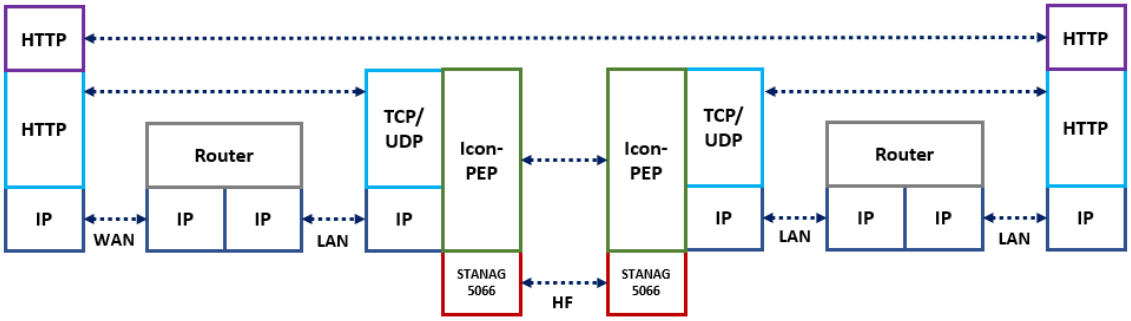
Isode

Icon-PEP 3.0 Evaluation Guide

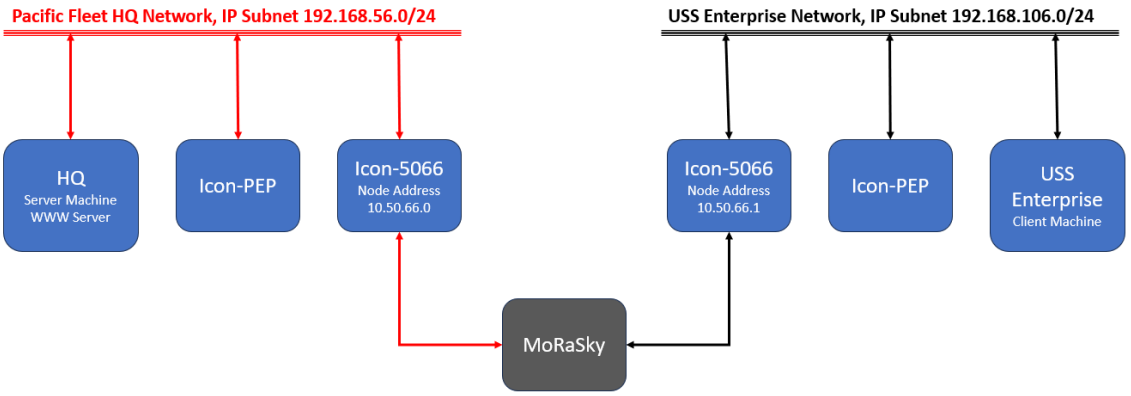
Contents

Introduction

To provide IP services over HF in a reasonably efficient manner, a central challenge is to provide a mechanism to support TCP-based applications efficiently. This can be done with a TCP PEP (Performance Enhancing Proxy) as shown in the diagram below supporting HTTP. By using an optimized protocol over HF, the system inefficiencies of TCP over IP Client can be avoided. Isode's approach is to use [SIS Layer Extension Protocol (SLEP)] (S5066-APP3)]. Note that although this eliminates TCP inefficiency, it cannot address applications with short timeouts or significant hand shaking.



Icon-PEP can be deployed in one of three modes; "Direct", "Tunnel" or "Simple". Tunnel mode requires a router that supports a GRE Tunnel, while this can be achieved in a Virtual Environment using virtual pfSense routers it adds a level of complexity that is likely not necessary for an Evaluation. This guide will cover a "Direct" deployment. The schematic below gives an overview of what we will build.



The "HF Network" will be provided by Isode's Modem, Radio, Sky simulator (MoRaSky).

If you do not have existing Icon-5066 Servers these will need to be configured prior to starting this evaluation.

