HealthShare Health Connect Installation Guide

Version 2024.1
2024-05-02

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

HealthShare Health Connect Installation Guide
HealthShare Version 2024.1 2024-05-02

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

1

Installing Health Connect

To install Health Connect, follow the instructions below, depending on your situation:

- How to perform an attended installation
- How to perform an unattended installation

Important: InterSystems strongly recommends that you review the pre-installation steps relevant for your operating system. See either Windows Pre-Installation or UNIX®, Linux, and macOS Pre-Installation.

1.1 Performing an Attended Installation

1.1.1 Running the Installer on Windows

To install a new instance of Health Connect on Windows, run the installer executable as an administrator.

Before installing make sure you have enabled Microsoft IIS or a different supported web server.

For detailed information on the options below, see the Windows Installation Guide.

The installation process will prompt you for some information:

1. Choose an instance name for your installation (multiple instances can run on the same machine).
2. Choose the folder for the installation.
3. For the setup type, *Development* will be appropriate for most situations, especially if you are installing Health Connect for the first time.
4. If you are automatically configuring IIS (InterSystems recommends this method), you will be prompted with "`Local IIS web server detected.`" Choose **Configure local IIS web server for this instance**.
5. For Unicode support, select **Unicode**.
6. For security type, InterSystems recommends that you select *Normal* for a development environment or *Locked Down* for a production environment.
7. The InterSystems IRIS Service upon which Health Connect relies can run under a default SYSTEM (Windows Local System) account or under an existing Windows account. You will be prompted to choose a common password for the Health Connect administrator accounts (**_SYSTEM**, **Admin**, **SuperUser**, and the Windows account you chose, if any) on the next screen.

8. You will be prompted to enter a password for the **CSPSystem** account.
9. In the **Ready to Install the Program** dialog box, you have the option to enter your license key: click **License** to do so and follow the prompts. You can obtain a license key from your sales engineer.
10. After that, click **Install** to complete the installation.

1.1.2 Running the Installer on Linux or macOS

To install a new instance of Health Connect on Linux or macOS, follow the instructions below.

Before installing make sure you have enabled Apache or a different supported web server.

For detailed information on the options below, see the UNIX®, Linux, and macOS Installation Guide.

1. Extract the installation components from the provided tarball.
2. Navigate to the directory where you extracted the components and run the command **irisinstall** with elevated privileges.
3. Choose an instance name for your installation (multiple instances can run on the same machine).
4. Enter the name of the directory where the installation will reside. If the directory does not exist yet, it will be created.
5. For the installation type, *Development* will be appropriate for most situations, especially if you are installing Health Connect for the first time.
6. For security settings, InterSystems recommends that you select *Normal* for a development environment or *Locked Down* for a production environment.
7. At the prompt `What user should be the owner of this instance?`, enter the name of an existing user account.
8. You will then be prompted to choose a password for the Health Connect administrator accounts upon which Health Connect relies (**_SYSTEM**, **Admin**, **SuperUser**, **CSPSystem**, and the user account you chose for owner).
9. At the prompt `What group should be allowed to start and stop this instance?` enter the name of an existing group.
10. Choose to install Unicode support.
11. If you are automatically configuring the Apache web server, you will be asked if you would like to use the detected web server to connect to your installation. Enter `y` to allow automatic configuration.
12. You can then choose to supply the full pathname for your license key, which you can obtain from your sales engineer.
13. After that, your chosen options are displayed on the screen. You can confirm the installation simply by pressing Enter.

1.2 Performing an Unattended Installation

Health Connect can be installed in unattended mode.

1.2.1 Running an Unattended Installation on Windows

If you will run Health Connect on Windows, follow the instructions in Windows Unattended Installation. During that process, keep in mind the following considerations that are specific to Health Connect.

The minimum required set of parameters includes: instance name, a *fully resolved physical pathname* for the location of the installation, and the password for the SYSTEM (superadmin) account. The /qb switch is essential to running the installer in unattended mode.

The command line syntax for the minimum required set of parameters is: C:\> *installation_executable*.exe /instance *instance_name* /qb INSTALLDIR="*install_directory*" IRISUSERPASSWORD="*password*"

Important: The unattended installer differs from the Health Connect unattended installer in that a few parameters work differently. See the table below.

