Overview of Authentication Mechanisms

Version 2024.1
2024-05-16

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

Overview of Authentication Mechanisms
InterSystems IRIS Data Platform Version 2024.1 2024-05-16

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

List of Figures

Overview of Authentication Mechanisms

1 About Authentication

Authentication verifies the identity of any user or other entity attempting to connect to InterSystems IRIS®. As it's often said, authentication is how you prove that you are who you say you are.

Once authenticated, a user has established communications with InterSystems IRIS, so that its data and tools are available. Without trustworthy authentication, authorization is moot — one user can impersonate another and then take advantage of the fraudulently obtained privileges.

2 Authentication Mechanisms

There are a number of different ways that a user can be authenticated; each is known as an *authentication mechanism*. InterSystems IRIS supports a number of authentication mechanisms:

- Kerberos — The Kerberos protocol was designed to provide secure authentication to services over an unsecured network. Kerberos uses tickets to authenticate a user and avoids the exchange of passwords across the network.
- Operating System–Based — OS-based authentication uses the operating system's identity for each user to identify that user to InterSystems IRIS.
- 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.
- Lightweight Directory Access Protocol (LDAP) — With the Lightweight Directory Access Protocol, InterSystems IRIS authenticates the user based on information in a central repository, known as the LDAP server.
- Delegated Authentication — Delegated authentication provides a means for creating customized authentication mechanisms. The application developer entirely controls the content of delegated authentication code.

You can also allow all users to connect to InterSystems IRIS without performing any authentication. This is known as *unauthenticated access*. Unauthenticated access option is appropriate for organizations with strongly protected perimeters or in which neither the application nor its data are an attractive target for attackers.

Generally, if you configure InterSystems to allow unauthenticated access, it is recommended there be unauthenticated access exclusively. If there is support for an authentication mechanism and then unauthenticated access if authentication fails, this is what is called *cascading authentication*, which is described in Cascading authentication. The circumstances for using more than one authentication mechanism are described in Use Multiple Authentication Mechanisms. InterSystems IRIS is typically configured to use only one of them.

3 How Authentication Works

The authentication mechanism is used by what are called *connection tools*. These specify the means by which users establish their connection with InterSystems IRIS. Each connection tool (such as the Terminal, Java, or web) uses an InterSystems

service that allows the administrator to specify the supported authentication mechanism(s). (A InterSystems service is a gatekeeper for connecting to InterSystems IRIS; for more information on services, see Services.)

There are three categories of connection tools, each of which is known as an *access mode*. Each access mode has its own characteristics and has its own supported services. The access modes are:

- Local — The user interacts directly with the InterSystems IRIS executable on the machine where that executable is running.
- Client-Server — The user is operating a separate executable that connects to InterSystems IRIS.
- Web — The user has a web browser and is interacting with InterSystems IRIS through a web-based application.

An end-user uses a connection tool to interact with InterSystems IRIS in a particular access mode using a particular authentication mechanism. Remember that the processes described in this chapter do not themselves establish authenticated access. Rather, they establish the infrastructure that an application uses when authenticating users via a particular mechanism in a particular access mode.

3.1 About the Different Access Modes

InterSystems IRIS supports the following access modes: Local, Client-Server, and Web.

3.1.1 Local Access Mode

With local access, the end-user is on the same machine as the InterSystems IRIS server. To gain access to the data, the user runs a private image of InterSystems IRIS that is reading from and writing to shared memory. If there are multiple local users, each has an individual copy of the InterSystems IRIS executable and all the executables point to the same shared memory. Because the user and the executable are on the same machine, there is no need to protect or encrypt communications between the two, since nothing is being passed from one executable to another. Because communications between the user and InterSystems IRIS go on within a single process, this is also known as *in-process authentication*.

Local access is available for:

- The terminal — **`%Service_Console`** on Windows and **`%Service_Terminal`** on other operating systems
- Callin — **`%Service_CallIn`**

3.1.2 Client-Server Access Mode

With client-server access, the InterSystems IRIS executable is the server and there is a client executable that can reside on a separate machine. InterSystems IRIS accepts a connection, possibly over a wire, from the client. This connection can use any language or protocol that InterSystems IRIS supports. These include:

- ComPort — **`%Service_ComPort`**
- Java — **`%Service_Bindings`**
- JDBC — **`%Service_Bindings`**
- ODBC — **`%Service_Bindings`**
- Telnet — **`%Service_Telnet`**

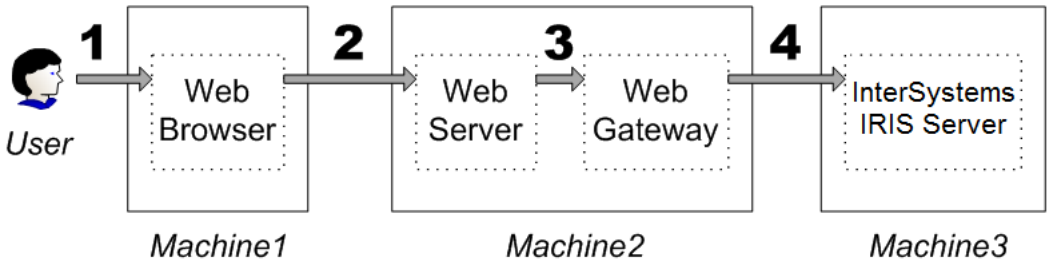
All connection tools support authentication through Kerberos or instance authentication except **`%Service_ComPort`**, which only supports authentication through instance authentication.

In each case, the server specifies the supported authentication type(s). When the client initiates contact with the server, it must attempt to use one of these supported types; otherwise, the connection attempt is rejected. Not all authentication types are available for all connection tools.

3.1.3 Web Access Mode

The web access mode supports connections of the following form:

Figure 1: Architecture of a Web Connection



1. A user requests content or an action in a web browser.
2. The web browser passes along the request to the web server.
3. The web server is co-located with the web gateway and passes the request to the gateway.
4. The gateway passes the request to the InterSystems IRIS server.

When the InterSystems IRIS server provides content for or performs an action relating to the user, the entire process happens in the other direction.

For the user to authenticate to InterSystems IRIS, a username and password must be passed down the line. Hence, this access mode is also known as a proxy mode or proxy connection. Once the information reaches the InterSystems IRIS machine, the arrangement between user and server is similar to that in the local access mode. In fact, the web access mode also uses in-process authentication.

4 Overview of Setting Up Authentication

1. Choose an authentication mechanism. Your choice may be based on your authorization needs and access modes.
2. Configure authentication according to the instructions in
   - Kerberos Authentication
   - Operating System–Based Authentication
   - Instance Authentication
   - LDAP Authentication
   - Delegated Authentication
3. Optionally implement two-factor authentication.
4. Optionally implement JSON web token (JWT) authentication.

It is recommended that each instance of InterSystems IRIS use only one authentication mechanism and that you choose the instance's authentication mechanism prior to installing InterSystems IRIS. Once installation has occurred, you can then begin configuring InterSystems IRIS to use the selected mechanism. This involves several steps:

- With Kerberos, ensure that all InterSystems IRIS users are listed in the Kerberos KDC (Key Distribution Center) or Windows Domain Controller.

- With operating system–based authentication, ensure that all InterSystems IRIS users appear in the operating system list.
- For all authentication mechanisms, configure all supported services to use only the selected authentication mechanism.
- For all authentication mechanisms, disable all unsupported services.
- For all authentication mechanisms, configure all applications to use only the selected authentication mechanism.

Note: Regardless of the selected authentication mechanism, during start-up and shut-down, operating system authentication is always used.