Interweave Console User Guide

Version 2.2

Table of Contents

1 Introduction 4

1.1 Purpose of this Document 4

2 User Guide 5

2.1 Initial Registration 5

2.2 Log On 5

2.3 Front Screen (Organisation) 7

2.4 Contacts and Users 9

2.5 Provider Settings 10

2.5.1 Provider basic setup 10

2.5.2 Endpoint Configuration 11

2.5.3 Certificates and Secret 13

2.5.4 Data Provider Approval Process 15

2.5.5 Other Environments 15

2.6 Provider Settings – Additional Options 16

2.6.1 View Access Restrictions 16

2.6.1.1 Consumer Pairing 16

2.6.1.2 Permitted Roles and Reasons 16

2.6.1.3 Resources 17

2.6.2 Health Check 18

2.6.2.1 Errors and Warnings 18

2.6.2.2 Capability Statement 18

2.6.2.3 Continuous Compliance 18

2.6.3 Audit Log 19

2.7 Consumer Settings 20

2.7.1 Consumer basic setup 20

2.7.2 Endpoint Configuration 22

2.7.3 Certificates and Secret 22

2.7.4 Approval Process 22

2.7.5 Other Environments 22

2.7.6 Audit Log 22

2.8 Validate FHIR Resource 23

Version Control

Version	Release Date	Released By	Reason for Release
1.0	09/11/2021	Tim Davey	Initial version
2.0	17/11/2021	Tim Davey	Updated following internal review
2.1	20/03/2024	Sophie Lowsley	Refresh of screenshots – full review to follow.
2.2	16/07/2024	Sophie Lowsley	Updated name from Onboarding Suite to Console

Reviewers

Initials	Name	Role	Organisation

1 Introduction

1.1 Purpose of this Document

This document provides a brief overview of how to use the Interweave Console.

It is intended for the (primarily) technical staff at each Data Provider and/or Data Consumer organisation who will be responsible for configuring their connectivity.

It does not aim to cover configuration and administration of the system, nor does it cover the special features for additional tasks such as Local Opt Out Management.

2 User Guide

2.1 Initial Registration

You will receive an invite email with a registration link when your account is created.

Onboarding User Registration

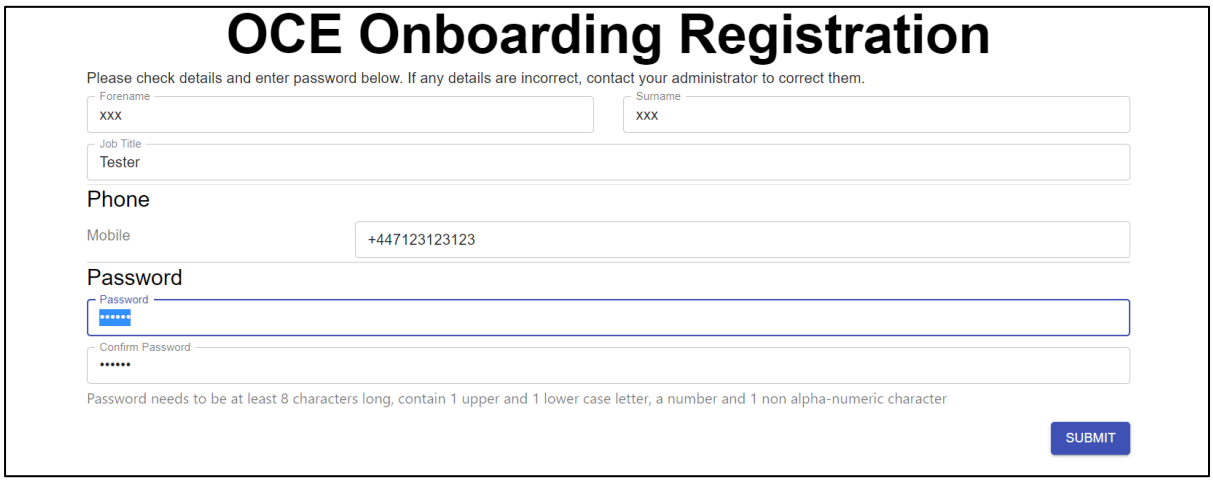
A request has been made for you to register as a user of the YHCR Onboarding System.

Please Click Here to acitivate your account.

Please note, the link will expire 30 minutes after the time on this email.

If 30 minutes have passed, please contact your administrator to receive another verification email.

The initial registration page will invite you to confirm your name and job title, enter a mobile number (for multi-factor authentication), and create a password



2.2 Log On

The Console can be found at:

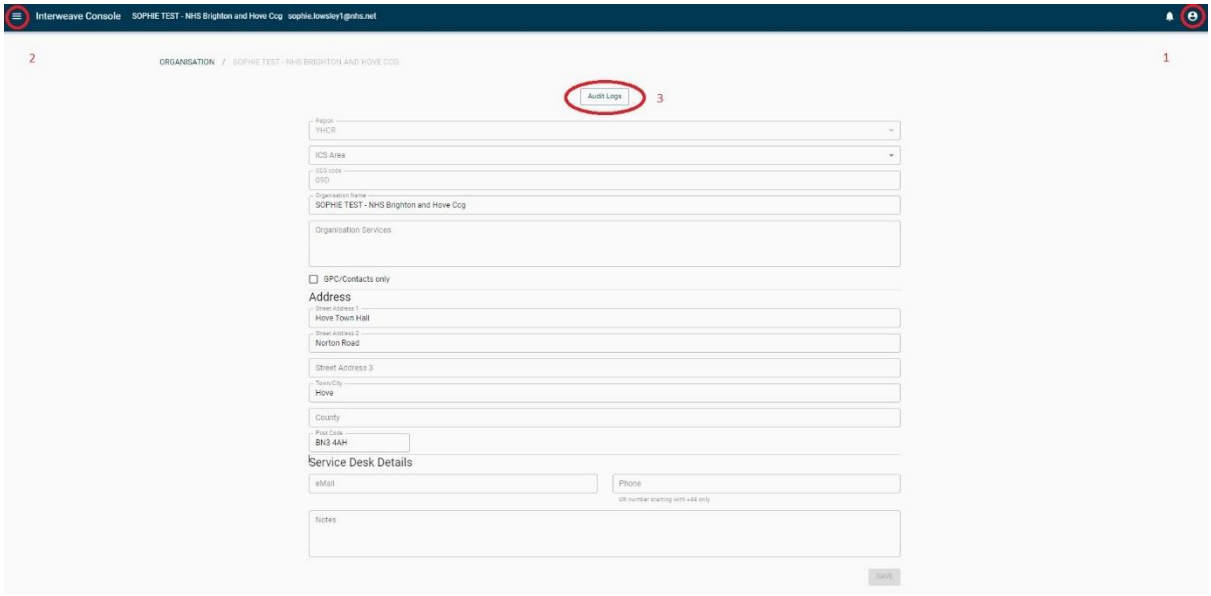
https://console.yhcr.nhs.uk/

Once registration is complete then you can log on.

