Securing Your Instance

Version 2023.1
2024-07-11

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

Securing Your Instance
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

List of Tables

1

Security Strategy

The best time to start planning for securing your InterSystems IRIS® instance occurs before you perform the initial installation. The section Prepare for InterSystems Security describes some issues you should consider prior to installing InterSystems IRIS® instance. In general, for production systems, InterSystems recommends that you start with the highest possible level of security and then grant privileges only as required. A good place to start is by performing an installation with the initial security setting of Locked Down and then fine tuning from there.

Once you have installed InterSystems IRIS, or if you have already installed your instance, see Tighten Security for an Instance for guidance on ways you can restrict access to the instance and reduce the surface of attack. If you have performed the installation using the Locked Down initial security setting, some of the steps outlined here have already been done for you. However, you should still review its contents to learn additional steps you can take to tighten your instance.

The InterSystems IRIS Management Portal includes the Security Advisor, which provides a list of areas that should be examined for your instance to see if they should be tightened further. For each such area, the Security Advisor provides a handy link to the appropriate page in the Management Portal so that the related setting can be adjusted, if needed.

Of course, running a secure system requires the hardening of attack surfaces apart from the InterSystems IRIS executable. InterSystems IRIS also uses other processes and resources that could be targets for malicious behavior. The section Secure InterSystems Processes and Operating-System Resources discusses these topics and provides guidelines for you to follow.

Lastly, the Checklist for Hardening Your Deployment is divided into a number of broader security categories, such as network, operating system, or web server, and provides a checklist for each category that your organization can use to harden your deployment as a whole.

2

Prepare for InterSystems Security

The material in this section describes some of the security-related issues you need to consider before installing InterSystems IRIS. For an overview of the InterSystems security features, see "About InterSystems Security"; you may also want to review details about authentication or authorization.

This section covers the following topics:

- Initial InterSystems Security Settings — Describes the characteristics of the different default security settings. It is particularly useful if you choose to use Normal or Locked Down InterSystems security.
- Configure User Accounts — Discusses the necessary permissions for a user account that runs InterSystems IRIS.
- Prepare the Security Environment for Kerberos — Details the additional tasks you need to perform if you are planning on using Kerberos as an authentication mechanism with InterSystems IRIS. If you are not using Kerberos in your environment, you can bypass this topic.

Important: If your security environment is more complex than those this document describes, contact the InterSystems Worldwide Response Center (WRC) for guidance in setting up such an environment.

After reading *About InterSystems Security* and following the procedures in this section, you are prepared to provide the pertinent security information to the installation procedure, as described in the Installation Guide.

2.1 Initial InterSystems Security Settings

During installation, there are three initial security configurations to choose from: **Minimal**, **Normal**, or **Locked Down**. A good rule of thumb is to choose Locked Down for instances to be used in production environments and Normal for instances to be used in development environments. The following sections describe the differences between these configurations, as well as the initial service properties for each configuration:

- Initial User Security Settings
- Initial User Account Passwords
- Initial Service Properties

For production environments, you should adjust the individual security settings after installation, regardless of which option you choose. For more information see the following sections:

- Tighten Security for an Instance
- Security Advisor

- Secure InterSystems Processes and Operating-System Resources
- Checklist for Hardening Your Deployment

Important: If you are concerned about the visibility of data in memory images (often known as core dumps), see Protect Sensitive Data in Memory Images.

2.1.1 Initial User Security Settings

For general information about InterSystems IRIS user accounts, see User Accounts.

All user accounts share certain password requirements and settings. The initial values for these settings are based on which security level you choose, as described in the following table:

Security Setting	Minimal	Normal	Locked Down	Description
Password Pattern*	3.32ANP	3.32ANP	8.32ANP	By default, passwords allow alphanumeric characters and punctuation. The initial length requirement is 3 to 32 characters for Minimal and Normal installations, or 8 to 32 for Locked Down installations. For more information about password patterns, see Password Strength and Password Policies.
Inactive Limit*	0	90 days	90 days	The Inactive Limit is the number of days an account can be inactive before it is disabled. For Minimal installations, the limit is set to 0 indicating that accounts are never disabled, no matter how long they are inactive. Normal and Locked Down installations have the default limit of 90 days.
Enable _SYSTEM User	Yes	Yes	No	
Roles assigned to UnknownUser	%All	None	None	When an unauthenticated user connects, InterSystems IRIS assigns a special name, `UnknownUser`, to $USERNAME and assigns the roles defined for that user to $ROLES. In a Minimal security installation, the `UnknownUser` is assigned the %All role; `UnknownUser` has no roles when choosing a security level other than Minimal. For more details on the use of $USERNAME and $ROLES, see Users and Roles.

* You can maintain these settings from the **System** > **Security Management** > **System Security Settings** > **System-wide Security Parameters** page of the Management Portal. See System-wide Security Parameters for more information.

2.1.2 Initial User Account Passwords

InterSystems IRIS creates multiple user accounts during installation. The predefined InterSystems IRIS user accounts have different default passwords and behavior depending on whether an installation uses Minimal security, Normal security, or Locked Down security. These differences are as follows:

- *Minimal security* – All the created accounts except _PUBLIC have an initial default password of “SYS”. With the exception of UnknownUser, you should change the account passwords after installation in order to prevent unauthorized access to your InterSystems IRIS instance.

  The _PUBLIC account has no password by default and should never be given a password, since it is never enabled.

- *Normal security* – All the created accounts except _PUBLIC receive the same password as is chosen for the privileged user account. It is recommended that you change these passwords after installation, so that each account has its own password.

  The _PUBLIC account has no password by default and should never be given a password, since it is never enabled.

- *Locked Down security* – All the created accounts except _PUBLIC receive the same password as is chosen for the privileged user account. It is recommended that you change these passwords after installation, so that each account has its own password.

  The _PUBLIC account has no password by default and should never be given a password, since it is never enabled. In Locked-Down installations, the _SYSTEM account is also disabled.

CAUTION: The default password is a security vulnerability, particularly in a Minimal Security installation. To address this issue, disable the accounts or change their passwords. InterSystems recommends disabling the account.

This is a critical concern with containerized instances in particular; see Authentication and passwords for more information, including ways in which you can address the issue.

2.1.3 Initial Service Properties

Services are the primary means by which users and computers connect to InterSystems IRIS. For detailed information about the InterSystems services see Services.

Service Property	Minimal	Normal	Locked Down	Description

Service Property	Minimal	Normal	Locked Down	Description
Use Permission is Public	Yes	Yes	No	If the Use permission on a service resource is Public, any user can employ the service; otherwise, only privileged users can employ the service.
Requires Authentication	No	Yes	Yes	For installations with initial settings of Normal or Locked Down, all services require authentication of some kind (Instance Authentication, operating-system–based, or Kerberos). Otherwise, unauthenticated connections are permitted.

Service Property	Minimal	Normal	Locked Down	Description
Enabled Services	Most	Some	Fewest	The initial security settings of an installation determine which of certain services are enabled or disabled when InterSystems IRIS first starts. The Enabled Services table below shows these initial settings.

Table 2–1: Enabled Services

Service	Minimal	Normal	Locked Down
%Service_Bindings	**Enabled**	**Enabled**	Disabled
%Service_CacheDirect	**Enabled**	Disabled	Disabled
%Service_CallIn	**Enabled**	Disabled	Disabled
%Service_ComPort	Disabled	Disabled	Disabled
%Service_Console*	**Enabled**	**Enabled**	**Enabled**
%Service_ECP	Disabled	Disabled	Disabled
%Service_Monitor	Disabled	Disabled	Disabled
%Service_Telnet*	Disabled	Disabled	Disabled
%Service_Terminal†	**Enabled**	**Enabled**	**Enabled**
%Service_WebGateway	**Enabled**	**Enabled**	**Enabled**

* Service exists on Windows servers only

† Service exists on non-Windows servers only

2.2 Configure User Accounts

During the installation process, you must choose an account to run the InterSystems IRIS process as the instance owner. The installation creates an InterSystems IRIS account with the %All role for the instance owner, providing that account with full administrator access to InterSystems IRIS.

To ensure that the instance owner has the necessary privileges, you may need to create a new user account. The following sections contain OS-specific details about what accounts and privileges are necessary:

- Windows — Windows User Accounts in the “Installing InterSystems IRIS on Microsoft Windows” chapter of the Installation Guide.
- Unix® and Linux — Determine Owners and Groups in the “Installing InterSystems IRIS on UNIX®, Linux, and macOS” chapter of the Installation Guide.