Objectives

By the end of this evaluation, you will have:

- Installed and configured two Icon-PEP Servers
- Installed and configured two Windows Servers (HQ and MU) to act as WWW Server supporting both the http and https protocols.
- Sent IP Traffic over HF between the two Windows Servers

More information on Icon-PEP can be found at https://www.isode.com/product/performance-enhancing-proxy/ . A comprehensive Administration Guide, which goes into far greater detail than this short document, can be found at *https://www.isode.com/support/*.

Using Isode Support

You will be given access to Isode support resources when carrying out your evaluation. Any queries you have during your evaluation should be sent to *isode.support@isode.com* . Please note that access to the Self-Service Portal for web-based ticket submission and tracking is not available to evaluators.

TAK Server Support

Icon-PEP can support TAK (*https://www.civtak.org/community-tak-server/*) Server Federation over HF. If you are interested in this please contact Isode Support *isode.support@isode.com* detailing what you would like to achieve as this requires additional configuration not covered in this manual.

Preparation

You should visit *https://www.isode.com/support/platform-support/* to discover which operating systems are supported for Isode evaluations. In addition to the server platforms listed, we support the use of Isode server products on Windows 11 for simple evaluations and demonstrations. However it should be noted that Icon-PEP is not supported on Windows platforms.

Isode supports the use of the latest versions of Google Chrome, Mozilla Firefox and Microsoft Edge browsers with the Icon-PEP Console. Internet Explorer is not supported.

Product Download

Product downloads are held in a password-protected section of the Isode website. If you have not already done so you should apply for a username/password by filling in the form located at *https://www.isode.com/request-an-evaluation/*. Products can be obtained by logging into the Isode Customer Portal (*https://www.isode.com/customer-portal/*) clicking on the Product required. The downloads page will give installation instructions specific to your platform.

Product Activation Key

Icon-PEP requires a valid Product Activation Key from Isode before it will run correctly. Keys are issued by Isode Customer Services. Once you have installed Icon-PEP you will need to request a Product Activation Key (PAK) from Isode Support by sending them the Generated Product Activation Request (PAR).

If you haven't already been sent a Key when requesting access to the evaluation files, please send a message to request one to *isode.support@isode.com* remembering to specify which Isode server products you need a Key for. Instructions for what to do with this Key can be found in the Installation section.

Installing Icon-PEP

Icon-PEP 3.0 is only available on Red Hat Linux 8, 9 & 10 (including Rocky Equivalents) and Ubuntu 24.04 & 26.06 you should use the installation method appropriate for your platform.

Icon-PEP can be started the with following command:

% sudo systemctl start iconpepd

To stop Icon-PEP run the command:

% sudo systemctl stop iconpepd

When you make some configuration changes to Icon-PEP you would need to restart Icon-PEP service, you can do so by running the command:

% sudo systemctl restart iconpepd

The directory where Activation and config files are stored on Linux is **/etc/isode/icon-pep.**

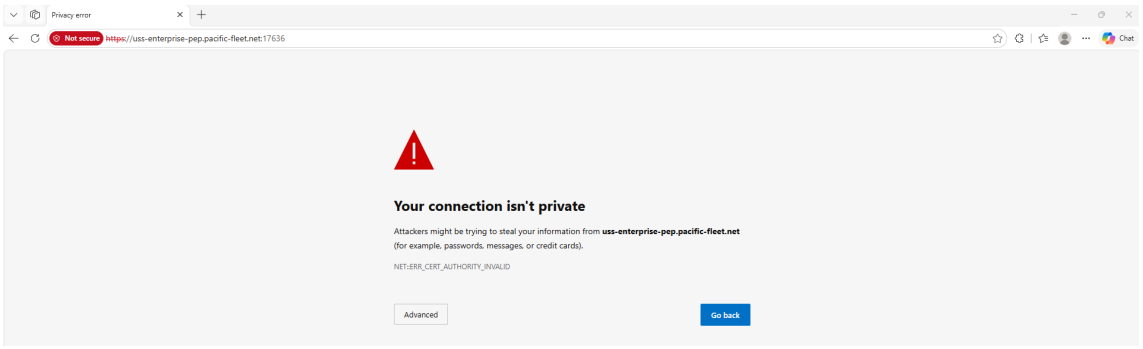
We will be installing in this guide on Rocky 9.