Note the option to reset password if it is forgotten.

You will be prompted for a second factor, in the form of a code sent by SMS to your phone

2.3 Front Screen (Organisation)

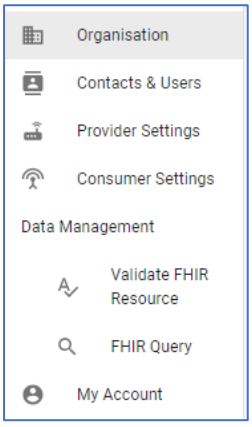


You will arrive by default in the screen displaying your **organisation details**. These have been pre-populated from the NHS Organisational Data Services (ODS) database, but please check they are correct. It is also important to fill in the **Service Desk Details**, so that they can be contacted in the event of issues occurring. Press **Save** to commit any updates.

At the top of the screen is the standard menu bar. On this you can see:

1) **The account button**. This enables you to log out, or to change your account details (name, job title, phone number, and password)

2) **The main menu**. This pops out as shown below.



- **Organisation** – is the organisation screen you are already on
- **My Account** – is for changing account details (it is the same screen as can also be reached via the account button in the top right)

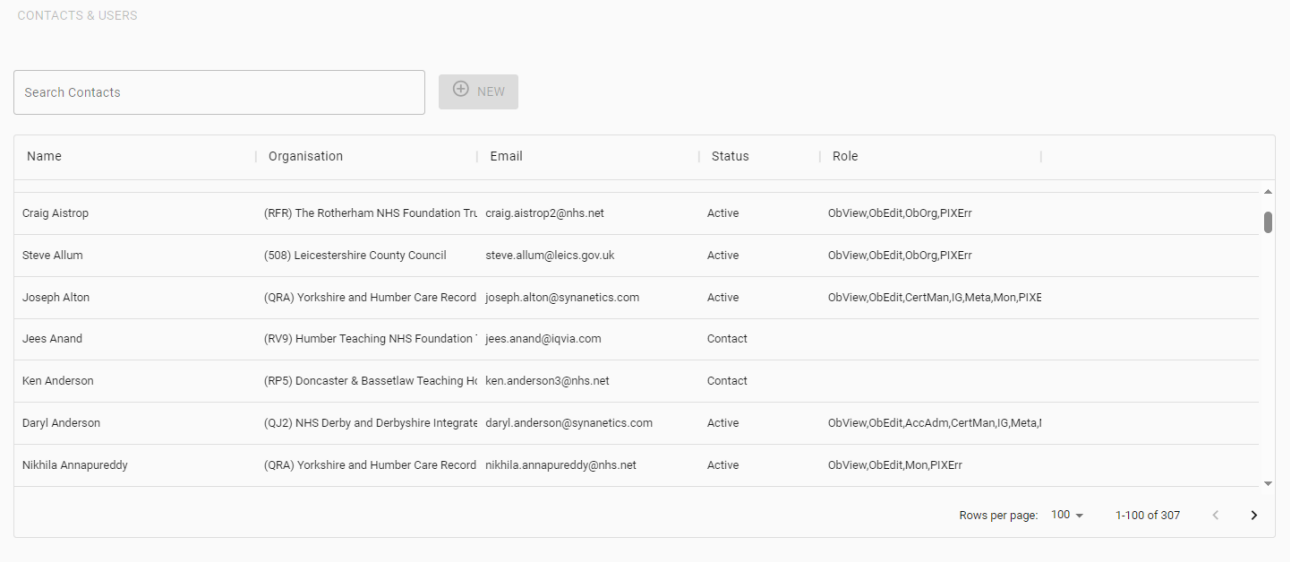
The other options will be walked through in detail in the sections which follow.

Finally you can see the "**Audit Logs**" button (3). This shows a log of all changes to your organisation settings. When you first log on there will not be much to see, but the log will grow if any actions are performed

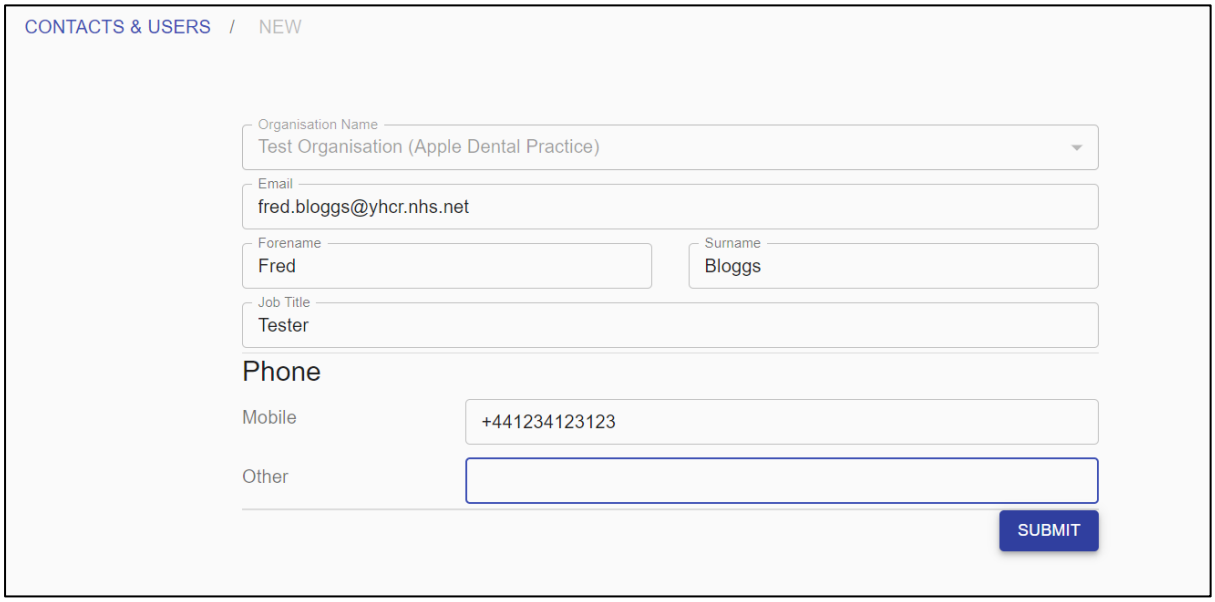
We will now look at the other menu options available.