2.3 Prepare the Security Environment for Kerberos

All InterSystems IRIS supported platforms have versions of Kerberos supplied and supported by the vendors. To use Kerberos, you must have either a Kerberos key distribution center (KDC) or a Windows domain controller available on your network. The installation preparations for each are as follows:

- Windows domain controller

  This configuration uses a Windows domain controller for KDC functionality with InterSystems IRIS servers and clients on Windows and non-Windows machines. A domain administrator creates domain accounts for running the InterSystems services on InterSystems IRIS servers. See the following sections for the requirements for using both Windows and non-Windows InterSystems IRIS servers:

  - Create Windows Service Accounts for Windows Servers
  - Depending on the applications in use on your system, you may also need to perform actions described in Configure Windows Kerberos Clients.
  - Create Windows Service Accounts for Non-Windows Servers

- Non-Windows KDC

  This configuration uses a UNIX® or Kerberos KDC with InterSystems IRIS servers and all clients on non-Windows machines. See the following two sections for the requirements for using a UNIX® or macOS KDC and InterSystems IRIS servers:

  - Create Service Principals on a KDC for Non-Windows Servers
  - Test Kerberos KDC Functions

A Note on Terminology

This document refers to related, but distinct entities:

- Service account — An entity within an operating system, such as Windows, that represents a software application or service.
- Service principal — A Kerberos entity that represents a software application or service.

2.3.1 Create Windows Service Accounts for Windows Servers

Microsoft Windows implements the Kerberos authentication protocol by integrating the KDC with other security services running on the domain controller. Before you install InterSystems IRIS in a Windows domain, you must use the Windows domain controller to create a service account for each InterSystems IRIS server instance on a Windows machine.

2.3.1.1 Account Characteristics

When you create this account on the Windows domain controller, configure it as follows:

- Set the account's **Password never expires** property.
- Make the account a member of the **Administrators** group on the InterSystems IRIS server machine.
- Add the account to the **Log on as a service** policy.

Important: If a domain-wide policy is in effect, you must add this service account to the policy for InterSystems IRIS to function properly.

2.3.1.2 Names and Naming Conventions

In an environment where clients and servers are exclusively on Windows, there are two choices for naming service principals. You can follow the standard Kerberos naming conventions, which ensures compatibility with any non-Windows systems in the future, or you can use any unique string. Each of these choices involves a slightly different process of configuring a connection to a server.

- For a name that follows Kerberos conventions, the procedure is:
    1. Run the Windows **setspn** command, specifying the name of service principal in the form *service_principal*/*fully_qualified_domain_name*, where *service_principal* is typically `iris` and *fully_qualified_domain_name* is the machine name along with its domain. For example, a service principal name might be `iris/irisserver.example.com`. For detailed information on the **setspn** tool, see the Setspn page in the Microsoft documentation.
    2. In the **InterSystems IRIS Server Manager** dialog for adding a new preferred server, choose Kerberos. What you specify for the **Service Principal Name** field should match the principal name specified in **setspn**.
- For a name that uses any unique string, the procedure is:
    1. Choose a name for the service principal. A suggested naming convention for each account representing an InterSystems IRIS server instance is "`iris`*HOST*", which is the literal `iris` followed by the host computer name in uppercase. For example, if you are running an InterSystems IRIS server on a Windows machine called WINSRVR, name the domain account `irisWINSRVR`.
    2. In the **InterSystems IRIS Server Manager** dialog for adding a new preferred server, choose Kerberos. Specify the selected name for the service principal in the **Service Principal Name** field.

For more information on configuring remote server connections, see Connecting to Remote Servers for the detailed procedure.

2.3.2 Configure Windows Kerberos Clients

If you are using Windows clients with Kerberos, you may also need to configure these so that they do not prompt the user to enter credentials. This is required if you are using a program that cannot prompt for credentials — otherwise, the program is unable to connect.

To configure Windows not to prompt for credentials, the procedure is:

1. On the Windows client machine, start the registry editor, **regedit.exe**.
2. Go to the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters key.
3. In that key, set the value of *AllowTgtSessionKey* to 1.

2.3.3 Create Windows Service Accounts for Non-Windows Servers

Before you install InterSystems IRIS in a Windows domain, you must use the Windows domain controller to create a service account for each InterSystems IRIS server instance on a non-Windows machine. Create one service account for each machine, regardless of the number of InterSystems IRIS server instances on that machine.

A suggested naming convention for these accounts is "`iris`*HOST*," which is the literal, `iris`, followed by the host computer name in uppercase. For example, if you run an InterSystems IRIS server on a non-Windows machine called UNIXSRVR, name the domain account `irisUNIXSRVR`. For InterSystems IRIS servers on non-Windows platforms, this is the account that maps to the Kerberos service principal.

Important: When you create this account on the Windows domain controller, InterSystems IRIS requires that you set the **Password never expires** property for the account.

To set up a non-Windows InterSystems IRIS server in the Windows domain, it must have a keytab file from the Windows domain. A keytab file is a file containing the service name for the InterSystems IRIS server and its key.

To accomplish this, map the Windows service account (`irisUNIXSRVR`, in this example) to a service principal on the InterSystems IRIS server and extract the key from the account using the **ktpass** command-line tool on the domain controller; this is available as part of the Windows support tools from Microsoft.

The command maps the account just set up to an account on the UNIX®/Linux machine; it also generates a key for the account. The command must specify the following parameters:

Parameter	Description
/princ	The principal name (in the form *iris/<fully qualified hostname>@<kerberos realm>*).
/mapuser	The name of the account created (in the form *iris<HOST>*).
/pass	The password specified during account creation.
/crypto	The encryption type to use (use the default unless specified otherwise).
/out	The keytab file you generate to transfer to the InterSystems IRIS server machine and replace or merge with your existing keytab file.

Important: The principal name on UNIX®/Linux platforms must take the form shown in the table with the literal `iris` as the first part.

Once you have generated a key file, move it to a file on the InterSystems IRIS server with the *key file characteristics* described in the section below.

2.3.4 Create Service Principals on a KDC for Non-Windows Servers

In a non-Windows environment, you must create a service principal for each UNIX®/Linux or macOS InterSystems IRIS server that uses a UNIX®/Linux or macOS KDC. The service principal name is of the form *iris/<fully qualified hostname>@<kerberos realm>*.

2.3.4.1 Key File Characteristics

Once you have created this principal, extract its key to a key file on the InterSystems IRIS server with the following characteristics:

- On most versions of UNIX®, the pathname is *install-dir*/mgr/iris.keytab. On macOS and SUSE Linux, the pathname is /etc/krb5.keytab.
- It is owned by the user that owns the InterSystems IRIS installation and the group `irisusr`.
- Its permissions are `640`.

2.3.5 Test Kerberos KDC Functions

When using Kerberos in a system of only non-Windows servers and clients, it is simplest to use a native UNIX®/Linux KDC rather than a Windows domain controller. Consult the vendor documentation on how to install and configure the KDC; these are usually tasks for your system administrator or system manager.

When installing Kerberos, there are two sets of software to install:

- The KDC, which goes on the Kerberos server machine.
- There also may be client software, which goes on all machines hosting Kerberos clients. This set of software can vary widely by operating system. Consult your operating system vendor documentation for what client software exists and how to install it.

After installing the required Kerberos software, you can perform a simple test using the **kadmin**, **kinit**, and **klist** commands to add a user *principal* to the Kerberos database, obtain a TGT (ticket-granting ticket) for this user, and list the TGT.

Once you successfully complete a test to validate that Kerberos is able to provide tickets for registered principals, you are ready to install InterSystems IRIS.

3

Tighten Security for an Instance

To provide increased security for an InterSystems IRIS® database, you can and should configure it to more tightly constrain user access. This can prevent unauthorized users from using system tools or from gaining access to sensitive resources. This section describes various actions that reduce the attack surface of a database instance or otherwise increase its security. The section assumes you have already installed an InterSystems IRIS instance with an initial security of Minimal. If you have chosen an initial security of Normal or Locked Down, some of these actions have already been performed for you.

There actions for tightening an instance's security are presented here roughly in the sequence in which they should be performed:

- Enable auditing
- Change the authentication mechanism for an application
- Restrict access to services. This involves:
  - Limit the number of enabled services
  - Limit the number of public services
  - Restrict access to services by IP address or machine name
- Limit remote privileged access
- Limit the number of privileged users
- Disable the _SYSTEM user
- Restrict access for UnknownUser
- Configure third-party software

The InterSystems Security Advisor also provides an automated analysis of the instance and recommendations for actions to increase the security of an instance.