Use the command:-

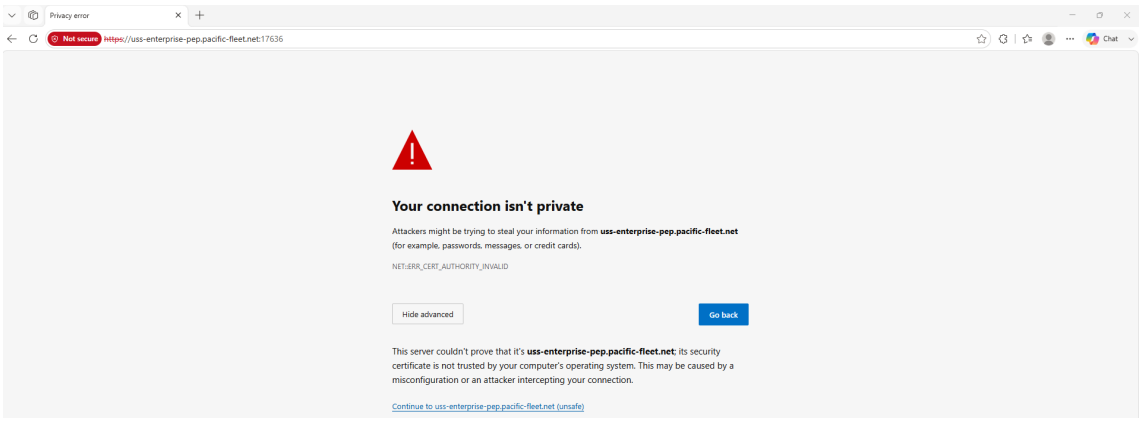
```
# rpm -i ISDiconpep-3.0v0-0.x86_64.rpm
```

Then point a browser at either the hostname (if it resolves) or the IP Address

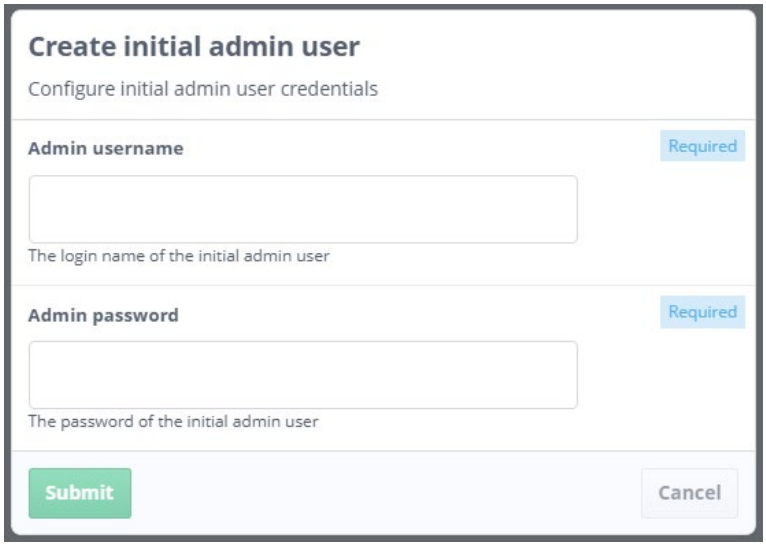
https://uss-enterprise-pep.pacific-fleet.net:17636 .



