Registry Guide for InterSystems IRIS for Health and HealthShare Health Connect

Version 2024.1
2024-05-02

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

Registry Guide for InterSystems IRIS for Health and HealthShare Health Connect
InterSystems 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

Managing the Service Registry

The Service Registry maintains a list of destinations for services. Typically these are URLs for SOAP services, either within your system or for external destinations.

1.1 Adding or Modifying a Service

To add a new service or modify an existing service:

1. Log in to the Management Portal as a user with the **`%HS_Administrator`** role.
2. Select the name of your Foundation namespace.
3. Click **Health** > **Service Registry**.
4. To add a new service click **Add Service**. Alternatively, you can click **Parse Web Service URL** to add a new SOAP service and then enter the URL in the dialog and click OK. The URL will be parsed into the appropriate fields in the Service Registry entry.
5. To modify an existing service click on the row for the service in the table. Use the **Service Type** drop-down above the table to filter the list of services shown in the table.
6. Enter the information for your service and click **Save**. The settings are documented in the next section.

1.2 Service Registry Settings

The data entry screen for services has two portions. The upper portion is fixed and contains nine fields. The contents of the lower portion change, depending on the **Service Type** selected. The settings for the upper portion are documented below. The settings for the specific service types are documented in the subsections that follow.

The following fields appear in the upper section of the Service Registry data entry screen:

Name

Required. Each service must have a unique name.

Timeout

Optionally enter the number of seconds before this service should time out.

Device

Optionally enter a code from the OID registry to tie this entry to a device OID.

Home Community

Optionally enter a code from the OID registry to tie this entry to a home community OID (for XCA).

Assigning Authority

Optionally enter a code from the OID registry to tie this entry to an assigning authority OID.

Repository

Optionally enter a code from the OID registry to tie this entry to a repository OID.

Device Function

Some Service Registry entries perform the function of a particular device. The entries available depend on the components you installed when you ran the FHIR installer. Standard entries include:

- `XCA.Query` — requires that a home community OID is specified as described above. Identifies the URL to direct XCA query transactions to in the specified home community.
- `XCA.Retrieve` — requires that a home community OID is specified as described above. Identifies the URL to direct XCA retrieve transactions to in the specified home community.
- `XDSb.Query` — identifies the document registry that XDS.b queries should be directed to.
- `XDSb.Retrieve` — requires that a repository OID is specified as described above. Identifies the URL to direct XDS.b retrieve transactions to for that repository OID.
- `PDQv3.Supplier` — identifies the PDQv3 supplier service.

Service Type

Required. Select a type for this service from the drop-down. The **Service Type** you select controls which fields appear in the lower portion of the screen. The options are:

- SOAP
- File
- FTP
- HTTP
- TCP
- UDP

The following sections document the settings specific to each service type. None of the settings are marked as required. For each service type, enter as many or as few settings as are needed to successfully perform the communication.

1.2.1 SOAP Service Settings

If you selected a **SOAP** service, you are presented with the following fields:

Host

Enter the hostname or IP address.

Port

Enter the port number.

SSL Configuration

Enter the name of an existing Secure Socket Layer (SSL) or Transport Layer Security (TLS) configuration to use to authenticate this connection. To create an SSL/TLS configuration, see Create or Edit a TLS Configuration. The SSL/TLS configuration includes an option called **Configuration Name**; this is the string to use in this setting. At the end of the SSL Configuration string, you can add a vertical bar (|) followed by the private key password.

URL

Enter the URL of the web service.

Proxy Host

Enter a proxy hostname, if applicable.

Proxy Port

Enter a proxy port number, if applicable.

HTTPCredentialsConfig

Enter the ID of the production credentials that contain the username and password to be used in the HTTP header. For information on creating production credentials, see the section "Configure Credentials" in the book *Configuring Productions.*

SOAP Version

Enter the SOAP version required. Use one of the following values:

- `""` — Use this value for SOAP 1.1 or 1.2.
- `"1.1"` — Use this value for SOAP 1.1. This is the default.
- `"1.2"` — Use this value for SOAP 1.2.

Username Token Profile

Specify the ID of the production credentials that contain the username and password to be used in the WS-Security header of the SOAP request.