Important: An InterSystems IRIS database instance has many interdependent elements. Because of this, it is recommended that you only do what is specified for a change, and not more or less. For example, simply removing UnknownUser from the **`%All`** role — without doing anything else — will cause problems for a minimal-security installation.

3.1 Enable Auditing

The primary elements of security are often described as the "Three A's": authentication, authorization, and auditing. Auditing provides two functions:

- It provides data about what has occurred if there is a security event.
- The knowledge of its existence can be a deterrent for an attacker, given that the attack will be tracked and there will be evidence of any malicious actions.

To enable auditing for key events, the procedure is:

1. From the Management Portal home page, select **System Administration** > **Security** > **Auditing** > **Enable Auditing**. If the choice is not available, auditing is already enabled.
2. From the Management Portal home page, go to **Configure System Events** page (**System Administration** > **Security** > **Auditing** > **Configure System Events**).
3. On the **Configure System Events** page, enable the following events if they are not already enabled by clicking **Change Status** in the event's row:
    - %System/%DirectMode/DirectMode — Provides information on console/terminal use. For sites that extensively use command-line utilities, can create large amounts of data. Recommended if increased data is not an issue.
    - %System/%Login/Login — Provides information on logins. For large sites, can create large amounts of data. Recommended if increased data is not an issue.
    - %System/%Login/LoginFailure — Provides feedback on possible attempted unauthorized logins. Recommended.
    - %System/%Security/Protect — Provides data on attempts to read, write, or use protected data. Recommended.

3.2 Change the Authentication Mechanism for an Application

A key element of restricting access to the database is configuring the instance to use a stricter authentication mechanism for its applications. This section describes how to perform this procedure, using the Management Portal as an example application and with the change from unauthenticated access (as in a minimal-security installation) to requiring a password as an example of moving to a stricter authentication mechanism.

Important: Performing the following procedure may affect aspects of the instance being modified beyond access to the Portal. The specifics depend on (1) the instance's configuration and (2) whether you are performing just this procedure or all the procedures in this section. Specifically:

- Making %Service_WebGateway:Use not public means that all users of web applications will need to be granted `%Service_WebGateway:Use` by some other means.
- Removing UnknownUser from the %All role can have many effects.

To provide properly functioning authentication for an application, there must be consistent authentication mechanisms for both the application and any service that it uses. For a web application, the Web Gateway must also be configured to match the Web Gateway service. Hence, to provide authentication for the Management Portal, there are three layers that all need to work together:

- The **`%Service_WebGateway`** service
- The Web Gateway
- The Management Portal application

If these layers do not have matching authentication mechanisms, this usually results in a denial of access — for example, there may be a “This page cannot be displayed” error instead of a login page or access to the Management Portal.

Important: If (1) a web application uses a more powerful authentication mechanism than the Web Gateway and **`%Service_WebGateway`** and (2) authentication succeeds, then the system’s security is only that of the less powerful mechanism.

For an instance with a minimal-security installation, the Web Gateway, **`%Service_WebGateway`**, and the Management Portal application are all set up for unauthenticated access. To provide password-level authentication for the Portal, various InterSystems IRIS elements must be configured as follows:

- The Web Gateway service must require password authentication.
- The Web Gateway must provide a username and password for that authentication.
- The user representing the Gateway must have sufficient privilege to use the Web Gateway service.
- The Management Portal must require password authentication.
- All the Portal’s users must have sufficient privilege to use the Portal.

Important: Complete the following set of procedures during a single session in the Portal. Otherwise, you may lock yourself out of the Portal and have to perform the remaining procedures through the ^SECURITY routine.

An overview of the procedure to make these changes is:

1. Optionally, turn on auditing to track the changes to the instance. This is described in Enable Auditing .
2. Give the %Service_WebGateway:Use privilege to the CSPSystem user.
3. Change the password of the CSPSystem user.
4. Configure the Web Gateway to provide a username and password for authentication.
5. Configure %Service_WebGateway to require password authentication.
6. Remove the public status of the %Service_WebGateway:Use privilege.
7. Configure the Management Portal application to require password authentication only.
8. Specifying the appropriate privilege level for the instance’s users.
9. Optionally, make the class reference available.
10. Begin enforcement of the new policies.

Once this process is complete, then a user’s next attempt to connect to the Portal will result in a login prompt.

CAUTION: An InterSystems IRIS database instance has many interdependent elements. Because of this, it is recommended that you only do what is specified for a change, and not more or less. Otherwise, you may lock yourself out of the instance or could even render the instance temporarily inoperative.

3.2.1 Give the %Service_WebGateway:Use Privilege to the CSPSystem User

The InterSystems IRIS installation process creates a CSPSystem user, which represents the Web Gateway in its interactions with the **`%Service_WebGateway`** service. Since the service is going to have restricted access, this user needs to hold the **`%Service_WebGateway:Use`** privilege for the authentication process.

Note: There is a *service* called **`%Service_WebGateway`** and a *resource* called **`%Service_WebGateway`**. The resource regulates access to the service. Therefore, to gain access to the service, a user must have Use permission for the resource — that is, the **`%Service_WebGateway:Use`** privilege.

To associate the **`%Service_WebGateway:Use`** privilege with the CSPSystem user, the procedure is:

1. From the Management Portal home page, go to the **Roles** page (**System Administration** > **Security** > **Roles**).
2. On the **Roles** page, click **Create New Role**. This displays the **Edit Role** page, where the **Name** field is editable.
3. Enter a name for the role to include the **`%Service_WebGateway:Use`** privilege (such as “GatewayRole”).
4. Click **Save**. InterSystems IRIS has now created the role.
5. In the **Privileges** section on the **General** tab of the **Edit Role** page, click **Add**, which displays a list of available resources for the role.
6. From this list, click **%Service_WebGateway** and then click **Save**. The newly created role now includes the **`%Service_WebGateway:Use`** privilege.
7. Select the **Members** tab of the **Edit Role** page.
8. On this tab, you can assign the CSPSystem user to the newly created role. Click CSPSystem from the users in the **Available** list and move it to the **Selected** by clicking the right arrow.
9. Click **Assign** to assign CSPSystem to the role. (In other words, CSPSystem is now a member of the role.) This means that CSPSystem holds the **`%Service_WebGateway:Use`** privilege.

Note: The system creates the CSPSystem user to represent the Web Gateway. If you prefer, a different user can perform this function. This procedure refers only to the CSPSystem user; if you use a different user, replace CSPSystem with that username where relevant.

3.2.2 Change the Password of the CSPSystem User

Because a minimal-security installation gives the CSPSystem user a password of “SYS”, it is important to change this to a new password — one that an attacker would not know or be able to guess. The procedure is:

1. In the Management Portal, go to the **Users** page (**System Administration** > **Security** > **Users**).
2. On the **Users** page, click **CSPSystem**. This displays the **Edit User** page.
3. Enter the new password for CSPSystem in the **Password** field. Since no user has to remember this password, you can make it as long and complex as you wish. You will need to remember it long enough to complete the next item, Configure the Web Gateway to Provide a Username and Password.
4. Reenter the new password in the **Password (Confirm)** field and click **Save**. If the Portal does not display an error message or dialog, then the password change has succeeded.

If you wish, you can also confirm that CSPSystem is assigned to the role created for authentication in the previous procedure. To do this, click on the **Roles** tab. The table with the column heading **CSPSystem is Assigned to the Following Roles** should list the newly-created role.

3.2.3 Configure the Web Gateway to Provide a Username and Password

Because you are going to configure `%Service_WebGateway` to require password authentication, the Web Gateway needs to provide a username-password pair. Having set up a user with the appropriate level of privilege, you have established a username-password pair that the Gateway can provide. The next step is to configure the Gateway to provide this username-password pair when the InterSystems IRIS server challenges it for them. The procedure is:

1. In the Management Portal, go to the **Web Gateway Management** page (**System Administration** > **Configuration** > **Web Gateway Management**).
2. On the **Web Gateway Management** page, select **Server Access** from the list on the left side. This displays the **Server Access** frame.
3. In the **Server Access** frame, the LOCAL server should be highlighted. Click **Submit** to edit it, which displays a page with Server Access and Error Pages parameters.
4. On this page, there is a **Connection Security** section.
5. Ensure that the **Connection Security Level** drop-down has “Password” displayed.
6. In the **User Name** field, enter `CSPSystem`.
7. In the **Password** and **Password (Confirm)** field, enter the password that you selected in the previous section.
8. Click **Save Configuration** near the bottom of the page.
9. To return to the Management Portal, click **Back to Management Portal** from the bottom of the list in the left pane.