Parameter or Switch	Supported by Health Connect	Notes
ADDLOCAL	Y	Optional. The default installation does not include the Web Gateway libraries for external web servers, such as IIS. To install those libraries within the Health Connect installation along with all other server components, add ADDLOCAL=ALL to the command line.
INITIALSECURITY	N	Defaults to “Normal”.
CLIENTINSTALL	N	
ISCSTARTCACHE	N/A	
UNICODE	N	Do not use this option. The installer will default to Unicode support as needed by Health Connect.
REPAIR	N	
REINSTALL	N	
REMOVE	N	

1.2.1.1 Examples: Microsoft Windows Unattended Installation

C:\> *installation_executable*.exe /instance HSHCsilent /qb
INSTALLDIR="D:\InterSystems\HSHCsilent" IRISUSERPASSWORD="*password*"

Installs all available components for Health Connect.

C:\> *installation_executable*.exe /instance HSHCclient /qb
INSTALLDIR="D:\InterSystems\HSHCclient" CLIENTINSTALL=1

Installs only the client components listed in the table above. Some graphical progress indicators will be displayed.

1.2.2 Running an Unattended Installation on Linux or macOS

If you are running Health Connect on Linux or macOS, follow the instructions in UNIX®, Linux, and macOS Unattended Installation. During that process, keep in mind the following considerations that are specific to Health Connect.

The minimum required set of parameters includes: instance name, a *fully resolved physical pathname* for the location of the installation, the password for the _system (superadmin) account, and “normal” security settings.

The command line syntax for the minimum required set of parameters is: $ sudo
ISC_PACKAGE_INSTANCENAME="*instance_name*" ISC_PACKAGE_INSTALLDIR="*install_directory*"

ISC_PACKAGE_USER_PASSWORD="*password*" ISC_PACKAGE_INITIAL_SECURITY="Normal" ./irisinstall_silent.

Important: The Health Connect unattended installer differs from the InterSystems IRIS unattended installer in that a few parameters work differently. See the table below.

Parameter or Switch	Supported by Health Connect	Notes
ISC_PACKAGE_INITIAL_SECURITY	N	Defaults to “Normal”.
ISC_PACKAGE_CLIENT_COMPONENTS	N	For a client-only installation, which includes components such as language bindings and SDKs and the InterSystems engine link libraries, use the `irisinstall_client` script. For more information on installing client components only, see UNIX®, Linux, and macOS Client-only Installation
ISC_PACKAGE_STARTCACHE	N/A	
ISC_PACKAGE_UNICODE	N	Do not use this option. The installer will default to Unicode support as needed by Health Connect.

1.2.2.1 Examples: Linux or macOS Unattended Installation

```
$ sudo ISC_PACKAGE_INSTANCENAME="HSHCsilent" ISC_PACKAGE_INSTALLDIR="/hs/HSHCsilent"
ISC_PACKAGE_USER_PASSWORD="password" ISC_PACKAGE_SUPERSERVER_PORT="59992"
ISC_PACKAGE_INITIAL_SECURITY="Normal" ./irisinstall_silent
```

Installs Health Connect in “normal” security mode with Superserver port 59992.

```
$ sudo ISC_PACKAGE_INSTANCENAME="HSHCsilent" ISC_PACKAGE_INSTALLDIR="/hs/HSHCsilent"
ISC_PACKAGE_USER_PASSWORD="password" ISC_PACKAGE_INITIAL_SECURITY="Normal"
ISC_PACKAGE_MGRUSER="hshcadmin1" ISC_PACKAGE_MGRGROUP="hshcadmin"
ISC_PACKAGE_WEB_CONFIGURE="Y" ISC_PACKAGE_WEB_SERVERTYPE="Apache" ./irisinstall_silent
```

Installs all Health Connect modules; specifies the user and group who own the instance; configures the Web Gateway to work with an existing instance of Apache on the same host (installs Web Gateway libraries in `/opt/gateway` and adds Web Gateway configuration information to `httpd.conf`). Note that this configuration is appropriate only for a development instance of Health Connect, not for a production installation.

2

Post-Installation Tasks

For security purposes, you need to immediately change the password of the `HS_Services` user account that was created by the installation process. To change the password:

1. Open the Management Portal.
2. Navigate to **System Administration** > **Security** > **Users**.
3. Select `HS_Services` from the list of users.
4. Select **Enter new password**.
5. Enter the new password and confirm it.
6. Select **Save**.

3

Upgrading Health Connect

The process for upgrading Health Connect to a new major release or maintenance release is similar to upgrading the underlying InterSystems IRIS technology:

1. Read the special considerations for upgrading Health Connect listed below.
2. Complete the Upgrading InterSystems IRIS procedure in the *InterSystems IRIS Installation Guide*.
3. Return here and complete the post-upgrade steps below necessary for your situation.

Note: If you are upgrading from Health Connect 15.03 see Upgrading from Health Connect 15.03.