X509 Token Profile for Encryption

Enter the alias of the X509 credentials to use for encryption of the message body. For information on creating these credentials, see "Creating and Editing InterSystems IRIS Credential Sets" in the book *Securing Web Services*.

X509 Token Profile for Digital Signing

Enter the alias of the X509 credentials to use for digitally signing the message. For information on creating these credentials, see "Creating and Editing InterSystems IRIS Credential Sets" in the book *Securing Web Services*.

MTOM

Select this check box if this is an XDS.b repository that accepts MTOM documents as attachments.

XUA Configuration

Select an XUA configuration from the drop-down to identify the SAML creator and SAML processor. See "Managing the XUA Registry" for details on XUA.

Send SAML Assertion

Controls whether SAML tokens should be sent in the security headers of SOAP calls.

There are several options:

- *No* — do not create a SAML assertion or forward any SAML assertions found in the request message.
- *Forward* — use the SAML creator class specified in the XUA configuration to forward any SAML assertion found in the request message. Do not create a SAML assertion.
- *Create* — use the SAML creator class specified in the XUA configuration to create a new SAML assertion based on the data in the request message. Do not forward any SAML assertion found in the request message.
- *Create then Forward* and *Forward then Create* — use the SAML creator class specified in the XUA configuration to create a SAML assertion *and* forward any SAML assertion found in the request message. The order that they are appear in the security header depends on the specific option chosen. If either the create or forward fails, an error is generated.
- *Forward or Create* — use the SAML creator class specified in the XUA configuration to forward any SAML assertion found in the request message. If no SAML assertion is found, create one. Only if both operations fail is an error generated.

Security Class

An optional class that overrides the default security code for signatures and encryption used in SOAP messages. Your security class should extend HS.Util.SOAPClient.Base and override the **AddSecurity()** class method.

1.2.2 File Service Settings

If you selected a **File** service, you are presented with the following fields:

File Name

Enter the name of the file on the local system.

File Path

Enter the full pathname of the directory for the specified file. This directory must exist, and it must be accessible through the file system on the local machine.

Overwrite Existing File

Select this check box to overwrite the existing file. If this is not selected, new data will be appended to the existing file.

1.2.3 FTP Service Settings

If you selected an **FTP** service, you are presented with the following fields:

File Name

Enter the name of the file to write on the FTP server.

File Path

Enter the full pathname of the directory on the FTP server for the specified file. This directory must exist, and it must be accessible using the Credentials provided.

Overwrite Existing File

Select this check box to overwrite the existing file. If this is not selected, new data will be appended to the existing file.

Host

Enter the IP address or server name of the FTP server.

Port

Enter the TCP port number to use on the FTP server. The default is 21.

User Credentials Config

Enter the production credentials that can authorize a connection to the FTP server. For information on creating production credentials, see the section "Configure Credentials" in the book *Configuring Productions.*

Use Passive

Select this check box to use passive FTP mode, where the server returns a data port address and the client connects to it. Most firewalls are more tolerant of passive mode FTP because both the control and data TCP connections are initiated by the client.

1.2.4 HTTP Service Settings

If you selected an **HTTP** service, you are presented with the following fields:

Host

Enter the IP address or hostname of the server.

Port

Enter the TCP port on the server. This defaults to 80 (or 443 if SSL Configuration is specified).

SSL Configuration

Enter the name of an existing Secure Socket Layer (SSL) or Transport Layer Security (TLS) configuration to use to authenticate this connection. To create an SSL/TLS configuration, see Create or Edit a TLS Configuration. The SSL/TLS configuration includes an option called **Configuration Name**; this is the string to use in this setting. At the end of the SSL Configuration string, you can add a vertical bar (|) followed by the private key password.

URL

Enter the URL path (not including http:// or the server address).

Proxy Host

Enter the IP address or hostname of the proxy server, if applicable.

Proxy Port

Enter a proxy port number, if applicable, This defaults to 8080.

HTTPCredentialsConfig

Enter the ID of the production credentials that can authorize a connection to the given destination URL. For information on creating production credentials, see the section "Configure Credentials" in the book *Configuring Productions.*

Proxy HTTPS

If your client uses this setting, make sure this value is the same as that for your client.

Proxy Tunnel

If your client uses this setting, make sure this value is the same as that for your client.