3.2.4 Configure %Service_WebGateway to Require Password Authentication

Now that the Gateway is configured to provide a username and password and you have given the CSPSystem user the necessary level of privilege, the next step is to configure the service that manages web applications (`%Service_WebGateway`) so that it requires password authentication. The procedure is:

1. From the Management Portal home page, go to the **Services** page (**System Administration** > **Security** > **Services**).
2. On the **Services** page, click **%Service_WebGateway**. This displays the **Edit Service** page for `%Service_WebGateway`.
3. On the **Edit Service** page, under **Allowed Authentication Methods**, make sure that **Unauthenticated** access is disabled and that **Password** access is enabled (also known as “Instance Authentication”). Click **Save**.

3.2.5 Remove the Public Status of the %Service_WebGateway:Use Privilege

With `%Service_WebGateway` requiring password authentication and the Gateway able to authenticate with an appropriately authorized user, the next step is to exclude `%Service_WebGateway:Use` from public availability. The procedure is:

1. From the Management Portal home page, go to the **Resources** page (**System Administration** > **Security** > **Resources**).
2. On the **Resources** page, in the row for `%Service_WebGateway`, click **Edit**. This displays the **Edit Resource** page for `%Service_WebGateway`.
3. In the **Public Permission** section, clear the **Use** box. Click **Save**.

Important: Once `%Service_WebGateway:Use` is not a public privilege, only those users who have been explicitly granted it will be able to use web applications. You may need to assemble a list of these users and grant them this privilege through other means.

3.2.6 Configure the Management Portal to Accept Password Authentication Only

Once the connection between the Gateway and the InterSystems IRIS server has a new authentication mechanism, the next task is to configure the Management Portal application to use a matching mechanism. In this example, this mechanism is Instance Authentication. The procedure for changing the Portal’s authentication mechanism is:

1. From the Management Portal home page, go to the **Web Applications** page (**System Administration** > **Security** > **Applications** > **Web Applications**).
2. On the **Web Applications** page, the /csp/sys application represents the Management Portal home page. Click the name **/csp/sys** in this row to edit the application. This displays the **Edit Web Application** page for the /csp/sys application.
3. In the **Security Settings** section, under **Allowed Authentication Methods**, disable **Unauthenticated** access and enable **Password** access. Click **Save**.
4. Also disable **Unauthenticated** access and enable **Password** access for all the applications that compose the other pages and choices of the Portal. These applications are:
   - /csp/sys/exp
   - /csp/sys/mgr
   - /csp/sys/op
   - /csp/sys/sec

   Note: After editing the application /csp/sys/op, you will need to authenticate to make further changes.

This configures the Portal to require password authentication (also known as “Instance Authentication”) and not to allow unauthenticated access, and so that all its parts behave consistently. The next step is to ensure that all relevant users have appropriate access to the Portal.

3.2.7 Specify the Appropriate Privilege Level for the Instance’s Users

When the Portal is configured to accept unauthenticated connections, any user can connect as the UnknownUser. Because a minimal-security installation makes UnknownUser a member of the **`%All`** role, there is no danger of being locked out of the Portal. Now that the Portal requires password authentication, its legitimate users need to be members of the **`%Operator`** role, the **`%Manager`** role, or the **`%All`** role.

In a minimal-security installation, SuperUser, Admin, _SYSTEM, and UnknownUser all have this level of privilege; further, these all have passwords of “SYS”.

Note: In a normal or locked-down installation, the UnknownUser is enabled, but is not assigned any roles.

In a normal or locked-down installation, passwords are set in the installation process, but you can choose to change them again here.

To properly secure users, the procedure is:

1. Either disable UnknownUser or remove UnknownUser from the **`%All`** role.
   - To disable UnknownUser, the procedure is:
     a. On the Users page (**System Administration** > **Security** > **Users**), click **UnknownUser** under the **Name** column. This displays the **Edit User** page for UnknownUser.
     b. Clear the **User Enabled** field and click **Save**.

- To remove UnknownUser from the `%All` role:
    a. On the **Users** page (**System Administration** > **Security** > **Users**), click **UnknownUser** under the **Name** column. This displays the **Edit User** page for UnknownUser.
    b. Go to the **Roles** tab on the **Edit User** page.
    c. In the **User UnknownUser is Assigned to the Following Roles** table, on the `%All` row, and click **Remove**.

Important: Limiting access through UnknownUser can have widespread effects, particularly if an instance's users are not sufficiently privileged.

2. Ensure that any other potentially unauthorized users are not members of `%All`, `%Developer`, `%Manager`, `%Operator`, `%SQL`, or any user-defined role that grants privileges. This involves a process analogous to removing UnknownUser from the `%All` role.

   (A user-defined role that grants privileges might have Use permission on any of the `%Admin...` resources, `%Development`, or any of the `%Service` or `%System` resources, or Write permission on `%DB_IRISLIB` or `%DB_IRISSYS`.)

3. Ensure that any user who *should* have access to the Portal is assigned to `%All`, `%Developer`, `%Manager`, `%Operator`, `%SQL`, or any user-defined role that grants Portal access. The procedure, for each of these users, is:
    a. On the **Users** page (**System Administration** > **Security** > **Users**), click the name of the user under the **Name** column. This displays the **Edit User** page for that user.
    b. Go to the **Roles** tab on the **Edit User** page.
    c. Move the desired role(s) from the **Available** to the **Selected** list by selecting the role, clicking the right arrow button, and then clicking **Assign** to assign the user to the role(s).

4. Change the passwords for SuperUser and Admin users from the default and disable the accounts. To do this:
    a. On the **Users** page (**System Administration** > **Security** > **Users**), click the name of the user under the **Name** column. This displays the **Edit User** page for that user.
    b. Click **Enter new password**.
    c. Enter the new password in the **Password** field.
    d. Confirm it in the **Password (confirm)** field.
    e. Clear the selection for **User enabled** and click **Save**.

   Note: InterSystems IRIS requires at least one enabled account with the `%All` role. InterSystems recommends creating a unique user with the `%All` role and disabling the SuperUser, Admin, and _SYSTEM users.

Important: Make sure that you know the password for at least one user who administers the Portal. Otherwise, you may lock yourself out of the Portal and have to log in using emergency access so that you can reset one or more passwords using the **^SECURITY** routine.

3.2.8 Make the Class Documentation Available

Once you finish configuring the service, the Web Gateway, and the Portal application, you may wish to ensure that the class documentation program is available. The procedure is:

1. From the Management Portal home page, go to the **Web Applications** page (**System Administration** > **Security** > **Applications** > **Web Applications**).

2. To make the documentation available:
    1. On the **Web Applications** page, the /csp/documatic application represents the class reference application. Click **/csp/documatic** in this row to edit the application. This displays the **Edit Web Application** page for the /csp/documatic application.
    2. In the **Security Settings** section, under **Allowed Authentication Methods**, disable **Unauthenticated** access and enable **Password** access. Click **Save**.

       Note: In a normal installation, password access is already enabled.

If you do not perform this procedure, the service requires a password prompt but the application attempts to use unauthenticated access. This prevents all users — including those assigned to **%All** — from reaching the documentation.

3.2.9 Begin Enforcement of New Policies

At this point, the InterSystems IRIS instance is fully configured to operate properly. However, all existing connections are still using unauthenticated access. To begin enforcement of the new policies, the following events must occur:

- The Web Gateway must establish an authenticated connection.
- All users must also establish authenticated connections.

3.2.9.1 Establish an Authenticated Web Gateway Connection

To force the Web Gateway to establish an authenticated connection, the procedure is:

1. From the Management Portal home page, select **System Administration** > **Configuration** > **Web Gateway Management**. This displays the **Web Gateway Management** page.
2. On the **Web Gateway Management** page, select **Close Connections** from the list on the left side. This displays the **Close Connections** frame.
3. Click **Close Connection(s)**. This displays a message indicating that all connections between the Gateway and InterSystems IRIS server have been closed.

The next time that a user requests a page, the Gateway will reestablish a connection to the InterSystems IRIS server. This connection will use the selected authentication mechanism.

3.2.9.2 Establish Authenticated User Connections

At this point, all connections to the Management Portal are still using unauthenticated access. If there is no pressing need to require authenticated access, then there is nothing else to do. Users will gradually end their connections to the Portal and will have to authenticate when they reconnect. (Connections may be ended due to machine reboots, stopping and restarting browsers, clearing browser caches, Portal logouts, etc.)