2.4 Contacts and Users

This presents the list of the contacts and users registered for your organisation. Double-click on a contact or user to view their details.



- **Users** – new users can only be created by a system administrator. ***Please raise a Service Request if you need additional user(s) creating.***
- **Contacts** – contacts are indicated by a status of "Contact" and ***you can create these yourself*** by pressing "New". A screen will pop up to enter details, similar to that used when first registering your account.

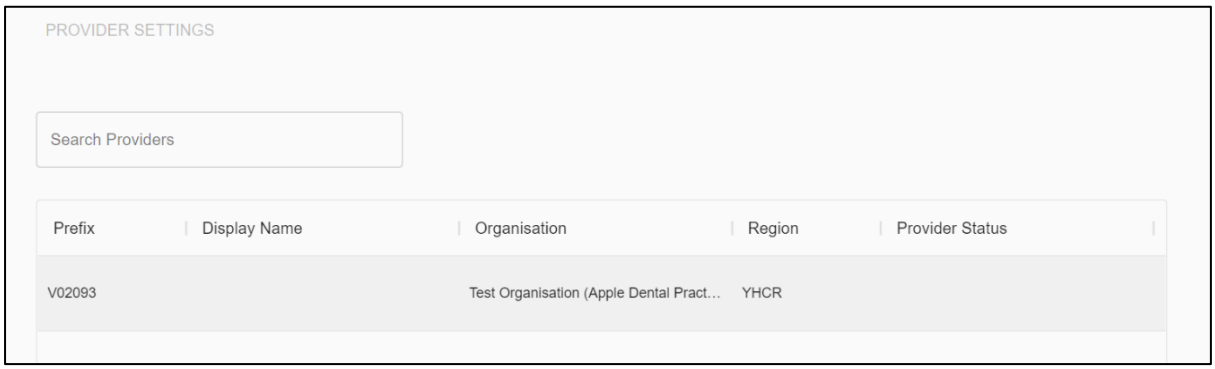


Contacts do NOT get a logon, and so cannot use the system. However they will be included on notifications – for example the emails about Release Notes, notifications of system outages, etc. (Contacts can also be promoted to a full User by raising a Service Request).

2.5 Provider Settings

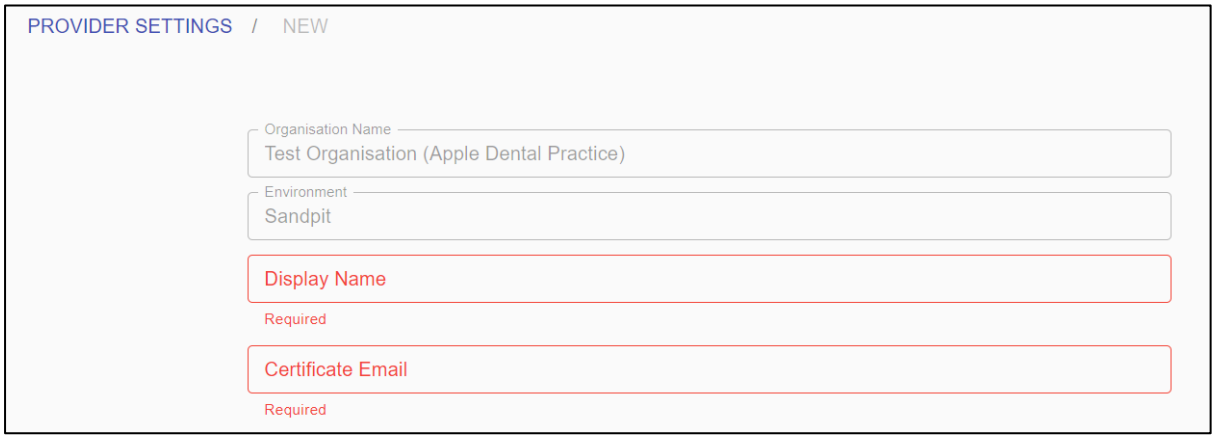
This menu option is one of the most important sections of the application. It allows Data Provider endpoints to be configured.

The initial screen shows a summary of your Data Provider, and you can double-click to go in.



2.5.1 Provider basic setup

The first step is to enter some basic details:



- **Organisation Name** – is fixed at your own organisation
- **Environment** – is fixed at "Sandpit" initially, as this is the first test environment you will work with. It is possible at a later stage in the process to also select other environments, ie Staging and Production
- **Display Name** – this is important, as it is likely be shown on-screen to end users. It should be a short but meaningful summary of who / what your Data Provider is. In many cases it will simply be your organisation name or initials again. However there are scenarios where it may be different – eg if a technology supplier is creating a single Data Provider connection for a system which hosts data from many organisations. Please get in touch to discuss if you are unsure.

