About TLS

Version 2023.3
2024-05-16

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

About TLS
InterSystems IRIS Data Platform Version 2023.3 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

About TLS

Transport Layer Security (TLS) provides strong protection for communication between pairs of entities. It allows you to perform authentication, data integrity protection, and data encryption. It is the successor to the secure sockets layer (SSL).

SSL was created at Netscape in the mid nineteen-nineties. TLS was created as a standardization of SSL 3.0; TLS version 1.0 was released in 1999. The latest version of TLS available with InterSystems IRIS is 1.3, often known as TLS v1.3. Among the supported versions of TLS for InterSystems IRIS® data platform, InterSystems recommends the use of the latest version available.

Note: In InterSystems documentation, the terms SSL/TLS and SSL are equivalent to TLS.

A TLS connection uses a client/server model; two entities establish a TLS connection through a *TLS handshake*. When two entities complete the handshake, this means that:

- The client has authenticated the server.
- If the server requires client authentication, this has happened. (If the client and the server have both authenticated each other, this is known as mutual authentication.)
- The client and server have agreed upon session keys. (*Session keys* are the keys for use with a symmetric-key algorithm that allow the entities to protect data during subsequent communications.)
- Subsequent communication can be encrypted.
- The integrity of subsequent communication can be verified.

The *cipher suites* of the client and server specify how these activities occur as part of the handshake or are supported for a protected connection. Specifically, a peer's cipher suites specify what features and algorithms it supports. The client proposes a set of possible ciphers for use; from among those proposed, the server selects one. (If there are no common ciphers between the client and server, the handshake fails.)

To perform the handshake, TLS typically uses public-key cryptography (though it can use other means, such as the Diffie-Hellman protocol). With public-key cryptography, each peer (either the client or the server) has a public key and a private key. The private key is a sensitive secret value and the public key is a widely published value; typically, the public key is encapsulated in a certificate, which also contains identifying information about the holder, such as a name, organization, location, issuer validity, and so on. For InterSystems IRIS, a TLS *configuration* (described in About Configurations) specifies a named set of TLS-related values, including a certificate file, a private key file, and an optional set of cipher suites.

If successful, the handshake creates session keys that are used to protect subsequent communications.

While InterSystems IRIS and applications require various interactions with TLS, the end-user typically has no such direct interactions. For example, a browser uses TLS to establish a secure connection with a specified web site by requiring that the site (the server, in this case) authenticate itself to the browser (which occurs unbeknownst to the browser's user) and the lock icon that appears in the browser is designed to indicate that TLS is protecting the connection.

1 InterSystems IRIS Support for TLS

InterSystems IRIS supports TLS to secure several types of connections:

- From various client applications that interact with the InterSystems IRIS superserver (including ODBC, JDBC, and Studio).
- From Telnet clients that interact with the Telnet server.
- For use with TCP connections where an InterSystems IRIS instance is the client or server (or an InterSystems IRIS instance is at each end).
- With the Enterprise Cache Protocol (ECP). For information on using TLS with ECP, see Securing Application Server Connections to a Data Server with TLS.

As a server, InterSystems IRIS accepts connections and establishes the use of TLS; as a client, InterSystems IRIS is able to connect to servers that require the use of TLS. In all cases, InterSystems IRIS uses what is called a TLS *configuration*, which specifies the various characteristics of an InterSystems IRIS instance as part of an TLS connection. To learn more about how to configure TLS, see Configuring TLS.

2 Which TLS Versions Does My Instance of InterSystems IRIS Support?

The versions of TLS that are available for an InterSystems IRIS instance depend on several factors:

1. The major version of the OpenSSL libraries available for the operating system (OS) version. These libraries determine the possible versions of the TLS protocol that the operating system supports.
2. Any further restrictions that the operating system vendor has placed on supported versions of the protocol, such as those on Ubuntu 20.04.
3. The minimum supported version of TLS for this version of InterSystems IRIS. For this release, it is TLS v1.0.

For containers, the supported versions of TLS depend on the operating system and version of the container host.

Important: Because the protocols vary by operating system version, two instances of the same version of InterSystems IRIS may not support the same versions of the TLS protocol. Note that TLSv1.2 is the only version of the protocol that is supported on all platforms.

OS	Version	OpenSSL Version	TLS Version	Notes
AIX	7.2	1.0.2	1.0, 1.1, 1.2	See AIX 7.2 TLS Notes below.
AIX	7.3	3.0	1.2, 1.3	
Red Hat Linux	8	1.1.1	1.0, 1.1, 1.2, 1.3	See Red Hat Linux 8 TLS Notes below.
Red Hat Linux	9	3.0	1.2, 1.3	
SUSE Linux	All	1.1.1	1.0, 1.1, 1.2, 1.3	
Ubuntu Linux	18.04	1.1.1	1.0, 1.1, 1.2, 1.3	
Ubuntu Linux	20.04	1.1.1	1.2, 1.3	See Ubuntu Linux 20.04 and 22.04 TLS Notes below.
Ubuntu Linux	22.04	3.0	1.2, 1.3	See Ubuntu Linux 20.04 and 22.04 TLS Notes below.
Windows	All	3.1.1	1.2, 1.3	See Windows TLS Notes below.

Note: For information on versions of Oracle Linux, see the analogous version of Red Hat Linux.

2.1 AIX 7.2 TLS Notes

Because AIX 7.2 uses the OpenSSL 1.0.2 libraries, note that:

- The OpenSSL 1.0.2 libraries support SSLv3 through TLSv1.2. Because InterSystems IRIS does not support SSLv3, there is support only for TLSv1.0 through TLSv1.2.
- The OpenSSL 1.0.2 libraries do not include SHA-3, so InterSystems provides its own implementation of SHA-3. This implementation is not compatible with the **RSASHA3Sign** and **RSASHA3Verify** functions. Calls to these functions return an <UNIMPLEMENTED> error.

2.2 Red Hat Linux 8 TLS Notes

In FIPS mode, Red Hat Linux 8 supports only TLSv1.2 and TLSv1.3.

2.3 Ubuntu Linux 20.04 and 22.04 TLS Notes

Ubuntu 20.04 and 22.04 support only TLSv1.2 and TLSv1.3. This is because these versions of Ubuntu prohibit the use of TLSv1.0 and TLSv1.1.

2.4 Windows TLS Notes

Windows does not use OpenSSL, so InterSystems ships the OpenSSL 3.1.1 libraries as part of the InterSystems IRIS distribution. Hence, there is support for TLSv1.2 through TLSv1.3.