Proxy HTTPS SSLConnect

If your client uses this setting, make sure this value is the same as that for your client.

1.2.5 TCP Service Settings

If you selected a **TCP** service, you are presented with the following fields:

Host

Enter the IP address to make a TCP connection to. If the address starts with a ! character, the adapter will wait for a connection from a remote system. If no IP address follows the ! character, any remote system may connect; otherwise only the listed IP addresses (and ports) will be allowed to connect.

Port

Enter the TCP port to connect to. TCP port numbers have a maximum value of 65535.

SSL Configuration

Enter the name of an existing Secure Socket Layer (SSL) or Transport Layer Security (TLS) configuration to use to authenticate this connection. To create an SSL/TLS configuration, see Create or Edit a TLS Configuration. The SSL/TLS configuration includes an option called **Configuration Name**; this is the string to use in this setting. At the end of the SSL Configuration string, you can add a vertical bar (|) followed by the private key password.

Stay Connected

- Set this to a positive value to stay connected to the remote system for this number of seconds after completing an operation.
- Set this to zero to disconnect immediately after every operation.
- Set this to –1 (the default) to stay permanently connected, even during idle times.

1.2.6 UDP Service Settings

If you selected a **UDP** service, you are presented with the following fields:

Host

Enter the IP address to make a UDP connection to.

Port

Enter the UDP port to connect to.

UDP Sender Command

Enter the desired UDP sender command.

1.3 Deleting a Service

To delete an existing service:

1. Open the Management Portal.
2. Select the name of your Foundation namespace.
3. Click **Service Registry**.
4. Click on the row for the service in the table. Use the **Service Type** drop-down above the table to filter the list of services shown in the table.
5. Click **Delete** at the bottom of the screen.
6. Click **OK** in the confirmation dialog box.

2

Managing the OID Registry

The OID Registry maintains a list of object identifiers (OIDs). An OID is a globally unique ISO identifier. OIDs used in InterSystems products consist of numbers and dots, for example, 1.3.6.1.4.1.21367.2010.1.2. OIDs use a tree structure where the leftmost number represents the root and the rightmost number represents a leaf.

OIDs can be used to identify:

- Facilities
- Gateways
- Assigning authorities
- Devices
- Home communities
- Coding systems
- Repositories

You can obtain a root OID for your organization from a registration authority, like HL7. To obtain an OID for your InterSystems installation, go to HL7.org (http://www.hl7.org/oid/index.cfm) and click the link "Click to Obtain or Register an OID."

Once you acquire the root OID, you can design your own namespace subtree. ISC recommends planning out how you map this subtree. For compatibility with the DICOM standard, OIDs should not exceed 64 characters.

2.1 Adding or Modifying an OID

To add a new OID registry entry or modify an existing one:

1. Log in to the Management Portal as a user with the **`%HS_Administrator`** role.
2. Select the name of your Foundation namespace.
3. Select **Health** > **IHE Configuration** > **OID Registry**.
4. To add a new OID click **Add OID**, or to modify an existing OID click on the row for the OID in the table. Use the **Identity Type** drop-down above the table to filter the list of OIDs shown in the table.
5. Enter the information for your OID and click **Save**. The settings are documented in the next section.

6. If you are modifying OID settings for a running production that uses SDA-FHIR transformations, you must restart the `HS.FHIR.DTL.Util.HC.SDA3.FHIR.Process` and/or `HS.FHIR.DTL.Util.HC.FHIR.SDA3.Process` business processes.

2.2 OID Registry Settings

Enter the following settings in the OID registry:

Code

Required. Enter the identity code for this OID. Two or more entries may use the same identity code as long as the OIDs are of different type. For example, an assigning authority and a home community may share an OID and use the same code.

OID

Required: the OID value.

Aliases

Optional: if you have more than one code that maps to this OID or URL, enter them here.

URL

Required: the namespace URL for the given code.

Description

Optionally enter a description for this OID entry.

Types

Select one or more types for this OID from the drop-down. The options are:

- Facility
- Gateway
- Assigning authority
- Device
- Home Community
- Code System
- Repository

2.3 Deleting an OID

To delete an existing OID registry entry:

1. Log in to the Management Portal as a user with the **`%HS_Administrator`** role.
2. Select the name of your Foundation namespace.