Tips for choosing a Display Name

- ✓ It is best to be concise, as they are often displayed in tables with limited column widths. (eg "Leicestershire County Council" is rather too long)
- ✓ Do not use your ODS code, as this is already captured elsewhere - and so does not add anything new or useful
- ✓ A well-recognised acronym for your organisation can be a good choice eg "NYCC"

✓ However try to avoid ambiguity – eg LCC could be either “Leicester City Council” or “Leicestershire County Council”

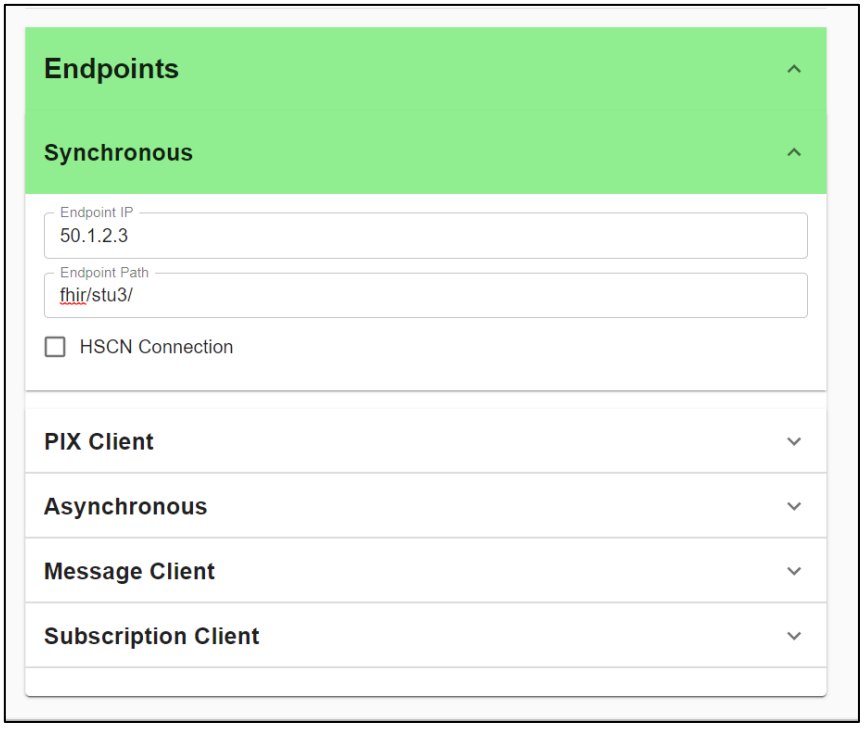
✓ An abbreviation of the organisation name can be a good choice eg "Leics County" and "Leics City"

- **Certificate email** – this is the email which is embedded into the certificates issued. It is required for creating certificates, however there are no current plans to actually send any emails to it. (The email address of a senior worker within your Network & Infrastructure team is recommended).

Once these details are entered, press “**Submit**” to create a skeleton Data Provider. Further sections of the screen are now enabled.

2.5.2 Endpoint Configuration

The “Endpoints” section can be expanded to show details of the various endpoints which you may wish to set up for your Data Provider. Whilst requirements can obviously vary, the endpoints are listed with those most commonly used first.



- **Synchronous (inbound)** – for receiving and responding to synchronous requests for data. This is typically the core of what a Data Provider does
- **PIX Client (outbound)** – you will need to send messages to register those NHS Numbers for which you hold data, and this is the address these messages will emanate from.
- **Asynchronous (inbound)** – for receiving asynchronous requests for data. For example analytic extract requests.
- **Message Client (outbound)** – for proactively transmitting data (eg Ambulance Transfer of Care). This is the address these messages will emanate from.
- **Subscription Client (outbound)** – similar to above, for transmitting data when a subscription is triggered.

Once endpoint details are entered then the sections light up (green), so that you can see at a glance which endpoints are in use.

- **For an inbound endpoint** – both the **IP address and path** are needed, so that the Interweave Exchange can construct the full path for sending the message to you.
    - The IP address can include a Port if desired
    - Note that there is the option to indicate if this is a HSCN connection. This does not do anything and is purely for documentation purposes – the actual arrangements for connectivity will need to be made separately. This should be an exceptional option – Internet-First connectivity is the norm.
- **For an outbound endpoint** – **only the IP address** is needed. This is used to whitelist you on the Interweave Exchange firewalls.
    - Note that if you are running on multiple servers then it is possible, if necessary, to enter multiple IP addresses and/or CIDR ranges here - separated by a space.

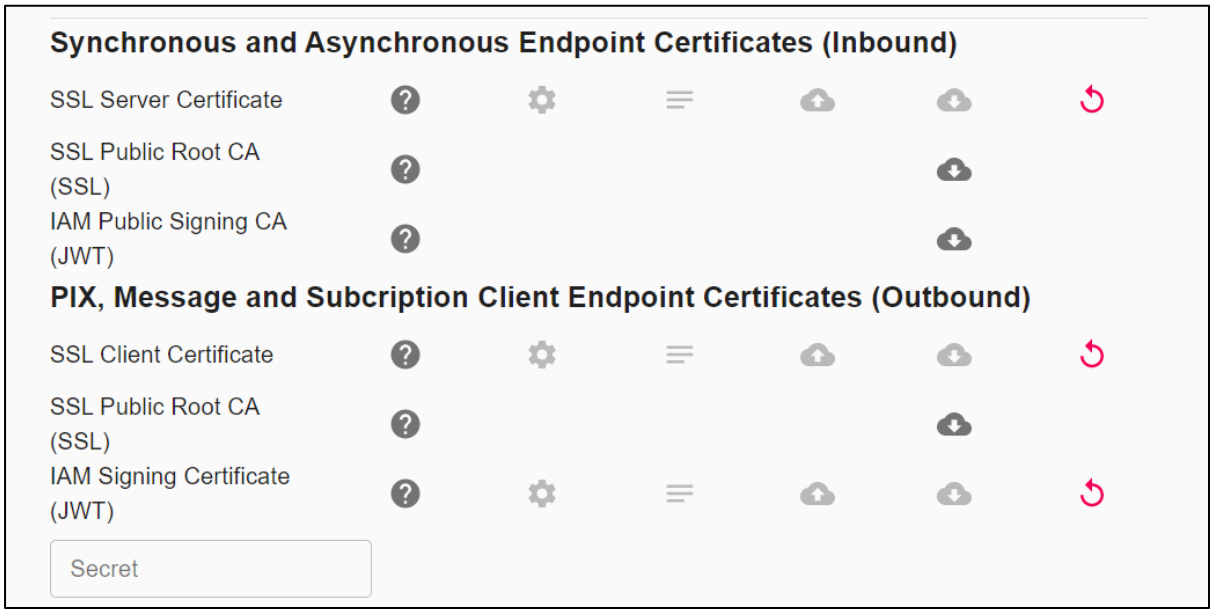
2.5.3 Certificates and Secret

Access to all endpoints is further controlled by two layers of authentication:

1) SSL Mutual Authentication
2) Signed JWT in message

This section therefore allows you to generate and download the various certificates you will need.