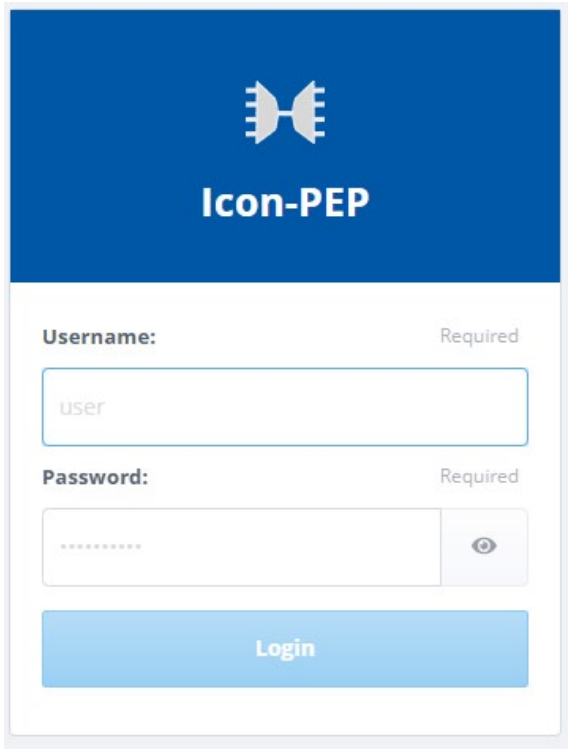
Click “Advanced…”



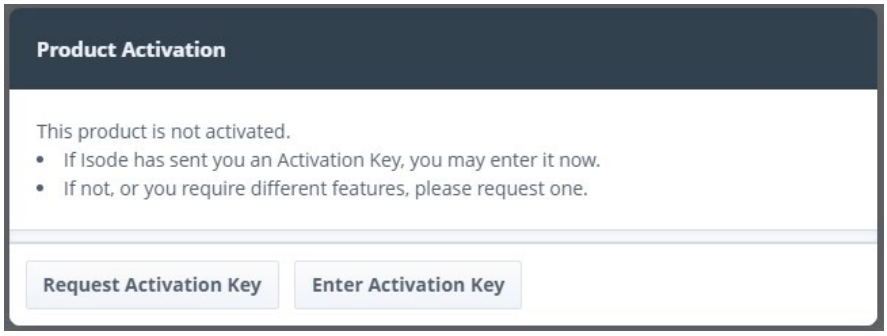
Click “Continue to uss-enterprise-pep.pacific-fleet.net (unsafe)” .



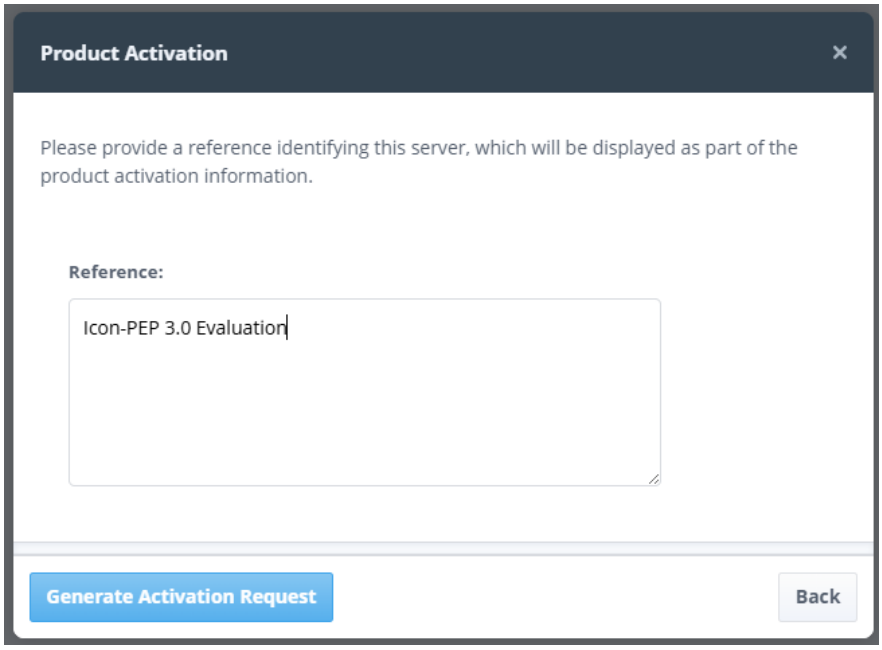
Enter an Admin username and password, we will use “Admin” and “secret”.