If there is a need to force connections to use authenticated access, you can stop and restart InterSystems IRIS. For example, on Windows, if you have InterSystems IRIS available through the default Start menu page:

1. From the Windows Start menu, select **Programs** > **InterSystems IRIS**, then the InterSystems IRIS instance to restart.
2. On the submenu for the instance of InterSystems IRIS, choose **Stop InterSystems**.
3. On the dialog that appears, select **Restart** and click **OK**.

Note: If you are using a production instance of InterSystems IRIS, you may want to choose a low-traffic time for the restart, since users will temporarily not have access to either InterSystems IRIS as a whole or the Portal.

3.3 Limit the Number of Public Resources

Any resource can be specified as a public resource. This means that any user has the ability to read, write, or use the resource, depending on its public settings. The following should always be public:

Table 3–1: Required Public Resources and Their Permissions

Resource	Permission
`%DB_IRISLOCALDATA`	R
`%DB_IRISLIB`	R
`%DB_IRISTEMP`	RW

To tighten the security of an instance, limit the number of public resources. To do this, the procedure is:

1. Ensure that all users who genuinely require access to these resources have been given privileges for them.

   Important: If you do not provide privileges for `%Service_WebGateway:Use` to the appropriate users, then this procedure can result in a widespread lockout from the Management Portal and other web applications.

2. From the Management Portal home page, go to the **Resources** page (**System Administration** > **Security** > **Resources**).
3. On the **Resources** page, each resource for which there is one or more public permissions has those permissions listed in the **Public Permissions** column of the table of resources. Select the resource by clicking **Edit**. This displays the resource’s **Edit Resource** page.
4. On the **Edit Resource** page, clear any checked **Public Permission** fields and click **Save**. The resource is no longer public.

Perform this procedure for all public resources.

3.4 Restrict Access to Services

There are various pathways by which users can interact with InterSystems IRIS. Services regulate access to these pathways. To limit access to InterSystems services, the available choices are:

- Limit the number of enabled services to only those required for the applications in use
- Limit the number of public services to only those required for the applications in use
- Restrict access to services by IP address or machine name

3.4.1 Limit the Number of Enabled Services

To limit the number of enabled services, the procedure is:

1. Determine the required services for the InterSystems IRIS instance. Typically, these are:
   - Whatever service is required for each form of user access
   - Whatever services are required for any automated access

  - Either `%Service_Console` (on Windows) or `%Service_Terminal` (on UNIX®), for local programmer-mode access

2. From the Management Portal home page, go to the **Services** page (**System Administration** > **Security** > **Services**).
3. On the **Services** page, for each service that is not required, select the service by clicking on its name. This displays the service’s **Edit Service** page.
4. On the **Edit Service** page, clear the **Service Enabled** field and click **Save**. The service is now disabled.

Once you have disabled all unnecessary services, the only pathways to InterSystems IRIS are the required services.

3.4.2 Limit the Number of Public Services

Each service is associated with a resource. In most cases, the resource has the same name as the service, such as `%Service_WebGateway`; the exception to this is the `%Service_Bindings` service, which is associated with the `%Service_Object` and `%Service_SQL` resources. Services are public because of the settings for the resources associated with them. Because of this, the procedure for making a service non-public is the same as for making any other resource non-public. This is described in Limiting the Number of Public Resources.

3.4.3 Restrict Access to Services by IP Address or Machine Name

For certain services, you have the option of restricting access to the service according to IP address or machine name. This is known as the ability to limit “allowed incoming connections.” The services that support this feature are:

- `%Service_Bindings`
- `%Service_CacheDirect`
- `%Service_ECP`
- `%Service_Monitor`
- `%Service_Shadow`
- `%Service_WebGateway`

By default, a service accepts connections from all machines. If a service has no associated addresses or machine names, then it accepts connections from any machine. If one or more addresses or machine names are specified from which a service accepts connections, then the service only accepts connections from these machines.

This feature is not available for `%Service_CallIn`, `%Service_ComPort`, `%Service_Console`, `%Service_DataCheck`, `%Service_Login`, `%Service_Mirror`, `%Service_Telnet`, and `%Service_Terminal`.

To restrict access to a service by IP address, the procedure is:

1. Determine the IP addresses of those machines with legitimate access to the service.
2. From the Management Portal home page, go to the **Services** page (**System Administration** > **Security** > **Services**).
3. On the **Services** page, for each service for which you are restricting access by IP address, select the service by clicking on its name. This displays the service’s **Edit Service** page.
4. On the **Edit Service** page, in the Allowed Incoming Connections section, click **Add New**.
5. In the displayed dialog, enter an IP address for an allowed incoming connection. Click **OK**.
6. Click **Add New** and enter other addresses as needed.

Perform this procedure for each service that is restricting the IP addresses from which it accepts connections.

3.5 Limit Remote Privileged Access

InterSystems IRIS supports ECP remote job requests. However, a remote job runs as root on the server, which could allow a user to operate on the server with more privileges than intended. To disable handling of remote jobs and limit remote privileged access on the server, follow the procedure in Changing This Parameter to set **`netjob`** to `false`. This setting is `true` by default.

3.6 Limit the Number of Privileged Users

Every instance of InterSystems IRIS must have at least one user who is assigned to the **`%All`** role. In fact, if there is only one user assigned to this role, then InterSystems IRIS prevents the user from being removed from the role. However, over time, an instance can end up having more users assigned to **`%All`** than are necessary. This can arise from assigned users leaving an organization but their accounts not being disabled, from temporary assignments not being revoked, and so on.

Along with the **`%All`** role, the system-defined roles of **`%Manager`**, **`%Developer`**, **`%Operator`**, and **`%SQL`** can give users undue privilege. There also may be user-defined roles that do this. Users assigned to such roles are sometimes known as "privileged users."

To limit the number of privileged users, determine which users are assigned to each privileged role and remove those who are not needed. The procedure is:

1. From the Management Portal home page, go to the **Roles** page (**System Administration** > **Security** > **Roles**).
2. On the **Roles** page, click the name of the role. This displays the **Edit Role** page for that role.
3. On the **Edit Role** page, click the **Members** tab, which displays a list of the users and roles assigned to the role.
4. To remove any user from the specified role, click **Remove** on the row for the user or role to be removed.

Perform this procedure for each privileged role, including **`%All`** and the others listed previously. It is also important to disable the _SYSTEM user; the procedure for this is described in Disabling the _SYSTEM User.

Important: Certain seemingly non-privileged roles may have what could be called "privileges by proxy." This occurs when a seemingly non-privileged role is assigned to a privileged role. In this case, any user who is assigned to role with privileges by proxy holds all the privileges associated with the privileged role.

Avoid creating privileges by proxy whenever possible. When not possible, have as few users as possible assigned to the roles with privileges by proxy.

3.7 Disable the _SYSTEM User

The InterSystems IRIS installation program creates the _SYSTEM user. This user is created in accordance with the SQL standard as the SQL root user. In a minimal-security installation, the default password for this user is "SYS"; in normal and locked-down installations, the default password is whatever was selected during the installation process. Because this user and the password of "SYS" are both publicly specified by the SQL standard, and because of this user's SQL privileges, disabling _SYSTEM is important for tightening access to an InterSystems IRIS instance.

To do this, the procedure is:

1. From the Management Portal home page, go to the **Users** page (**System Administration** > **Security** > **Users**)).

2. On the **Users** page, click the name **_SYSTEM** to open the **Edit User** page for _SYSTEM.
3. On the **Edit User** page for _SYSTEM, clear the **User Enabled** field. Click **Save**.

Note: If you need to check root-level SQL privileges after disabling _SYSTEM, you will have to temporarily enable the user to perform the required action.

3.8 Restrict Access for UnknownUser

In instances that support unauthenticated access, connections that do not use authentication are established with the UnknownUser account. In minimal-security installations, the default behavior is that:

- All connections use UnknownUser.
- UnknownUser is assigned to the `%All` role.
- UnknownUser holds all SQL privileges.

To restrict access for UnknownUser, disable unauthenticated access for all enabled services. (Other actions may not be effective or may result in a lockout from the Management Portal.)

Note: If you have performed all of the previous actions listed in this section, you may have already disabled UnknownUser and limited the number of public resources.

3.8.1 Potential Lockout Issue with the UnknownUser Account

If an instance has been installed with Minimal security, UnknownUser has the `%All` role; the instance also has unauthenticated access available for all services and applications. If you simply change the user’s role (from `%All` to something else) and still allow unauthenticated access, you may be unable to use basic features.