NB: Make sure to configure your endpoints and press "submit" before attempting to use this section of the screen. The screen is "smart" and, based on the endpoints you have selected, will only enable the certificates you actually need.



The certificates are in a grid with icons to guide you through the process of generating a Certificate Signing Request.

Note: It is assumed that you already have an understanding of the concepts involved in using a Certificate Signing Request to generate a Certificate. If not it may be useful to search the internet for "Certificate Signing Request process" to read up on the background before continuing

- **Question Mark** – this provides help-text with a brief description of what each certificate is for. It also includes important details of:
    - ***The Interweave Exchange endpoints*** – these are environment-specific and are the URL and path to send requests to, plus the IP address(es) to whitelist on your firewalls to allow incoming traffic.
    - ***Your Provider Client Id*** – this is needed for IAM authentication to acquire a JWT token
- **Cog** – allows you download a Configuration file containing all the necessary details for generating your Certificate Signing Request (CSR)
- **Lines** – instructions for generating a Certificate Signing Request (CSR) from the configuration file. This includes the customised commands for your installation – ready to cut-and-paste into an OpenSSL command line.

- **Upload Cloud** – opens a dialog to select the CSR you have thus generated and upload it. This then creates your certificate, and also downloads it ready to use.
- **Download Cloud** – once the certificate has been generated, allows you to download another copy
    - ***Note*** – there are also several **public certificates** which you will need. These only have a "download cloud" as nothing personalised needs to be generated – the standard pre-generated certificates can simply be downloaded.
- **Circular Arrow** – start again. This resets the certificate generation process to the start and allows you to generate a fresh certificate[1].

Finally, at the bottom of this section is a text box:

- **Secret** – here you can enter a secret (password) that is used – along with your Provider Client Id - for IAM authentication when acquiring a JWT token.

NB: There is no way for anyone (including yourself) to ever see what has been typed in to this Secret. Therefore it is very important to remember what you enter! (You can of course always type in a new secret if you forget – noting however that this will require re-approval).

[1] As of this writing this feature is disabled, and a reset must be manually requested via a Service Request. To be added in a future release.

2.5.4 Data Provider Approval Process

At the very bottom of the screen are two approval tickboxes:

Everything in the screen is a draft and is NOT applied to the actual system until BOTH boxes are ticked.

As you can see, there is one box for "Organisation Approved" – which you tick once you are happy with the configuration. The other box is greyed out as it is for an Interweave Exchange Administrator to review and approve.

Note that this works both ways. For example an Interweave Exchange Administrator can use the screens to change your settings and can tick "their" box once happy. However YOUR approval on behalf of your organisation is also required before the changes become operational.

2.5.5 Other Environments

Once you have saved your Data Provider for the first time, then the **"Environments" dropdown** at the top of the screen becomes enabled. This allows you to switch between environments (Sandpit, Staging, Production) – to continue configuring other environments and to view their settings.

Note: there are governance gates controlling access to the environments beyond Sandpit, and your configuration will not be approved and enabled to connect until it has passed those gates. HOWEVER there is nothing to stop you going ahead to get all of the configuration done in advance, including downloading and installing all of the necessary certificates.

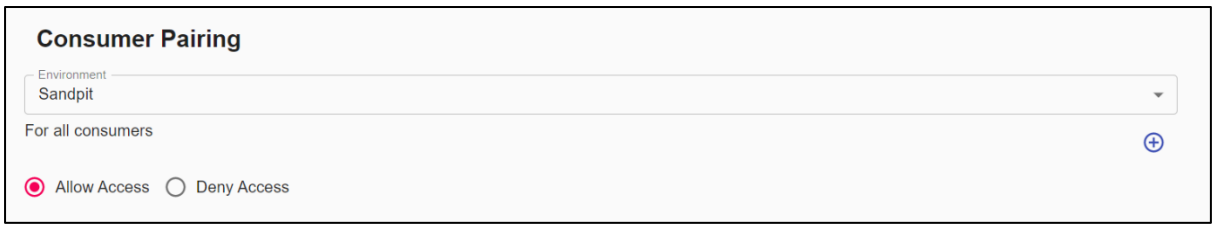
2.6 Provider Settings – Additional Options

Once you have saved the Provider Settings for the first time, additional buttons appear at the top of this screen. These take you to an additional screens, from where you can press the “View Provider” button to return.

2.6.1 View Access Restrictions

This is an important screen in its own right, as it allows you to control what data you make available and to whom. At the top is a selector to choose the environment, and there are then three main sections:

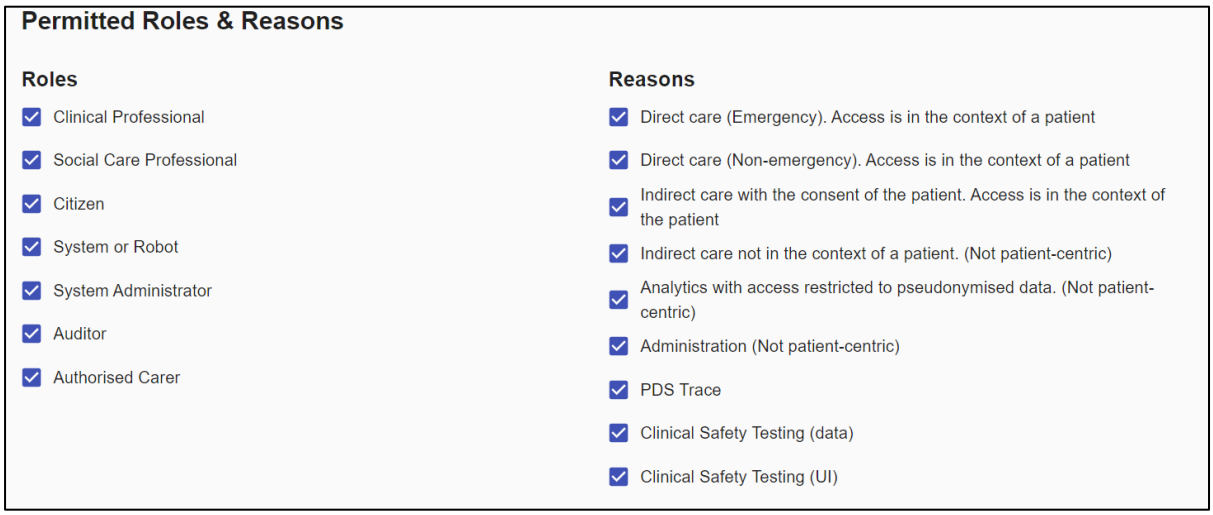
2.6.1.1 Consumer Pairing



By default this is blank, meaning that ALL Data Consumers may access your Data Provider – and this is likely to be the normal setting.