3. Select **Health** > **IHE Configuration** > **OID Registry**.
4. Click **Add/Edit OIDs**.
5. Click on the row for the OID entry in the table. Use the **Identity Type** drop-down above the table to filter the list of OIDs shown in the table.
6. Click **Delete** at the bottom of the screen.
7. Click **OK** in the confirmation dialog box.

2.4 Importing OIDs from a File

You can import your OIDs from a file into your OID registry:

1. Navigate to the **OID Registry Import** page:
   a. Log in to the Management Portal as a user with the **%HS_Administrator** role.
   b. Select the name of your Foundation namespace.
   c. Select **Health** > **IHE Configuration** > **OID Registry**.
   d. Click **Import OIDs**.
2. Click **Select File** to identify the location of your import file. Your import file should contain one or more <OIDMap> entries in XML format as shown in the example below:

XML

```
<?xml version="1.0" encoding="UTF-8"?>
<root>
     <OIDMap>
          <OID>2.16.840.1.113883.6.22</OID>
          <IdentityCode>XYZ81</IdentityCode>
          <IdentityTypes>
               <OIDType>
                    <Description>CodeSystem</Description>
               </OIDType>
          </IdentityTypes>
          <Description>My Test Code System</Description>
          <Types>CodeSystem</Types>
     </OIDMap>
     <OIDMap>
          <OID>1.3.6.1.4.1.21367.2010.1.2.300.2.44</OID>
          <IdentityCode>ABC123</IdentityCode>
          <IdentityTypes>
               <OIDType>
                    <Description>AssigningAuthority</Description>
               </OIDType>
               <OIDType>
                    <Description>Facility</Description>
               </OIDType>
               <OIDType>
                    <Description>Organization</Description>
               </OIDType>
          </IdentityTypes>
          <Description>My Test Assigning Authority</Description>
          <Types>AssigningAuthority,Facility,Organization</Types>
     </OIDMap>
</root>
```

Note: In the XML file:

- The `<Description>` element (not the `<OIDType><Description>` element) is optional.
- OID types appear twice:
  - once each in individual `<OIDType>` elements where the `<Description>` contains the type.
  - then together as a comma-separated list in the `<Types>` element.

2.5 Exporting OIDs to a File

You can export your OID registry, or a portion of it, to a file:

1. Navigate to the **OID Registry Export** page:
   a. Log in to the Management Portal as a user with the **`%HS_Administrator`** role.
   b. Select the name of your Foundation namespace.
   c. Select **Health** > **IHE Configuration** > **OID Registry**.
   d. Click **Export OIDs**.
2. Click **Select Export Destination** to identify the location of your export file. The default filename is OIDRegistryExport_*YYYY-MM-DD*.xml, for example OIDRegistryExport_2015-10-01.xml.
3. Select the rows in the OID table that you wish to export and click **Export Selected**, or click **Export All**.

The export file is formatted as XML as shown in the previous section.

3

Managing Assigning Authorities for Identifiers

InterSystems supports several different types of patient and clinician identifiers. Most identifiers are associated with a particular assigning authority. For example, driver's license numbers in the US are associated with a state. Passport numbers are associated with a country.

InterSystems products maintain an *assigning authority registry.* Entries in the registry are categorized by *identifier type*. The default identifier types are:

- corporate ID
- driver's license
- doctor number
- insurance ID
- medical record number
- PIX identifier

3.1 Accessing the Assigning Authority Registry

To define an assigning authority, modify the details of an existing assigning authority, or delete an assigning authority, use the **Assigning Authority Registry**. To access this page:

1. Log in to the Management Portal as a user with the **`%HS_Administrator`** role.
2. Select your Foundation namespace.
3. Click **Health** > **Assigning Authority Registry**.

3.2 Adding or Modifying an Assigning Authority

To add an assigning authority or modify its details, do the following:

1. Select the identifier type whose assigning authorities you wish to edit from the drop-down list.

2. In the table, click the row for an existing assigning authority or click **Add Assigning Authority** to create a new entry.
3. Enter the name and code of the assigning authority.
4. Optionally click the **Allow Multiples** check box, to allow multiple identifiers of this type for a particular individual. (This feature is not currently implemented.)
5. If you are using the QuadraMed MPI, enter in the **Other ID** field the code that QuadraMed has designated for this assigning authority. If you are not using QuadraMed, you can leave this field blank.
6. Click **Save Assigning Authority** to save your changes.