This is because, under these conditions, InterSystems IRIS establishes a connection to the selected tool without performing authentication. When there is no authentication, the system automatically sets the user account to UnknownUser. The next step is to check user privileges. If UnknownUser has insufficient privileges, access to the tool is limited or not available. For example, under these circumstances, the Terminal displays an “Access Denied” message and then shuts down; the Portal displays its main page, but no options can be selected.

To correct this condition:

1. Start InterSystems IRIS in emergency access mode.
2. Restore sufficient privileges to the UnknownUser account.

If you wish to prevent use of UnknownUser, you must upgrade the authentication mechanism for the Management Portal.

3.9 Configure Third-Party Software

InterSystems products often run alongside and interact with non-InterSystems tools, including virus scanners. For important information about the effects these interactions can have, see Configuring Third-Party Software to Work in Conjunction with InterSystems Products.

4

Security Advisor

To assist system managers in securing an InterSystems IRIS system, the InterSystems IRIS Management Portal includes a tool called the Security Advisor. This is a web page that shows current information related to security in the system configuration. It recommends changes or areas for review, and provides links to other pages in the Management Portal so that you can make the recommended changes.

Important: The Security Advisor provides general recommendations, but does not have any knowledge of an instance's needs or requirements. It is important to remember that each InterSystems IRIS instance has its own requirements and constraints, so that issues listed in the Security Advisor may not be relevant for your instance; at the same time, the Security Advisor may not list issues that are of high importance for you. For example, the Security Advisor exclusively recommends that services use Kerberos authentication, but, depending on your circumstances, authentication through the operating system, Instance Authentication, or even unauthenticated access may be appropriate.

There are some general features in the Security Advisor:

- **Details** button — Each section has a **Details** button. Selecting this button displays the page for managing that aspect of InterSystems IRIS regulated by the section.
- **Name** button — Each named item in each section is a link. Selecting one of these items displays the page for managing that item.
- **Ignore** check box — Each named item in each section has an associated **Ignore** check box. If you have determined that the item does not apply to your specific requirements, selecting this box grays out the line for the specified item. The line does not appear if InterSystems IRIS is set up according to the Security Advisor's recommendations, whether or not the **Ignore** check box is selected.

4.1 Auditing

This section displays recommendations on auditing itself and on particular audit events:

- Auditing should be enabled — Auditing creates a record that can provide forensic information after any notable or unusual system events.
- Auditing for this event type should be enabled — Auditing particular events can provide more specific information about various topics. Specifically, since the events noted when not enabled are:
  - The DirectMode event — Auditing this event can provide information about connections to InterSystems IRIS that give users significant privileges.

  - The Login event — Auditing this event can provide information questionable logins.
  - The LoginFailure event — Auditing this event can provide information about attempts to gain inappropriate access to the system.

4.2 Services

This section displays recommendations on InterSystems services. For each service, depending on its settings, the Security Advisor may address any of the following issues:

- Ability to set % globals should be turned off — Since % globals often hold system information, allowing users to manipulate these globals can result in serious, pervasive, and unpredictable effects.
- Unauthenticated should be off — Unauthenticated connections give all users, including the unidentified UnknownUser account, unregulated access to InterSystems IRIS through the service.
- Service should be disabled unless required — Access through any service monitored by the Security Advisor can provide an undue level of system access.
- Service should use Kerberos authentication — Access through any other authentication mechanism does not provide the maximum level of security protection.
- Service should have client IP addresses assigned — By limiting the number of IP addresses from which connections are accepted, InterSystems IRIS may be able to more tightly oversee the connections to it.
- Service is Public — Public services give all users, including the unidentified **`UnknownUser`** account, unregulated access to InterSystems IRIS through the service.

4.3 Roles

This section displays recommendations for all roles that hold possibly undue privileges; other roles are not listed. For each role, the Security Advisor may address any of the following issues:

- This role holds privileges on the Audit database — Read access to the Audit database may expose audited data inappropriately; Write access to the Audit database may allow the inappropriate insertion of data into that database.
- This role holds the **`%Admin_Secure`** privilege — This privilege can allow for the establishing, modifying, and denying access of users to assets; it also allows the modification of other security-related features.
- This role holds Write privilege on the %IRISSYS database — Write access to the %IRISSYS database may allow the compromise of system code and data.

4.4 Users

This section displays recommendations related to users generally and for individual user accounts. In this area, the Security Advisor may address any of the following issues:

- At least 2 and at most 5 users should have the **`%All`** role — Too few users holding **`%All`** can lead to access problems in an emergency; too many users holding it can open the system to compromise

- This user holds the %All role — Explicitly announcing which users hold **`%All`** can help eliminate any who hold it unnecessarily.
- UnknownUser account should not have the **`%All`** role — A system cannot be properly secured if anonymous users have all privileges. While this is part of any instance with a Minimal security level, such an instance is not properly secured by design.
- Account has never been used — Unused accounts provide an attractive point of entry for those attempting to gain unauthorized access.
- Account appears dormant and should be disabled — Dormant accounts (those that have not been used for over 30 days) provide an attractive point of entry for those attempting to gain unauthorized access.
- Password should be changed from default password — This is a commonly attempted point of entry for those attempting to gain unauthorized access.

4.5 Web, Privileged Routine, and Client Applications

Each application type has its own section, which makes it simpler to review details for each application type. These sections display recommendations related to access to and privileges granted by applications. In this area, the Security Advisor notes the following issues:

- Application is Public — Public applications give all users, including the unidentified **`UnknownUser`** account, unregulated access to the data associated with the application and actions that the application supports. This is even more notable if the application also grants the **`%All`** role, either conditionally or absolutely.
- Application conditionally grants the **`%All`** role — A system cannot be properly secured if users have the possibility of holding all privileges. This is even more notable if the application is also public.
- Application grants the **`%All`** role — A system cannot be properly secured if users have all privileges. This is even more notable if the application is also public.

5

Secure InterSystems Processes and Operating-System Resources

5.1 Introduction

This document describes how to reduce the potential attack surface available to an intruder by hardening the operating system on which an instance of an InterSystems IRIS® data platform runs. Topics include:

- The operating system services that an InterSystems IRIS instance requires
- The various types of InterSystems IRIS processes, along with the purpose of each
- Methods for identifying the function of InterSystems IRIS processes in a running instance
- How to remove or disable optional InterSystems IRIS processes that your site may not need
- Processes required by an instance that is running, in addition to either the iris process on UNIX® or the irisdb.exe process on Windows
- The TCP and UDP ports for InterSystems IRIS processes, along with the purpose of each

5.2 InterSystems IRIS Processes

Most processes comprising an InterSystems IRIS instance use the iris executable on UNIX® and the irisdb.exe executable on Windows, and each of these files resides in the bin directory under the installation directory. A running instance uses a number of system processes to coordinate and support the processes running user code. InterSystems IRIS processes can be examined in the Management Portal under **System Operation** > **Processes**.

5.2.1 Core Processes

Core system processes are started early in the initialization of an instance and have no value in the **User** column. You can identify these processes by the value in the **Routine** column which, in the case of system processes, does not always contain the name of an InterSystems IRIS routine. The **Routine** column lists the following core system processes by name:

- CONTROL — Creates and initializes shared memory and provides various control functions.
- WRTDMN — Performs all writes to databases and WIJ (the write daemon).

- GARCOL — Garbage collects large kills.
- JRNDMN — Performs journal writes.
- EXPDMN — Performs database expansions.
- AUXWD — Performs write daemon tasks (write daemon auxiliary workers).
- MONITOR — Writes alerts to the alert file and transmits email alerts.
- CLNDMN — Detects dead processes and cleans up stranded resources.
- RECEIVE — Manages ECP worker processes.
- ECPWork — Performs ECP tasks (ECP worker process).
- %SYS.SERVER — Accepts TCP requests and dispatches workers to serve them (the superserver process).
- %CSP.Daemon — Manages expiration of web sessions.
- LMFMON — Monitors the InterSystems IRIS license and sends usage data to the license server over UDP.
- %SYS.Monitor.xxx — Performs system monitor tasks (various system monitor workers).
- SYS.Monitor.xxx — Writes alerts to alert file and transmits email alerts.

Do not stop the core system processes. Doing so disrupts the normal operation of an InterSystems IRIS instance.

A number of other InterSystems IRIS system processes are started after the core system processes. Many are started dynamically. These processes have a value displayed in the User column. Many of them are optional and are not started unless needed or configured. These processes can usually be identified by the values of the **Routine**, **User**, and **Client EXE** columns of the process display.