However there is also the option to configure an “include” or “exclude” list of specific Data Consumers who can access your data. This might be used, for example, to enable a limited pilot with a small set of other organisations, or to restrict access based on particular data-sharing agreements

2.6.1.2 Permitted Roles and Reasons

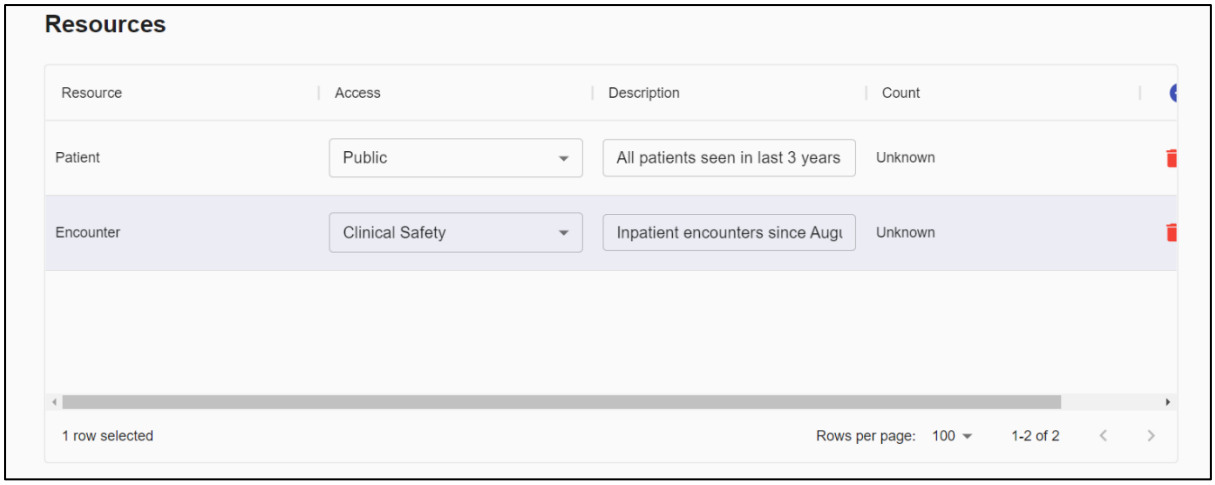


Roles and Reasons are the “permissions” presented by Data Consumers in their JWT tokens. By default all options are permitted, but there is the option to restrict this if necessary.

For example, it might be required to limit access to Clinical and Social Care Professionals only, or to limit access for Direct Care purposes only.

(***Note*** that whilst the full list is displayed, there are several administrative / auditor Roles and Reasons which the system will NOT allow you to remove).

2.6.1.3 Resources



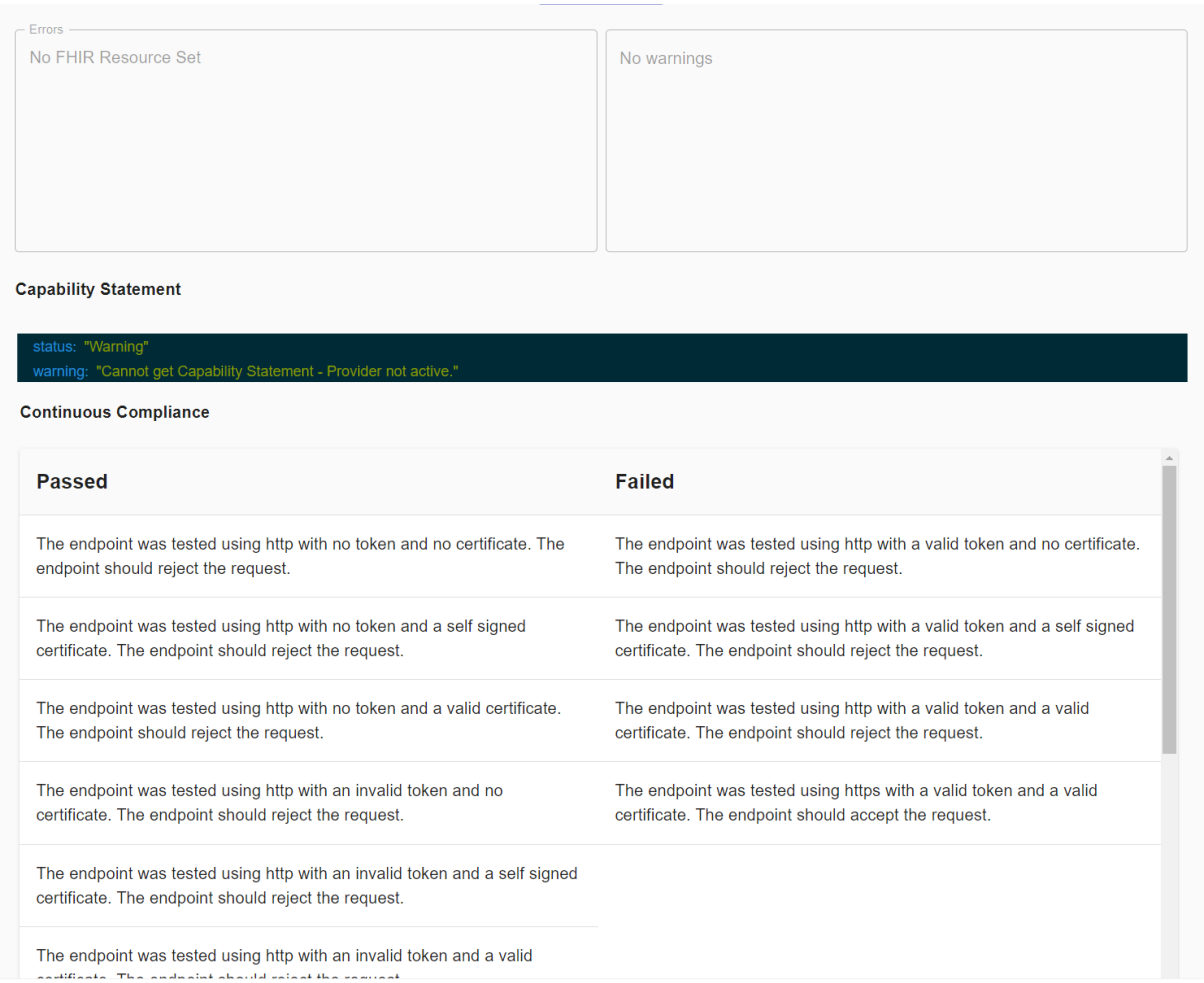
The "Resources" section lists the types of FHIR Resources which you are publishing.