3.1 SSL/TLS Configuration in the Configure Secure Communication Dialog

If you are upgrading from *a version prior to 2022.2* and *your system is configured for secure communication*, meaning that you had an Active configuration in the **Configure SSL Access** option in the Installer Wizard prior to your upgrade, note that the **Configure SSL Access** dialog in the Installer Wizard has been renamed to **Configure Secure Communication**. In the new dialog you must now specify an SSL/TLS Configuration in order to make the secure communication settings Active. A default value of `HS.Secure.Demo` was entered for the SSL/TLS Configuration setting when you upgraded.

If you previously had an Active configuration in the **Configure SSL Access** option, you must modify the default value to reflect the SSL/TLS configuration in use on your instance as follows:

1. Navigate to the Installer Wizard.
2. Select the new **Configure Secure Communication** option.
3. Confirm that your **Secure Port** is identified and the **These Settings are Active** checkbox is selected.
4. In the **SSL/TLS Configuration** field, select the name of the SSL/TLS configuration in use on your instance.
5. Click **Save**.

3.2 Post-Upgrade Steps for Pre-2021.1 FHIR Endpoints

If you are upgrading from a version prior to 2021.1, the following steps that may be required depending upon on how you have customized your FHIR server. Perform these tasks in the following order:

1. If your FHIR server uses custom subclasses, you must modify your architecture subclasses.
2. If your FHIR endpoint uses custom search parameters, migrate them to a FHIR package and apply them to the endpoint.

Once you have completed these steps you can re-index the search tables.

3.2.1 Step 1: Modifying Architecture Subclasses

As part of the FHIR architecture that was introduced in Health Connect 2020.1, you can use a custom InteractionsStrategy to implement a custom FHIR server. If your FHIR server's endpoint uses a custom InteractionsStrategy, including if it uses a subclass of the Resource Repository, complete the following steps:

1. Complete the upgrade of your Health Connect instance.
2. Using your IDE, do *one* of the following in your endpoint's namespace:
   - If the InteractionsStrategy of your endpoint extended the Resource Repository (`HS.FHIRServer.Storage.Json.InteractionsStrategy`), create a subclass of `HS.FHIRServer.Storage.Json.RepoManager`.
   - If the InteractionsStrategy of your endpoint subclassed `HS.FHIRServer.API.InteractionsStrategy` directly, create a subclass of the `HS.FHIRServer.API.RepoManager` superclass.
3. Add the following parameters to your subclass of the Repo Manager:
   - `StrategyClass` — Specifies the subclass of your InteractionsStrategy.
   - `StrategyKey` — Specifies the unique identifier of the InteractionsStrategy. This must match the value of the `StrategyKey` parameter in the InteractionsStrategy subclass.
4. If your InteractionsStrategy subclass included custom code for the methods that manage the Service, you must move that logic to the new methods in the Repo Manager subclass that you created. Specifically, you must move custom code from the `Create`, `Delete`, `Decommission`, and `Update` methods to the corresponding methods in your Repo Manager subclass (`CreateService`, `DeleteService`, `DecommissionService`, and `UpdateService`).

3.2.2 Step 2: Migrating Custom Search Parameters to a FHIR Package

In earlier versions of Health Connect, using custom FHIR search parameters required you to define a custom metadata set. In this version, defining FHIR metadata, including custom search parameters, has been migrated to FHIR packages. When you upgrade from an earlier version, the upgrade will remove any custom metadata sets, and configure the FHIR endpoint with the base FHIR package, either STU3 or R4, depending on what was in use before the upgrade.

If you use custom FHIR search parameters, you must manually migrate them to a FHIR package and apply them to the endpoint before they can be used. The instructions for creating and applying FHIR packages are in the "FHIR Profiles and Adaptations" chapter of *FHIR Support in InterSystems Products*. Using the files that you originally used to used to create the custom metadata set, perform the steps below in the recommended order:

1. Create a custom FHIR package.
2. Import your package or confirm that your package has been imported.

3. Apply the custom package to your endpoint.
4. To complete this procedure, you must re-index the endpoint. You will do this in a later post-upgrade step.

Alternatively, you can perform these steps using the FHIR Package API.

3.3 Re-Indexing FHIR Search Tables

Re-index any FHIR search tables that require it:

1. In the Management Portal, navigate to **Health** > *myFHIRnamespace* > **FHIR Configuration**.
2. Select the **Server Configuration** card.
3. For each existing endpoint, select **Reindex Now**.
4. When prompted, click **Select All**, and then select **Reindex**.

   Note: This step may take some time to complete.