3.3 Deleting an Assigning Authority

To delete an assigning authority, do the following:

1. Select the identifier type for the assigning authority you wish to delete from the drop-down list.
2. Click **Delete** in the row for an existing assigning authority.
3. Click **OK** to confirm your action.

4

Managing the Configuration Registry

The configuration registry is a database of key-value pairs. Here you can register custom web pages, custom functions, and details for certain predefined values.

To access the configuration registry:

1. Log in to the Management Portal as a user with the **`%HS_Administrator`** role.
2. Select your Foundation namespace.
3. Click **Health** > **Configuration Registry**.
4. To create a new key, click the **Add Value** button. To modify an existing key, select the key in the table.
5. Enter the key and its value in the appropriate fields and click **Save**.

Configuration registry key categories include:

- \HomeCommunity — details of the home community's contact information.
- \IHE — details required for IHE communication.
- \LegalAuthenticator — details about the person legally responsible for exported content.
- \UI — configuration details for custom web pages invoked by the Management Portal.

These are detailed in the sections that follow.

4.1 Home Community Keys

Use the `\HomeCommunity` keys to hold the contact details of your IHE home community:

- `\HomeCommunity\Address\StreetLine1`
- `\HomeCommunity\Address\StreetLine2`
- `\HomeCommunity\Address\City`
- `\HomeCommunity\Address\State`
- `\HomeCommunity\Address\Zip`
- `\HomeCommunity\Address\Country`
- `\HomeCommunity\Telecom\Workphone`

4.2 IHE Keys

Use the `\IHE` keys to control various aspects of IHE functionality.

`\IHE\HomeCommunity`

Use this key to identify the OID of your home community. A home community is an entity that has a single XDS document registry. The value of this key may be an OID value or the IdentityCode of an OID identified in the OID registry. For example: you might have an OID called "HomeCommunity", that is both an AssigningAuthority and a HomeCommunity type OID. In that case, enter `HomeCommunity` as the value for this key.

`\IHE\AffinityDomain`

An affinity domain is responsible for assigning unique MPI IDs for one or more home communities. Use this key to identify the OID of your IHE affinity domain assigning authority. This may be an OID value or the code of an OID identified in the OID registry. Often, this is the same OID as the `\IHE\HomeCommunity` OID.

`\IHE\XDSb\Repository\`*`RepositoryName`*`\Retrieve\MTOMRequired`

Set this key to zero if the XDS.b repository, called *RepositoryName*, does not support MTOM attachments.

4.3 Legal Authenticator Keys

Use the `\LegalAuthenticator` keys to hold the contact details and identity of the individual in your organization who bears legal responsibility for exported content:

- `\LegalAuthenticator\Name\Given`
- `\LegalAuthenticator\Name\Family`
- `\LegalAuthenticator\Address\StreetLine1`
- `\LegalAuthenticator\Address\StreetLine2`
- `\LegalAuthenticator\Address\City`
- `\LegalAuthenticator\Address\State`
- `\LegalAuthenticator\Address\Zip`
- `\LegalAuthenticator\Address\Country`
- `\LegalAuthenticator\Telecom\Workphone`

4.4 UI Keys

The `\UI` keys identify user interface pages that have been customized for a site. Most of the Zen pages in the user interface may be customized, including any page that is invoked by one of the $$$HSUILink macros. Typically, custom user interface pages extend the standard UI page and replace one or more XDATA blocks. To replace a standard UI page with your own page, use a key of the form `\UI\`*`[subpackage \]...\class`* to identify the page you are replacing, and set the value to the complete class name of your custom page, including the `.cls` extension. For example:

To replace the class HS.UI.Logout.cls, use the key `\UI\Logout` and a value like Custom.Logout.cls

Note: After adding a custom page you must log out and the log back in in order to see the new page.

4.4.1 The Application Class

The class HS.UI.Application specifies styles and banners that are used by all UI pages. To customize styles and banners system-wide, extend HS.UI.Application.cls. You may customize the stylesheet by overriding the `Style` XDATA block, or customize page headers by overriding the **DrawTitle()** method.