NB: This is a very important section which you MUST populate to enable use of your data. Data Consumer requests will ONLY be routed to you for those FHIR Resource types listed here.

Against each resource is noted:

- **Access status** – normally this will be "***Public***" to allow access to the data. Alternatively a resource can be flagged as "***Clinical Safety***". This will embargo it so that is only visible to testers claiming the specific "***Clinical Safety Testing (data)***" Reason for access.
- **Description** – this provides the opportunity for a short explanatory description which can be shown to users. For example this could describe the coverage and any particular known issues with the dataset.
- **Count** – where possible this indicates the number of data items available. (This is refreshed periodically – eg nightly – and not all Data Providers may support the count feature)

2.6.2 Health Check



This is a good starting point for troubleshooting, as it provides diagnostics about the Data Provider. It is in three sections:

2.6.2.1 Errors and Warnings

This shows the results of running a set of diagnostic and connectivity tests against the endpoint. It is a good place to check that your endpoint is configured correctly and connecting as expected.

2.6.2.2 Capability Statement

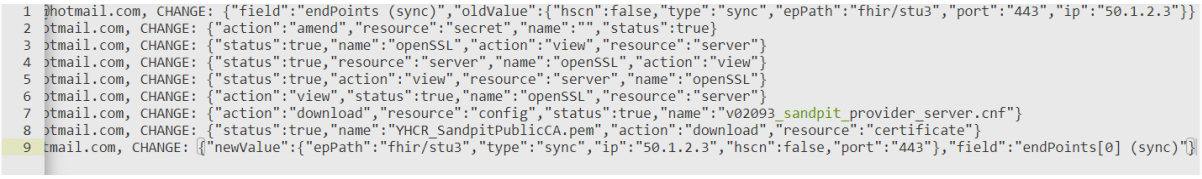
This retrieves the Data Provider's Capability Statement. (A standard FHIR resource containing information about the Data Provider system). Being able to retrieve the Capability Statement is itself a good "smoke test", and furthermore the technical information within provides useful details about the system at the other end.

2.6.2.3 Continuous Compliance

This provides the results from a suite of security tests – which probe the Data Provider endpoint to ensure all of the necessary authentication and certificate checks are in place. Any deficiencies indicate a potential vulnerability which should be urgently addressed.

NB: All of the above checks are run periodically, currently nightly, and so may take some time to update. (There is the option to do an additional run at other times by special request).