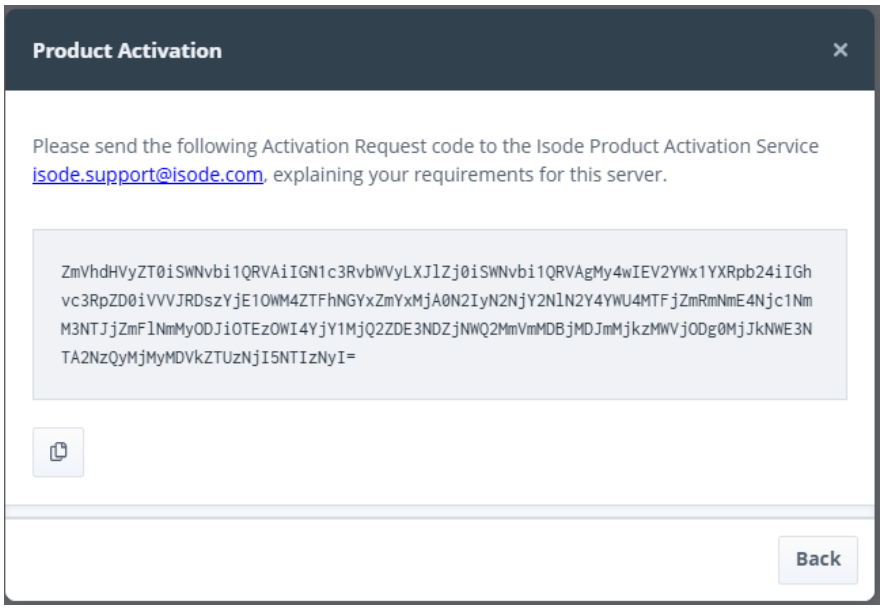
Login with these credentials.



This is where we generate the “PAR” using the “Request Activation Key” button.

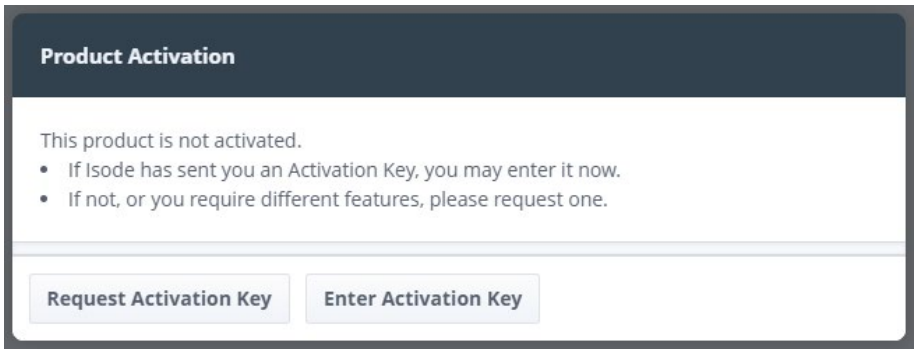


Enter a suitable Reference of your choice and click “Generate Activation Request”.

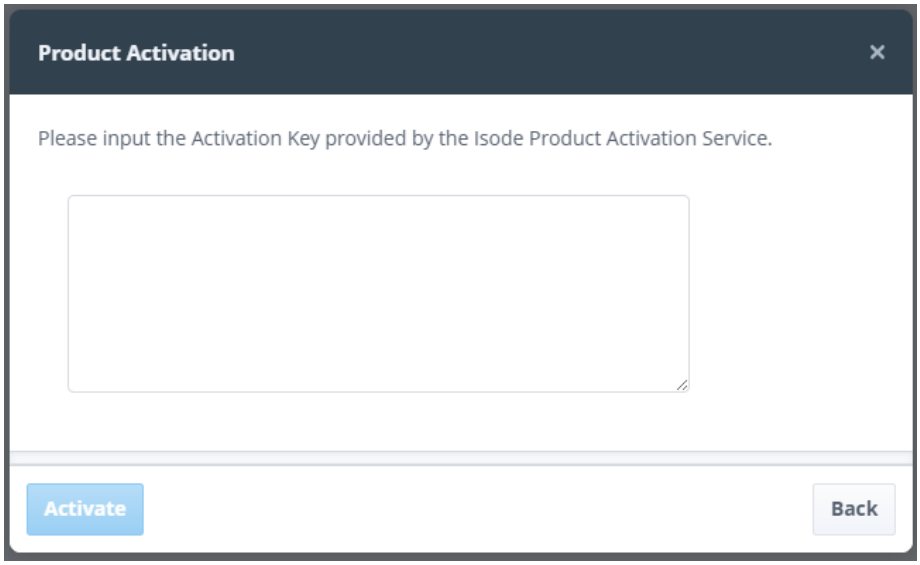


Use the  to copy this request that can then be sent to isode.support@isode.com noting the product you require a Key for and any Project Reference.

