Managing Superservers

Introduction to the Superserver

The InterSystems IRIS® superserver is a process that runs the **%SYS.SERVER** routine. It does the following:

1. Listens on the superserver port
2. Recognizes certain types of incoming TCP requests
3. Handles those requests and responds to the original sender

InterSystems IRIS supports multiple superserver per instance. Each superserver can accept a different combination of connection requests and use TLS independently of each other.

Supported Requests

The superserver supports many requests out of the box. These include:

- JDBC and ODBC clients
- CSP/REST
- DataCheck
- ECP (system default superserver only)
- Mirroring (system default superserver only)
- Sharding (system default superserver only)
- SNMP (Windows only)

Additionally, the superserver supports some legacy connections. These connections are disabled by default. These include:

- CacheDirect
- Shadowing
- WebLink
- NodeJS

How It Works

The superserver is a process that listens on a predefined port. For the first installed instance of InterSystems IRIS, the system default superserver port number is 1972. Any additional superservers you create have a port number you set during creation.

Each superserver recognizes TCP requests, as detailed in Supported Requests, incoming on the predefined port and handles those connections with InterSystems IRIS appropriately. It acts as a middle layer between external connections, which could be clients or other instances of InterSystems IRIS, and the superserver's associated instance of InterSystems IRIS. You can configure each superserver you create to handle different requests. For example, you can set the system default superserver to only accept system and CSP/REST connections. You can then configure a second superserver to handle some combination of client and other connections and a third superserver to handle a different set of connections.

System Default Superserver

> InterSystems IRIS comes installed with a superserver as the system default superserver. You can configure this superserver to handle client connections, system connections, such as ECP, Mirroring, and Sharding, and other connections, as well as access to the management portal. See Changing the System Default Superserver and Using the CPF and CMF for details on how to change this superserver.

How to Configure

How to Configure

You can configure a superserver through the management portal, through the **^SECURITY** routine, through the configuration merge file, or programmatically with the Security.Servers class.

Using the Management Portal

You can view all of the superserver configuration definitions in **System** > **Security Management** > **Superservers**.

Creating a Superserver with the Management Portal

To create a new superserver, click **Create New Superserver**. This takes you to a form of configuration settings with the following fields:

- **Description** — Optional. Text describing this superserver.
- **Port** — Required. A number for a valid, unused port on the system. The superserver listens on this port.
- **Bind Address** — Optional. An IP address or DNS hostname representing which network interface the superserver listens on. For example, a value of **`127.0.0.1`** binds the superserver to localhost. The superserver with this bind address only accepts local connections.
- **Enabled** — If selected, this superserver is set to active and listening.
- **Client Connections** — Connections that support TLS. Includes:
  - **Enable Clients** — Allow JDBC and ODBC client connections. See Getting Started: ODBC or JDBC Fundamentals for more details on ODBC or JDBC, respectively.
  - **Enable CSP/REST** — Allow web API connections. See Introduction to CSP-Based Web Applications or Introduction to Creating REST Services for more details on CSP or REST, respectively.

> **IMPORTANT:**

IMPORTANT

To maintain access to the management portal, you must have **Enable CSP/REST** selected for the system default superserver.

- **Enable DataCheck**— Allow data consistency checking connections. See Data Consistency on Multiple Systems for more details.

InterSystems IRIS superservers also support legacy client connections. Click **Legacy Settings** to reveal additional connection options. These include:

- **Enable CacheDirect** — See Introduction to Caché Direct for more details.
- **Enable Shadows** — See Shadowing for more details.

Client connections support TLS for encrypting communications. The options for configuring TLS for a superserver are below:

- **SSL/TLS support level** — The requirement level for connections to use TLS. It has three options:
  - **Disabled** — Client communications do not use TLS.
  - **Enabled** — Client communications may use TLS.
  - **Required** — Client communications must use TLS.
- **SSL/TLS Configuration** — Required if SSL/TLS support level is enabled or required. See Configuring TLS for more details.

- **System Connections** — Only the system default superserver supports system connections. These include:
  - **Enable ECP** — See ECP Overview for more details.
  - **Enable Mirror** — See Mirroring Overview for more details.
  - **Enable Sharding** — See Sharding Overview for more details.
- **Other Connections** — Connections that do not support

TLS. Includes:

- **Enable SNMP** — Allow Simple Network Management Protocol (SNMP) connections on Windows systems only. See Monitoring InterSystems IRIS Using SNMP for more details.