3.4 Validate Production Interfaces

You can validate that your upgraded system behaves the way you expect it to by using the Production Validator. The Production Validator extracts HL7 headers, messages, and operation messages to a temporary database, which is then copied to an upgraded InterSystems IRIS for Health instance and replayed. By comparing the original messages to the messages processed on the upgraded system, you can evaluate and address differences.

3.5 Upgrading from Health Connect 15.03

Health Connect 2019.1 was the first release of Health Connect that is powered by InterSystems IRIS. Because of this change in underlying technology, a special upgrade procedure is required when upgrading from a previous version of Health Connect. If you are upgrading to Health Connect 2019.1 or later from Health Connect 15.03, see the *InterSystems IRIS In-Place Conversion Guide*, which is available from the InterSystems WRC Documents page.

4

Creating a Healthcare Interoperability (Foundation) Namespace and Production Using the Installer Wizard

The Installer Wizard allows you to create a Foundation namespace and production that contains all of the mappings and libraries needed for health care interoperability. If you need to modify a Foundation namespace, for example to modify the routine database, you can use the Namespaces page (**System Administration** > **Configuration** > **System Configuration** > **Namespaces**) after you have created and activated your Foundation namespace in the Installer Wizard.

In order to create a secure and portable configuration for your Health Connect Foundation namespace and production, use the Installer Wizard to:

1. Set the Network Host Name
2. Set up Secure Communication
3. Create your Foundation namespace and production

Note: When you select the **Start All** button on pages accessed through the **Health** menu, only *Foundation* productions are started. If you open a different production in a Foundation namespace, that production will not be started.

The business host `Ens.Activity.Operation.Local` that is automatically added to a Foundation production is used for activity monitoring, and can be removed if you do not need this functionality.

4.1 Accessing the Installer Wizard

1. Log in to the Management Portal for your instance as a user with the **`%HS_Administrator`** role.
2. Click **Health** in the menu on the left.
3. Click the **Installer Wizard** link in the banner at the top of the page.

4.2 Setting the Network Host Name the Installer Wizard

HealthShare Health Connect uses the *Network_Host_Name* during configuration to generate URLs that address the various system components on a particular instance. The *Network_Host_Name* defaults to the machine's host name if you do not explicitly set it in the **Network Host Name** page in the Installer Wizard.

Important: Always set the *Network_Host_Name* before you begin configuring Health Connect.

Because the URLs based on the *Network_Host_Name* become embedded in your productions, InterSystems strongly recommends that you use a hostname that is resolved by your DNS as the value for *Network_Host_Name* rather than a machine IP address or a fully-qualified domain name that might be longer than the maximum of 50 characters. Using a DNS hostname provides the flexibility to redirect resources at the network level, making it much easier to later clone a system for testing, move a system to a new server, or restore a backup on another machine.

In a mirrored Health Connect installation, the *Network_Host_Name* should be set to the mirror VIP (or DNS entry for the mirror VIP).

To set the *Network_Host_Name*:

1. Follow the instructions to access the Installer Wizard.
2. Click **Configure Network Host Name**.
3. In the **Network Host Name** field, replace the machine's host name with a host name resolved by your DNS that refers to the machine. For a mirrored system, use the DNS entry of the mirror VIP. The maximum length for this string is 50 characters.
4. Click **Save**.

4.3 Setting Up Secure Communication for a Foundation Production

Live Health Connect systems should always use secure communication.

Note: If you set up secure communication before you create a Foundation namespace and production, then your Foundation production will automatically use the secure communication settings when you activate it.

Follow the instructions below to securely configure your Foundation namespace and production:

1. If you have not already done so, set the Network Host Name.
2. Configure your web server(s) to enable SSL/TLS. See the documentation for the web server you are using. Make a note of each *SSL/TLS hostname* and *port*.
3. Create an InterSystems IRIS *SSL/TLS Configuration* for your Health Connect instance:

   Follow the instructions in Create or Edit a TLS Configuration. Note the **Configuration Name**.

   When you create or edit endpoints in the service registry, you can specify which SSL/TLS configuration to use. You can also specify the SSL/TLS Configuration directly in each production web client in the SSLConfig property.
4. Configure secure communication in the Installer Wizard:

a. Follow the instructions to access the Installer Wizard.

b. Click **Configure Secure Communication**.

c. The **Server HostName** field displays the value you entered in the **Configure Network Host Name** dialog. This is typically a "short name" that is resolved by your DNS rather than a fully-qualified domain name.

d. In the **Secure Port** field, enter the SSL port number for your secure web server.

e. Optionally enter a **Web Server Prefix**. If you are configuring a single web server to serve multiple HealthShare instances, enter the instance name to which you want to connect in the **Web Server Prefix** field, just as you would enter it in the **CSP Server Instance** field if you were defining a remote server connection.

f. Confirm that the value in the **Secure Root Endpoint** field is correct.

g. Select the **These Settings are Active** checkbox.