Register your custom application page using the key `\UI\Application`.

Individual pages may also override the `Style` XDATA block or **DrawTitle()** method on a per-page basis.

5

Managing the XUA Registry

Cross-Enterprise User Assertion (XUA) is an IHE profile that supports user authentication across enterprise boundaries using the SAML 2.0 Identity Assertion to verify claims about an authenticated identity. SAML tokens are sent in the security headers of SOAP calls.

To enable creation of outbound SAML Assertions using the XUA registry:

1. Create one or more XUA configurations in the XUA registry (documented in the next section).
2. Select an **XUA Configuration** in the appropriate Service Registry entry.

   For XCA and XDS.b, the Service Registry entry should be one that has a **Device Function** set to either `XCA.Retrieve` or `XDSb.Retrieve`.
3. Select a style of SAML Assertion in the **Send SAML Assertion** field in the Service Registry entry. See "SOAP Service Settings" in the chapter Managing the Service Registry for details on the various styles of assertions.

Setting up SAML in the Service Registry allows different SAML Assertion types to be sent to different repositories (which may come from different vendors). For example, if you request documents from different XDS.b repositories or different XCA Home Communities, the same consumer operation can be used for all of the requests. By assigning a different XUA configuration to each Service Registry entry, the SAML creator can be customized for each system. Health Connect uses the repository OID or the Home Community OID in the document request to identify which Service Registry entry (and XUA configuration) to use for that request.

Note: The XDS.b consumer operation contains **SendSAMLAssertion** and **SAMLCreator** settings, but these have been deprecated in favor of XUA configurations and the settings on the Service Registry as they provide for more flexibility.

To enable inbound SAML Assertion processing, create an XUA configuration that identifies the sending organization using the organization OID or URL found in the assertion.

5.1 Creating or Editing an XUA Configuration

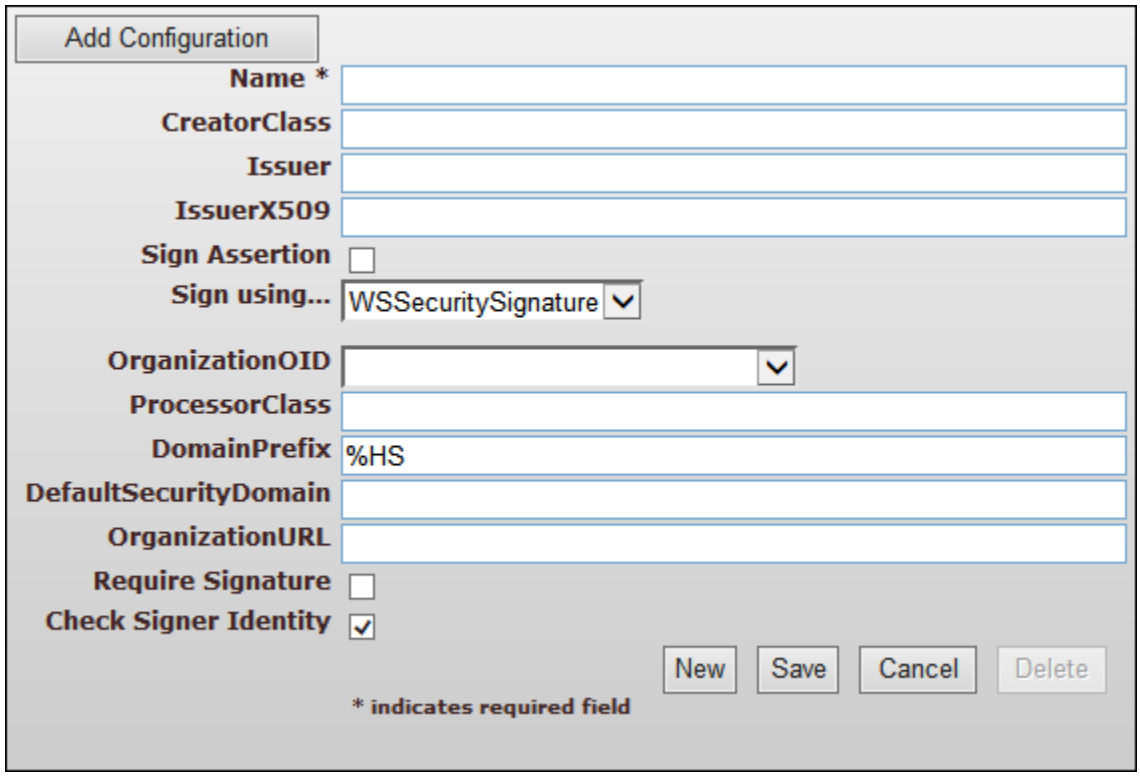
An XUA configuration defines how to create an outbound SAML Assertion and how to process an inbound SAML Assertion. To create or edit an XUA configuration:

1. Log in to the Management Portal as a user with the **`%HS_Administrator`** role.
2. Select your Foundation namespace.
3. Select **Health** > **IHE Configuration** > **XUA Configuration Registry**.

4. Select a configuration from the table to edit an existing configuration or select **Add Configuration** to create a new one.
5. Enter appropriate values in the various settings and select **Save**. The settings are described in the next section.

5.1.1 XUA Configuration Settings

The image below is the XUA Configuration screen:



The first block of settings relates to creating an outbound SAML Assertion. The second block of settings relates to processing an inbound SAML Assertion.

5.1.1.1 XUA Settings for Creating a SAML Assertion

Name

The name of the configuration. Only **Name** is required to save a configuration, but several additional settings are required in order to make the XUA configuration functional for creating or processing assertions.

CreatorClass

The name of the class that creates the SAML Assertion. This setting is required for creating assertions. The creator class may be HS.IHE.XUA.Creator.cls or a custom class that extends HS.IHE.XUA.Creator. An example is provided in the class HS.IHE.XUA.SHINNY.Creator.cls.

Issuer or IssuerX509

The string to use for the name of the SAML Issuer. Set either one property or the other:

- **Issuer** — a string containing the distinguished name of the organization's certificate.
- **IssuerX509** — the alias of an X.509 certificate that references the organization's certificate. If **Sign Assertion** is selected, then the X.509 certificate is used to sign the SAML token.

If both **Issuer** and **IssuerX509** are empty, an error is reported when creating new tokens. If both values are set, **IssuerX509** takes precedence over **Issuer**.

Sign Assertion

Select this to ensure that each SAML token is signed by the X.509 certificate indicated in the **IssuerX509** setting. If **Sign Assertion** is selected, then **IssuerX509** must have a value.

Sign Using

Whether to sign the message using the WSSecuritySignature or Signature. Signing with both causes problems validating the Signature, because the Signature signs the assertion when only a placeholder WSSecuritySignature is present, but would be validated against a message containing the full WSSecuritySignature. This defaults to `WSSecuritySignature`.

As part of the signature verification process, the XUA processor checks that the WSSecuritySignature or Signature actually signs the entire assertion by comparing the reference URI to the assertion ID, based on SAML 2.0 spec, section 5.4.2.

5.1.1.2 XUA Settings for Processing an Inbound SAML Assertion

OrganizationOID or OrganizationURL

Select the code of an OID registry entry identifying the organization in the **OrganizationOID** field. Optionally set the URL of the organization in the **OrganizationURL** setting.

An inbound SAML Assertion should contain an organization identifier of some kind. This may be in the form of an OID or a URL. InterSystems uses the organization identifier to identify which XUA configuration should process the assertion. InterSystems recognizes the following forms of attribute name for the organization identifier:

- IHE: `urn:oasis:names:tc:xspa:1.0:subject:organization-id`
- SHIN-NY: `UserOrganizationOID`

If you receive SAML Assertions that use a different attribute naming convention, write a custom method to locate the organization identifier in the assertion and assign the method to `OrgURLAttributeCode` in the web service. The method should return an organization identifier in the form of an OID or URL. An example method is provided in **GetOrganizationID()** in the class HS.IHE.XUA.SHINNY.Processor.

ProcessorClass

The name of the class that processes inbound SAML Assertions. This setting is required for processing assertions. The processor class may be HS.IHE.XUA.Processor.cls or a custom class that extends HS.IHE.XUA.Processor. An example is provided in the class HS.IHE.XUA.SHINNY.Processor.cls.