2.6.3 Audit Log

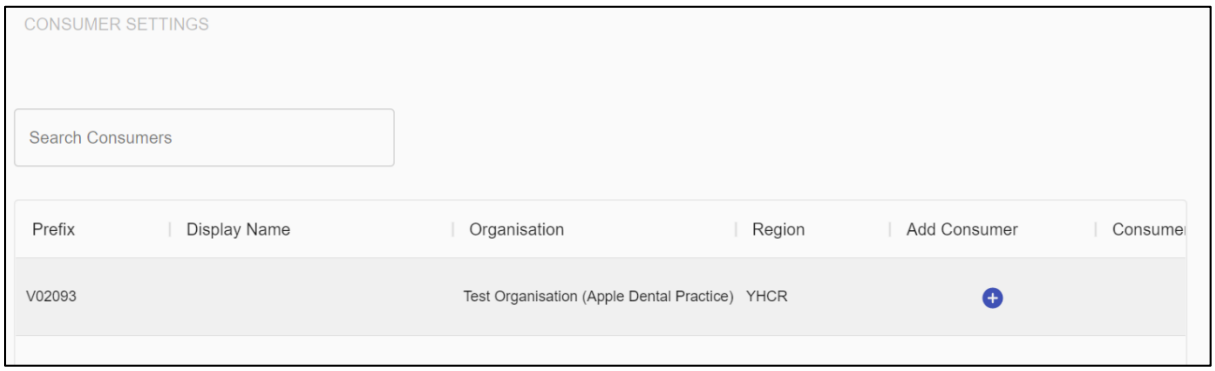


This captures an audit log of all changes to the Data Provider configuration

2.7 Consumer Settings

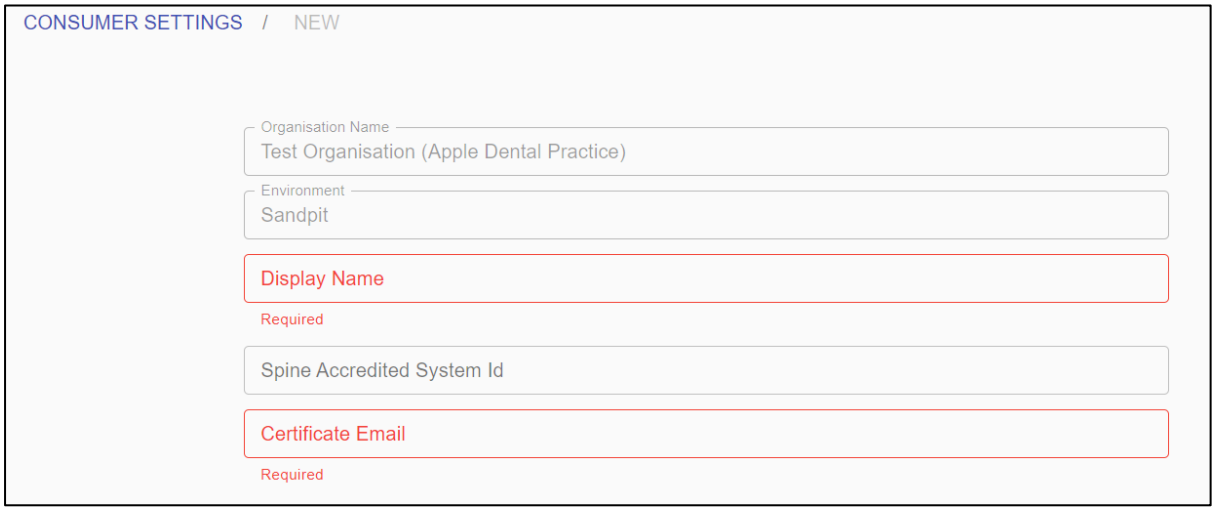
This menu option is the counterpart of “Provider Settings” and allows a Data Consumer endpoint to be configured.

The initial screen shows a summary of your Data Consumer, and you can double-click to go in.



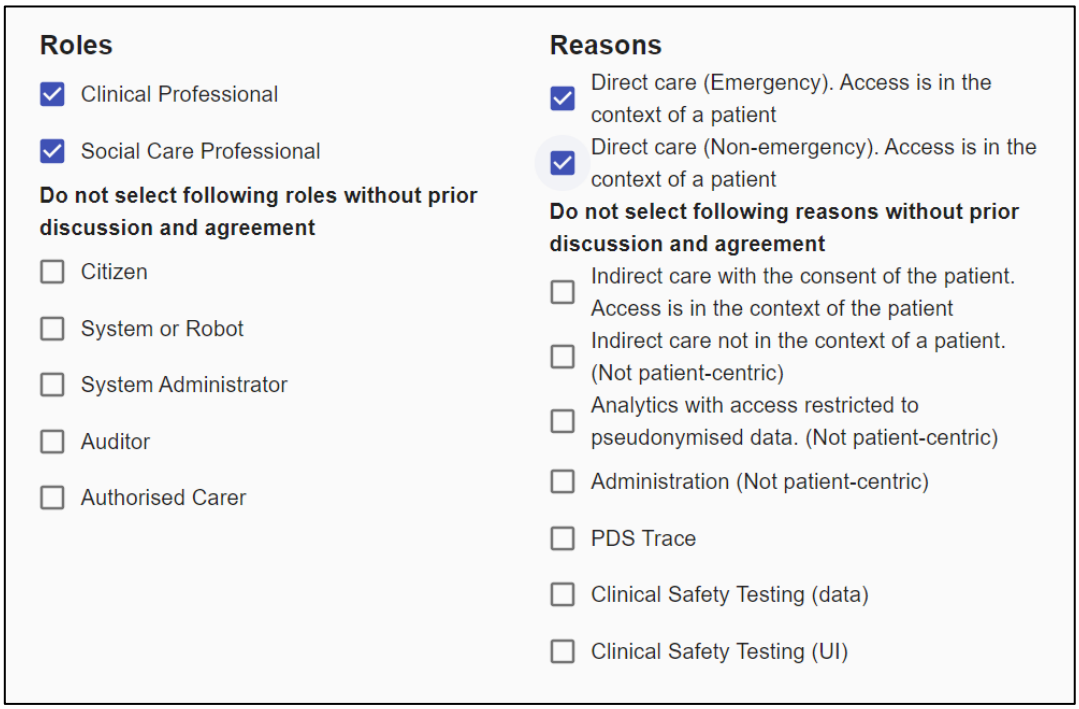
2.7.1 Consumer basic setup

The first step is to enter some basic details:



- **Organisation Name** – is fixed at your own organisation
- **Environment** – is fixed at “Sandpit” initially, as this is the first test environment you will work with. It is possible at a later stage in the process to also select other environments, ie Staging and Production
- **Display Name** – this may be shown on-screen to end users. It should be a short but meaningful summary of who / what your Data Consumer is. In many cases it will simply be your organisation name again. However there are scenarios where it may be different – eg if a technology supplier is creating a single Data Consumer connection for a viewer used by from many organisations.
- **Certificate email** – this is the email which is embedded into the certificates issued. It is required for creating certificates, however there are no current plans to actually send any emails to it. (The email address of a senior worker within your Network & Infrastructure team is recommended).

Beneath this is an important section to configure the Roles and Reasons which your Data Consumer will be permitted to use:



By default nothing is ticked, so to gain access you will need to make some selections. The screen indicates the most likely choices, but there are other permissions which may be relevant to special use cases.

Please follow the principle of "least privilege" and request only the permissions which your Data Consumer actually needs. This will be reviewed before approving your Data Consumer into operation.

Once these details are entered, press "**Submit**" to create a skeleton Data Consumer. Further sections of the screen are now enabled.

2.7.2 Endpoint Configuration

The “Endpoints” section can be expanded to show details of the various endpoints which you may wish to set up for your Data Consumer. Whilst requirements can obviously vary, the endpoints are listed with those most commonly used first.

- **Client (outbound)** – for making requests for data. This is typically the core of what a Data Consumer does
- **Message (inbound)** – for receiving incoming messages containing “pushed” data. (For example, the Ambulance Transfer of Care)
- **Subscription (inbound)** – similar to above, for receiving incoming subscription notifications

Other details of the endpoint configuration work in the same way as for a Data Provider – so see that section for further details

2.7.3 Certificates and Secret

This works in the same way as for the Data Provider – see above for details

2.7.4 Approval Process

This works in the same way as for the Data Provider – see above for details

2.7.5 Other Environments

This works in the same way as for the Data Provider – see above for details

2.7.6 Audit Log

In a similar way to the Data Provider, there is a button at the top of the screen to view “Audit Logs” for the Data Consumer

2.8 Validate FHIR Resource

This menu option is a simple but useful screen for testing.

A FHIR Resource dataset (JSON) can be pasted into the screen, and the “Validate” button used to check it against the relevant FHIR Profile. This is a useful way to self-test your data during development.