is implemented as Active Directory.

An LDAP server is a central repository of user information, from which InterSystems IRIS retrieves authentication and authorization information:

- With LDAP authentication, InterSystems IRIS prompts the user for a username and password. The instance is associated with an LDAP server, which performs authentication and optionally retrieves the user's roles and other authorization information. The instance can also be configured to use cached credentials to authenticate users, in cases where it cannot connect to the LDAP server. LDAP authentication can also use delegated authorization.
- With LDAP authorization, InterSystems IRIS uses LDAP groups to assign roles to users. Users can then perform actions based on the privileges of those roles. LDAP authorization is also available for use with OS-based authentication for logins from the local InterSystems IRIS terminal and delegated authentication.

Supported LDAP features include:

- Active Directory for Windows domain controllers.
- OpenLDAP.
- LDAP version 3 protocols.
- Multiple LDAP domains.

4 TLS: Industry-Standard Protection for Data in Transit

TLS, the Transport Layer Security protocol, provides strong protection for communication between pairs of entities. It supports authentication, data integrity protection, and data encryption. It is the successor to and supersedes SSL, the secure sockets layer.

InterSystems IRIS supports TLS to secure connections:

- From client applications that interact with the InterSystems IRIS superserver.
- From Telnet clients that interact with the InterSystems IRIS Telnet server.
- Over TCP where InterSystems IRIS is the client, server, or at both ends.
- That use the Enterprise Cache Protocol (ECP).

5 SQL Security: Protecting Relational Access

InterSystems IRIS provides a set of SQL security tools that seamlessly integrate with its security infrastructure, including its authentication and authorization tools. These tools allow you to ensure the security of relational table data and for users to access required data appropriately and simply. They include:

- Granting, checking, and revoking privileges at the table or view level.
- Creating and dropping SQL roles.
- Using the system-wide variables for users and roles.

6 Encryption: Protecting Data at Rest

InterSystems IRIS includes a suite of encryption technologies that prevent unauthorized access to data at rest, which is data stored on disk or in the cloud. This suite of tools implements encryption using the AES (Advanced Encryption Standard) algorithm. Its technologies include:

- Block-level database encryption — InterSystems IRIS performs database encryption and decryption when writing to and reading from disk. The encrypted content includes the data itself, indexes, bitmaps, pointers, allocation maps, and incremental backup maps.
- Data-element encryption for use in applications — Data-element encryption uses a simple and comprehensive set of methods that allow an application to encrypt and decrypt content as needed.
- Encryption key management — To support encryption operations, InterSystems IRIS provides tools for creating and managing data encryption keys. These keys can be stored either in key files or on key servers that use the key management interoperability protocol (KMIP).

As with every aspect of InterSystems IRIS, encryption and decryption are optimized for performance. When writing to the database, there is no effect on performance at all. For reading the database, the effect is both deterministic and small.

7 System Security: Hardening an Instance

Because security requires actions within an instance and in an instance's larger environment, InterSystems IRIS provides both guidance and tools to help secure an instance. These include:

- A checklist of topics to review as you prepare to deploy InterSystems IRIS.
- A guide and tools for securing an instance using its built-in features.
- A checklist for hardening security for an instance at the operating-system level and by managing its processes.

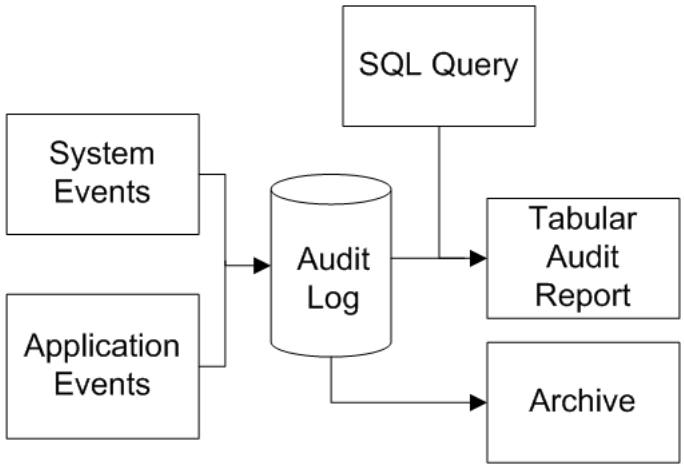
8 Auditing: Knowing What Happened

Auditing provides a verifiable and trustworthy trail of actions related to the system. Auditing serves multiple security functions:

- It provides proof — the proverbial "paper trail" — recording the actions of the authentication and authorization systems in InterSystems IRIS and its applications.
- It provides the basis for reconstructing the sequence of events after any security-related incident.
- If attackers know or assume it exists, it deters them (since it will record information about their actions during an attack).

The auditing facility allows you to enable logging for various system events, as well as user-defined events. Authorized users can then create reports based on this audit log, using tools that are part of InterSystems IRIS. The included InterSystems IRIS tools support archiving the audit log and other tasks.

Figure 2: InterSystems IRIS Auditing System



9 Public Key Infrastructure (PKI): Using with Certificates and Private Keys

InterSystems IRIS includes a PKI implementation. A Public Key Infrastructure (PKI) supports cryptographic operations for creating and managing private keys, public keys, and certificates. These operations include encryption, decryption, digital signing, and digital signature verification.

With the InterSystems PKI implementation:

- An instance of InterSystems IRIS can serve as a Certificate Authority (CA). As a CA server, an instance can either generate and use a self-signed CA Certificate, or it can use a CA Certificate issued by a commercial third party or product.
- An instance of InterSystems IRIS can be a CA client that uses the services of an InterSystems IRIS CA. As a CA client, an instance is associated with a CA server; the CA client's certificate is available for use with TLS, XML encryption, and signature verification.
- An instance of InterSystems IRIS can serve as both a CA server and a CA client. For example, you can configure a CA client to also serve as an intermediate CA.

InterSystems IRIS uses web services to perform PKI communications.