Important: If you do not select **These Settings are Active**, then your secure communication settings will *not* be used when you create your Foundation namespace and production in the Installer Wizard.

h. Select an **SSL/TLS Configuration** from the dropdown. Selecting an SSL/TLS Configuration allows the Installer Wizard to correctly construct your service registry entries to use secure communication.

i. Click **Save**.

4.4 Creating a Foundation Namespace and Production in the Installer Wizard

Important: Before you create a Foundation namespace and production for a live system, set up secure communication, so that your Foundation production automatically uses secure communication settings. Failure to do so may result in security vulnerabilities.

To install and activate a Foundation production using the Installer Wizard:

1. Follow the instructions to access the Installer Wizard.
2. Click **Configure Foundation**.
3. For **Local Name**, enter the name that will identify the Foundation production. This name will become the namespace that contains the class definitions for the production. The maximum length for this string is 50 characters. The local name is referred to below as *<LOCAL_NAME>*.
4. The Network Name is the network-wide, unique name for the Foundation production. It defaults to *Network_Host_Name:<LOCAL_NAME>*.

   Note: *Network_Host_Name* defaults to the machine's host name if you do not explicitly set it in the **Configure Network Host Name** option in the Installer Wizard. *Network_Host_Name* should always be set in the Installer Wizard before you begin configuring your instance.

   A DNS entry is a better choice of *Network_Host_Name*, as it provides more flexibility. In a mirror, it is important that *Network_Host_Name* be set to the VIP (or DNS entry) of your mirror before you use the Installer Wizard to configure your productions.

5. For **Description**, enter an optional short description.

6. If the system is a mirror member and you want to mirror the database, select **Mirror Database**. For additional information about mirroring with Health Connect, see the considerations for health care products described in Managing Mirroring.

   Note: On versions prior to 2022.1, in order to mirror a foundation namespace, request an ad hoc patch for HSHC-3009 from the WRC, and follow the ad hoc instructions provided.

7. For **Production**, enter the package and class name that you will use for this production in the form *Package.Class*. The default is <*LOCAL_NAME*>`PKG.FoundationProduction`. For example, "HSFOUNDATIONPKG.Foundation-Production". Adding `PKG` to <*LOCAL_NAME*> makes it easy to differentiate between namespace and code package names, and prevents naming collisions.
8. For **Template**, choose **`Generic Production`**.
9. The default location for the production database, `IRIS.DAT`, is *installDir*`/mgr/`*localName*. To specify a location for the database other than the default, enter the alternate location in the **Alternate Database Location** field. If you specify an absolute location, then that location will be created if it does not exist. Your database will be in *alternateDatabaseLocation*`/`*localName*. If you specify a relative location then the database will be created in *installDir*`/mgr/hslib/`*alternateDatabaseLocation*`/`*localName*.
10. Click **Save**. This production is now displayed in the list of configurations.
11. In the row for the production you just created, click **Activate**. A window pops up, asking if you want to proceed. It is at this step that your Foundation production is created.
12. Click **Start** to start the activation process.

    Note: If you close the dialog box before it displays a message that indicates completion, you will not see any error messages that may occur in the creation of your production.

    The result of the activation process is a new namespace that contains a Foundation production and other related classes. If you used the default values, the namespace for this production will be <*LOCAL_NAME*>, and the production name will be <*LOCAL_NAME*>`PKG.FoundationProduction`. So, for example, if you enter **`HSFOUNDATION`** in the **Local Name** field, you will create an **`HSFOUNDATION`** namespace that contains a **`FoundationProduction`** in the **`HSFOUNDATIONPKG`** package.

5

Running Health Connect in a Docker Container: Special Considerations

Running Health Connect in a Docker container is much the same as running InterSystems IRIS in a container, but you should make the following change once the container is up and running:

- Change the network host name

For more information on running Health Connect in a container, see *Running InterSystems Products in Containers*.

5.1 Changing the Network Host Name

When you are running Health Connect in a container, the network host name is defined as the container ID by default. This causes problems when you need to replace the container because the network host name will change to the ID of the new container. To avoid this problem, do the following to define a new network host name that will not change when you replace the container:

1. Log in to the Management Portal.
2. Make sure you are in the %SYS or HSLIB namespace.
3. From the Home page, select **Health**.
4. In the top navigation bar, select **Installer Wizard**.
5. Select **Configure Network Host Name** and enter the new name. A DNS entry is a good choice for a name.