The task manager process (TASKMGR) is created during instance startup. It starts various scheduled system and user defined tasks and runs with the settings:

- Username = TASKMGR
- Routine = %SYS.TaskSuper.1
- Operating System Username = TASKMGR

If you are not using ECP, you can prevent the ECPWork process from being started:

1. From the Management Portal, select **System Administration** > **Configuration** > **Connectivity** > **ECP settings** and set the maximum number of application and data servers to zero.
2. Disable the ECP service.

5.2.2 ECP Server Processes

ECP server processes that are dynamically started have a routine name beginning with “ECP”. The user name or Operating System Username is usually **`Daemon`** or **`%System`**, but it may be the name of the Instance Service user on Windows. Examples of process names follow:

- ECPCliR – ECP client reader
- ECPCliW – ECP client writer
- ECPSrvR – ECP server reader
- ECPSrvW – ECP server writer

5.2.3 Web Server Processes

Web server processes are dynamically started. They will display CSPSystem in the **User** column when they are idle and waiting for a task. When they are active, they will display the InterSystems IRIS user for the web session and the current routine name. The **OS Username** column will display **Web Gateway**.

- %SYS.cspServer and %SYS.cspServer2 – Webserver routines that processes use to handle web application requests.
- %SYS.cspServer3 – Webserver routine that processes use to handle asynchronous communication and Web Gateway management.

These processes are associated with legacy applications from other InterSystems products. For more details on these routines in those applications, see the question about them in the FAQ for this feature.

Note: These routines do not consume licenses. Licenses are associated with web application sessions.

For each of these servers, on Windows the executable is CSPAP.dll; on UNIX®, it is CSPap.so. The operating system username is `Web Gateway`. The program name may change as the process changes tasks.

5.2.4 Mirroring System Processes

Mirror system processes are started if mirroring is configured. They perform various functions related to mirroring.

- MIRRORMGR – Mirror Master. The User is the description of the mirror function performed: `Mirror Master`, `Mirror Primary`, `Mirror Dejournal`, `Mirror Prefetch`, or `Mirror JrnRead`. The operating system username is `Daemon`. No TCP port is open. The device is the operating system null device.
- MIRRORCOMM – Mirror communication process. The username is `Mirror Arbiter`, `Mirror Backup`, or `Mirror Svr:RdDmn`. The operating system username is `Daemon`. The device is `|TCP|XXX`. The TCP port can be determined from the Device name or the Mirror configuration.

5.3 IP Protocols

5.3.1 TCP

An InterSystems IRIS instance accepts connections on TCP/IP ports specified by configuration options. Any Operating System restrictions on usage of ports, for example with a fire wall, require port settings to allow inbound access that are consistent with the ports configured for InterSystems IRIS. If the firewall defines rules for executables, as it does on Windows, you may need to grant permission to programs as well, for example, the irisdb.exe, licmanager.exe, ISCAgent.exe, and the httpd.exe executables will require such permissions.

TCP/IP ports used by InterSystems IRIS are defined by the instance configuration. The configured ports can be examined in the `iris.cpf` file in the installation directory. The `[Startup]` section configures `DefaultPort`, `DefaultPortBindAddress` and `WebServerPort`. `DefaultPort` specifies the port on which the superserver accepts connections; the default value is 1972. `DefaultPortBindAddress` optionally specifies an interface address the superserver binds to. `WebServerPort` specifies the port on which the private web server accepts connections; the default value is 52773.

The private web server is mostly used in development environments and is not recommended for production environments.

The `[SQL]` section contains `JDBCGatewayPort` which defines the Java Database Connectivity (JDBC) gateway port number. Its default value is 62972.

The `[Telnet]` section contains a `Port` value to specify the port on which the InterSystems Telnet service (ctelnetd.exe) accepts Telnet connections to InterSystems IRIS on Windows.

5.3.2 UDP

InterSystems IRIS and the license server (licmanager or licmanager.exe) communicate primarily using the UDP protocol. InterSystems IRIS sends messages as UDP packets to the license server port. This port is 4002 by default, and is configured in the Management Portal > System Administration > Licensing > License Servers. The license server replies to InterSystems IRIS at the port that InterSystems IRIS used to send the original message (it looks up the port in the packet header). TCP is only used between InterSystems IRIS and the license server during a query request. InterSystems IRIS opens a TCP port for accept/listen and sends this port number in the query request. The license server connects back to that port and sends the results over the TCP connection. The port number is the license server port; if this fails, it uses port 0 which signals the operating system to select a free port at random. The port is open only during transmission of the query results.

5.3.3 SNMP

The %System_Monitor Service enables InterSystems IRIS to act as a subagent to an SNMP Agent on the managed system. This supports both SNMP requests (GET or GETNEXT) for InterSystems IRIS management and monitoring data (as defined in the supplied MIBs), and SNMP Traps (asynchronous notifications sent by InterSystems IRIS). Disabling the %System_Monitor service will disable all communication between InterSystems IRIS and the SNMP Agent on the local system, and consequently with any remote SNMP manager applications.

5.3.4 HTTP

Refer to the description of the components of the Web Gateway used by InterSystems IRIS to serve HTTP requests by navigating through the online documentation as follows: Documentation > InterSystems IRIS Web Development > Web Gateway Guide > Introduction to the Web Gateway. The private Web Server is httpd.exe (httpd on UNIX®) located in the httpd\bin subdirectory under the installation directory. Startup of the private web server is controlled by the Management Portal > System Administration > Configuration > Additional Settings > Startup > WebServer set to true or false.

5.3.5 Gateways

InterSystems IRIS provides a number of Gateways to external data. These include SQL Gateway, JDBC Gateway, Object Gateways, and XSLT 2.0 Gateway servers. The TCP/IP ports used are defined using the gateway setup pages accessed via the Management Portal > System Administration > Configuration > Connectivity. See the documentation of these gateways for an explanation of Operating System services or processes on which they depend.

5.4 Remove Unneeded InterSystems IRIS Processes

InterSystems service processes are not created unless the services they support are enabled and configured. There is no need to take any additional action to prevent InterSystems service processes from running.

5.5 External Processes

An InterSystems IRIS instance will start processes running executables other than iris[.exe] to perform a number of functions in support of the instance. Instance specific versions of these executables, which are generally specific to the instance version, live in the bin subdirectory of the installation directory. Executables that may be shared by multiple InterSystems IRIS instances live in a common directory.

Persistent processes may be running the following executables, which live in the bin directory on Windows.

- irisdb.exe — The InterSystems IRIS executable.
- licmanager.exe — The InterSystems IRIS license server.
- CStudio.exe — Studio.
- iristray.exe — The InterSystems IRIS launcher in the system tray.
- Iristerm.exe — The Terminal.
- iristrmd.exe — The local Terminal connection daemon. Accepts local Terminal connections (not Telnet) and creates InterSystems IRIS server processes to serve the connection.
- irisirdimj.exe — Executable that processes the WIJ file during InterSystems IRIS startup and shutdown.

Persistent processes may be running the following executables, which live in the bin directory on UNIX®.

- iris — The InterSystems IRIS executable.
- licmanager — The InterSystems IRIS license server
- irisirdimj — Processes the WIJ file during InterSystems IRIS startup and shutdown.

Other programs in the bin directory are used from time to time, but the processes are short running and unlikely to be displayed by a process listing for long.

Executable binaries shared by InterSystems IRIS instances reside in subdirectories of C:\Program Files (x86)\Common Files\InterSystems on Windows. The processes may be seen running these executable binaries from the common directory on Windows.

- ISCAgent.exe – Controls mirror failover.
- Iristerm.exe – The Terminal.

Shared binaries are usually installed in /usr/local/etc/irissys on UNIX®.

- ISCAgent* - Controls mirror failover.

In addition to executable binaries, a number of shared library binaries are stored in the common directory.

5.6 Interoperability

5.6.1 Adapters

InterSystems IRIS provides communication with external interfaces using adapters.

5.6.1.1 Email

Email adapters are InterSystems IRIS processes. They use TCP/IP to send/receive email from an email server. Outbound adapters send mail to a SMTP server. Inbound adapters poll for relevant (filtered) messages from a POP3 serve. Email servers are likely to be on a remote server, so while there would be no local process, the remote system would need to be reachable through a firewall

5.6.1.2 File

File Input Adapters are InterSystems IRIS processes. They periodically inspect a directory they have been configured to monitor, read files that appear there, pass the files to the Business Service they have been configured to support, and move the files to the configured archive directory. The EnsLib.File.InboundAdapter class provides the implementation. The *FilePath*, *WorkPath*, and *ArchivePath* properties define the input, temporary work, and archive directories, respectively.