InterSystems IRIS superservers also support other legacy connections. To configure these connections, click **Legacy Settings**. Options include:

- **Enable WebLink** — See Caché WebLink Guide for more details.
- **Enable NodeJS** — See Using Node.js with Caché for more details.

Editing a Superserver with the Management Portal

You can edit a superserver configuration by clicking the port number of the superserver you want to change in the superserver definitions list. The only settings you cannot change from this page are the port number, the bind address, and the system default superserver selection.

Changing the System Default Superserver with the Management Portal

You can change the system default superserver port number in the management portal. You can find the **Superserver Port Number** field in **System** > **Configuration** > **Memory and Startup** > **(configuration settings)**. If the port number is not associated with a superserver configuration, the current system default superserver changes port numbers to the newly defined one. If the port number is associated with a superserver configuration, this superserver configuration becomes the new system default superserver. The change takes effect on system restart.

IMPORTANT:

To maintain access to the management portal,

you must have **Enable CSP/REST** selected for the system default superserver.

Using ^SECURITY

The **^SECURITY** routine has a menu-driven interface that enables you to perform the following superserver management tasks:

- Create a superserver.
- Edit a superserver.
- List superservers.
- Delete a superserver.
- Export superservers.
- Import superservers.

See Command-Line Security Management Utilities for more information about **^SECURITY**.

Creating a Superserver with ^SECURITY

Similar to the management portal, you can create a superserver using **^SECURITY**. The fields are the same as in the management portal. To create a superserver using **^SECURITY**, follow these steps:

1. Start the Terminal and log in as a sufficiently privileged user for the relevant instance.
2. At the terminal prompt, switch to the **%SYS** namespace:

```
>zn "%SYS"
```

3. Run **^SECURITY**:

```
%SYS>do ^SECURITY
```

4. In **^SECURITY**, select option **15) Superserver setup**. This presents you with different options for managing superservers. To create a superserver, select option **1) Create Superserver**.

5. Follow the prompts to enter details about the superserver configuration you wish to create. The fields are the same as in the management portal; see Using the Management Portal for more details.

Editing a Superserver with ^SECURITY

Similar to the management portal, you can edit a superserver using ^SECURITY. To do so, follow these steps:

1. Start the Terminal and log in as a sufficiently privileged user for the relevant instance.

2. At the terminal prompt, switch to the **%SYS** namespace:

```
>zn "%SYS"
```

3. Run **^SECURITY**:

```
%SYS>do ^SECURITY
```

4. In **^SECURITY**, select option **15) Superserver setup**. This presents you with different options for managing superservers. To edit a superserver, select option **2) Edit Superserver**.

5. To identify which superserver you wish to edit, first enter the port number associated with that superserver. When prompted for the bind address, enter the associated bind address with that superserver. If the bind address is empty, simply continue through the prompts. You need both of these pieces of information to correctly identify and edit the superserver.

IMPORTANT:

IMPORTANT

The port number and bind address must match the existing superserver configuration exactly to edit it.

Using the CPF and CMF

The system default superserver port configuration is defined in the configuration parameter file (CPF) under the **[Startup]** section in the **`DefaultPort`** field. You can change the default port of the system default superserver in the CPF. You can also change the default bind address with the **`DefaultPortBindAddress`** field. If the port number is not associated with a superserver configuration, the current system default superserver changes port numbers to the newly defined one. If the port number is associated with a superserver configuration, this superserver configuration becomes the new system default superserver. The port and bind address are initialized on instance start.

You can also configure superservers using the configuration merge file (CMF). The CMF supports the following three actions for superservers: *CreateServer*, *DeleteServer*, and *ModifyServer* using the properties defined in the Security.Servers class.

Programmatically

You can programmatically configure superservers using the Security.Servers class. Refer to the class reference for more details on using this class.

Support for

← Configuring TLS

OAuth 2.0 and OpenID Connect →

© 2026 InterSystems Corporation, Boston, MA. All rights reserved.

Privacy & Terms Guarantee Accessibility

Content date/time: 2026-10-26 18:37:03