DomainPrefix and DefaultSecurityDomain

DefaultSecurityDomain is the name of the default security domain. This is optional.

InterSystems uses information from the SAML attributes along with the optional **DomainPrefix** to locate the appropriate security domain where the SAML users are defined. It searches in the following order for a domain identified by the value of **DomainPrefix** concatenated with the:

1. OID registry code for the *organization-id* from the SAML Assertion
2. *organization* name directly from the SAML assertion
3. OID registry code for the *homeCommunityId* of the sender from the SAML Assertion

The provided value for **DomainPrefix** is "%HS " for the internal security domains.

If InterSystems locates an appropriately named security domain, it searches for the users there. Otherwise it uses the value in **DefaultSecurityDomain**, without the domain prefix, to locate users.

For example, if all SAML users are identified in your system in security domains that begin with "SAML_", enter SAML_ in the **DomainPrefix** field. For a SAML Assertion with the following attributes:

- an *organization* attribute of "XYZ"
- an *organization-id* of "1.2.3" which resolves to "XYZ-Organization" in the OID registry
- a *homeCommunityID* of "4.5.6" which resolves to "RHIO-A" in the OID registry

InterSystems would look in the following order for domains named:

1. "SAML_XYZ-Organization"
2. "SAML_XYZ"
3. "SAML_RHIO-A"

If none of those domains are found, InterSystems looks in the default domain.

You can change this behavior by overriding the **GetDomain()** method in your processor class. In the provided example, HS.IHE.XUA.SHINNY.Processor.cls, the following scheme is used:

1. DomainPrefix_*UserOrganizationOID*
2. DomainPrefix_*UserOrganizationName*
3. DomainPrefix_*UserRHIO* (which is an OID)

Require Signature

Select this to require that inbound SAML Assertions be signed by an X.509 certificate in order to be processed.

Check Signer Identity

If selected (the default), the XUA processor inspects the KeyInfo property of the signature of an inbound SAML assertion as part of signature validation. The assertion will only pass validation if the following two conditions are met:

- it is possible to identify the signer from the KeyInfo.
- the signer's credentials are trusted.

Important: If an RSA public key is used in lieu of an X.509 certificate, it must be added to the Trusted RSA Key Registry.

If not selected, assertions that are signed with only an RSA public key or with symmetric encryption will pass validation without attempting to identify the signer.

6

Managing the Trusted RSA Key Registry

The XML signature of an inbound SAML Assertion for XUA messaging can include a RSA public key in lieu of an entire X.509 certificate. If you use an RSA public key for inbound SAML Assertions, you must add it to the Trusted RSA Key Registry.

To add a key to the Trusted RSA Key Registry:

1. Log in to the Management Portal as a user with the **`%HS_Administrator`** role.
2. Select your Foundation namespace.
3. Select **Health** > **IHE Configuration** > **Trusted RSA Key Registry**.
4. Select an entry from the table to edit an existing entry or select **Add Trusted Key** to create a new one.
5. Enter appropriate values in the various settings and select **Save**. The settings are described below.

Alias

Required.

Public Key Modulus (Base64 encoded)

Required.

Public Key Exponent (Base64 encoded)

Required.

7

Managing the Coded Entry Registry

The Coded Entry Registry defines the codes, templates, and identifiers required for IHE communication. InterSystems is installed with a substantial set of these codes. For details on the various code types, refer to the IHE wiki.

To access the Coded Entry Registry:

1. Log in to the Management Portal as a user with the **%HS_Administrator** role.
2. Select your Foundation namespace.
3. Select **Health** > **IHE Configuration** > **Coded Entry Registry**.
4. Select an entry from the table to edit an existing entry or select **Add Code** to create a new one.
5. Enter appropriate values in the various settings and select **Save**. The settings are described below.

Use the **Code Type** drop-down list to filter the table by code type, or enter terms in the **Search** box. You can adjust the number of entries displayed on each page with the **Page Size** box.

Each entry contains the following information:

CodeType

The following code types are available:

- associationDocumentation
- classCode
- confidentialityCode
- contentTypeCode
- eventCodeList
- folderCodeList
- formatCode
- healthcareFacilityTypeCode
- practiceSettingCode
- typeCode

Code

The value of the code.

Scheme

The standard to which the code conforms.

Description

An optional description.