File Output Adapters are employed by production Business Operations to write data to files. The file path and file name are specified by the Business Operation and operations on the file are invoked by calling methods of the EnsLib.File.OutboundAdapter class. Messages are usually queued to a worker job that performs the actual output operation. This implies the existence of Ens.Queue processes.

5.6.1.3 FTP

InterSystems IRIS acts as a client for FTP communication with remote FTP servers using the %Net.FtpSession class. The %Net.FtpSession class can be configured to use PASV for the data channel to avoid an inbound connection. InterSystems IRIS provides FTP inbound and outbound adapters. Both act as FTP clients to get (input) or put (output) under the control of a Business Service created by the customer. The FTP server and port are configurable. The FTP adapters are InterSystems IRIS processes.

5.6.1.4 HTTP

The HTTP adapters (EnsLib.HTTP.InboundAdapter and EnsLib.HTTP.OutboundAdapter) enable productions to send and receive HTTP requests and responses. HTTP adapters are implemented by InterSystems IRIS processes. The port and interface IP addresses of the inbound HTTP adapter are configurable. The server and port to which the outbound HTTP adapter is provided by class settings.

5.6.1.5 Java Gateway

Production adapters use the Java Gateway to communicate through a Java intermediary process. A Java process is started which depends on the existence of a Java Virtual Machine. The InterSystems IRIS server process communicates with the Java process via a TCP connection. The TCP ports used are configurable.

5.6.1.6 LDAP

The EnsLib.LDAP.OutboundAdapter class can be used like other adapters by Business Services to send requests to an LDAP server and receive responses.

5.6.1.7 MQSeries

The classes EnsLib.MQSeries.InboundAdapter and EnsLib.MQSeries.OutboundAdapter enable productions to retrieve messages from and send messages to message queues of IBM WebSphere MQ. Dynamically loaded shared library binaries are used for the communication.

5.6.1.8 Pipe

The classes EnsLib.Pipe.InboundAdapter and EnsLib.Pipe.OutboundAdapter enable productions to invoke operating system commands or shell scripts. They create a process external to InterSystems IRIS and communicate with it via a pipe, so an external process will exist while the Pipe adapter is communicating with it. The command that the process runs is determined by the value assigned to the *CommandLine* property of the adapter class.

5.6.1.9 SAP

The Java Gateway is used to communicate with the SAP Java Connector using classes imported with the EnlLib.SAP.BootStrap class ImportSAP method.

5.6.1.10 SQL

The SQL inbound and outbound adapters enable productions to communicate with JDBC or ODBC-compliant databases. In general, the inbound SQL adapter (EnsLib.SQL.InboundAdapter) periodically executes a query and then iterates through the rows of the result set, passing one row at a time to the associated business service. The SQL adapters use the underlying capabilities of InterSystems SQL and JDBC Gateways.

5.6.1.11 TCP

InterSystems IRIS provides input and output TCP adapters. Each TCP inbound adapter checks for data on a specified port, reads the input, and sends the input as a stream to the associated business service. Within a production, an outbound TCP adapter is associated with a business operation that you create and configure. The business operation receives a message from within the production, looks up the message type, and executes the appropriate method in the outbound TCP adapter to transmit the data over TCP.

5.6.1.12 Telnet

InterSystems IRIS provides the EnsLib.Telnet.OutboundAdapter which permits outbound telnet connections to the telnet facility on another system. This adapter provides methods to programmatically emulate the effect of manually logging in to the remote system using telnet client software. The InterSystems IRIS TCP device is the underlying technology.

6

Checklist for Hardening Your Deployment

This checklist is intended to provide your organization with guidelines for assessing how secure your environment is and to provide tips for hardening your environment that will help your organization avoid and prevent security breaches. This checklist is not intended to be a “how to list” and is not all-inclusive. The points below are items to consider rather than a definitive list of rules to apply.

You alone are responsible for the security of your infrastructure. If you are uncertain about your approach to hardening and protection, consult a security professional.

6.1 Network and Firewalls

ID	Topic	Description
1.	Network, hardware, software and policies	Obtain copies of and review security polices, firewall logs, firewall configuration and patch levels, public facing IP addresses, diagrams of network, and firewall topologies.
2.	Auditing the physical environment	Ensure firewalls and management servers are in a physically secure location that can only be accessed by authorized personnel. Ensure that they are patched up to date.
3.	Reviewing change management process, rule base modifications	Review procedures and approval process for changes. Automation tools are available for this.
4.	Vulnerability testing	Run automated tools to analyze and identify unsecured services, protocols, and ports.
5.	Using brute force detection systems	Stop people from guessing passwords, and prevent them from connecting to the server, by blocking their current IP address in your server firewall.
6.	Ongoing audits and real-time monitoring and alerting	Ensure a process is in place for continuous auditing of firewalls. Ensure real-time monitoring is in place to alert on changes to the firewall. Review their logs regularly.

6.2 Operating System

ID	Topic	Description
1.	Installation planning	Understand the server role, and document the install procedure. Download appropriate operating system securing and hardening guides for more detailed information.
2.	Patch levels	Ensure operating system patches are up to date, especially security patches. Turn off automatic updates.
3.	Endpoint protection software	Install and appropriately configure this software. (Formerly listed as antivirus software.)
4.	Disabling unnecessary software, services, and ports	Disable unnecessary network services such as IPv6, telnet, and FTP. Disable unnecessary daemons that are not used such as DHCP, scheduling and queuing services, and laptop services. Configure in-use services to be as secure as possible; for example, secure SSH by limiting SSH protocol to Version 2 (Version 1 is not secure).
5.	Logs	Maintain server logs and mirror those logs to a separate log server.
6.	Monitoring and alerting	Configure monitoring and alerting settings to notify of events such as changes to the system, and unauthorized access.
7.	Physical security	Configure the BIOS to disable booting from CDs/DVDs, floppies, and external devices; set a password to protect these settings.

6.3 Web Server

ID	Topic	Description
1.	Installation planning	Understand the role of the web server: what content will it serve; will the pages be static; what web services are provided? Document the installation procedure. Download and review the appropriate hardening security guide.
2.	Patch levels	Ensure web server is up to date, especially with regard to security patches.
3.	Web server header info	Configure the servers so that HTTP headers do not provide information relating to the web server software being run, or system types and versions.
4.	Disabling HTTP TRACE	When enabled, HTTP TRACE request is used to echo back all received information.
5.	Error handling	Implement proper error handling by utilizing generic error pages and error handling logic to force the application to avoid default error pages. These often leak sensitive system and application information.
6.	Disabling modules	Disable all unused modules to reduce surface area of the web server; these modules often provide too much information – *Apache:* autoindex, cgi, imap, info, status, userdir, actions, negotiation… *IIS:* ASP, ASP.NET, WebDAV, CGI, directory browsing…
7.	Users and groups	*Apache:* Run Apache as a separate user and group so Apache processes cannot be used by other system processes. *IIS:* Remove unused accounts; disable Guest account

6.4 Users, Passwords, Groups, Ownerships, and Permissions

ID	Topic	Description
1.	User management	Disable root login. All administrators should be named users. Regularly check for unused user accounts, and for default user accounts and passwords.
2.	Password policy	Require and use very strong passwords with mixed case, numbers, and special characters. Change passwords on a regular basis. Lock accounts after too many login failures.
3.	UNIX®	Create groups and users before installation. Install InterSystems IRIS as root. Ensure groups, ownerships, and permissions for InterSystems IRIS databases are maintained as specified.
4.	Windows	Install InterSystems IRIS using the Windows Administrator, and then disable the default Windows Administrator account. Also disable Guest and Help Assistant accounts.

6.5 Encryption (Data At Rest and Data In Motion)

ID	Topic	Description
1.	Data at rest	Ensure all production data at rest on disk is encrypted.
2.	Key management	Review the key management policies and procedures.
3.	Data In motion	Ensure all HTTP data communications is encrypted, such as with TLS. Ensure that all TLS configurations are using the latest version.

6.6 InterSystems Security

ID	Topic	Description
1.	Installation	Always install with the Locked Down initial security setting type.
2.	Authentication	Regularly review users and passwords.
3.	Authorization	Review application requirements; define roles, resources, and services.
4.	Auditing	Ensure that auditing is enabled. Review the logs regularly.
5.	Disabling services	If services such as ECP and mirroring are not used, do not enable them.
6.	Removing unused databases and applications.	Remove unused databases such as USER.