When you have received your PAK from Isode Support click the “Back” button.

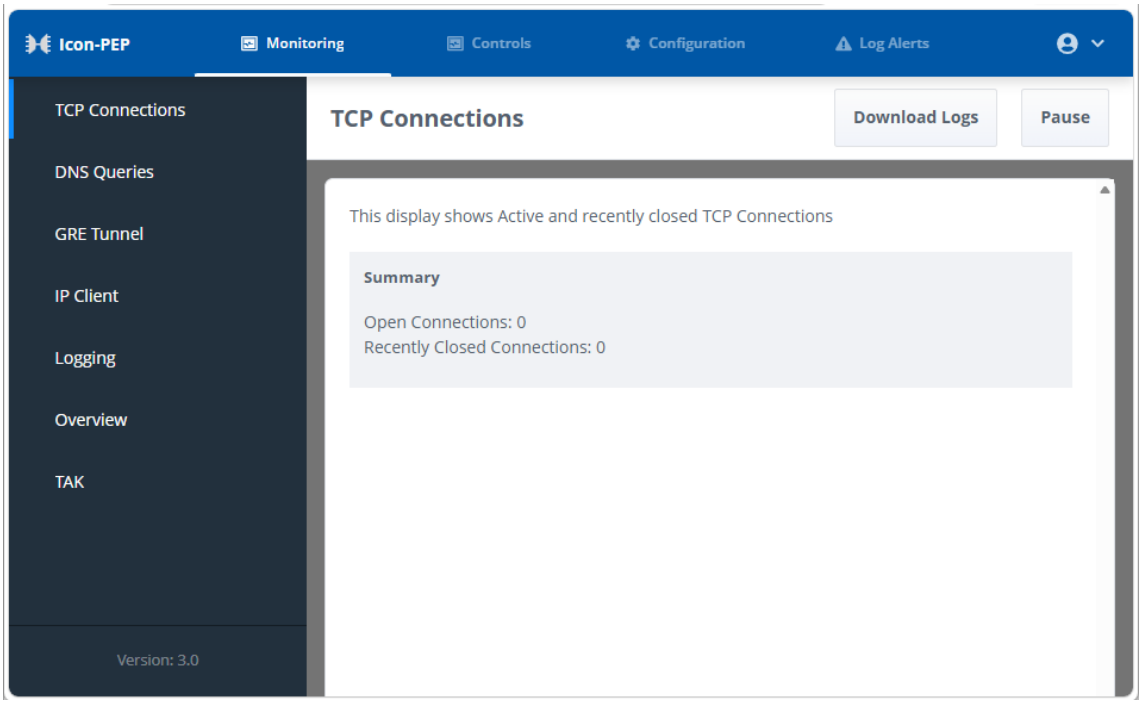


Click “Enter Activation Key”



Paste in your PAK, then click “Activate”.

If successfully activated you will see this screen.



You can now start to configure Icon-PEP.

Below are some important IP Addresses, you should note these down for your system.

Icon-PEP USPF HQ	192.168.56.183
Windows Server/Client USPF HQ	192.168.56.100
Icon-5066 USPF HQ	192.168.56.101
Icon-PEP USS Enterprise	192.168.106.189
Windows Server/Client USS Enterprise	192.168.106.120
Icon-5066 USS Enterprise	192.168.106.120

Note that the Icon-5066 USS Enterprise & Windows Server/Client USS Enterprise have the same IP because in this setup they are the same server. That may well not be the case in your setup.

Configuring Icon-PEP

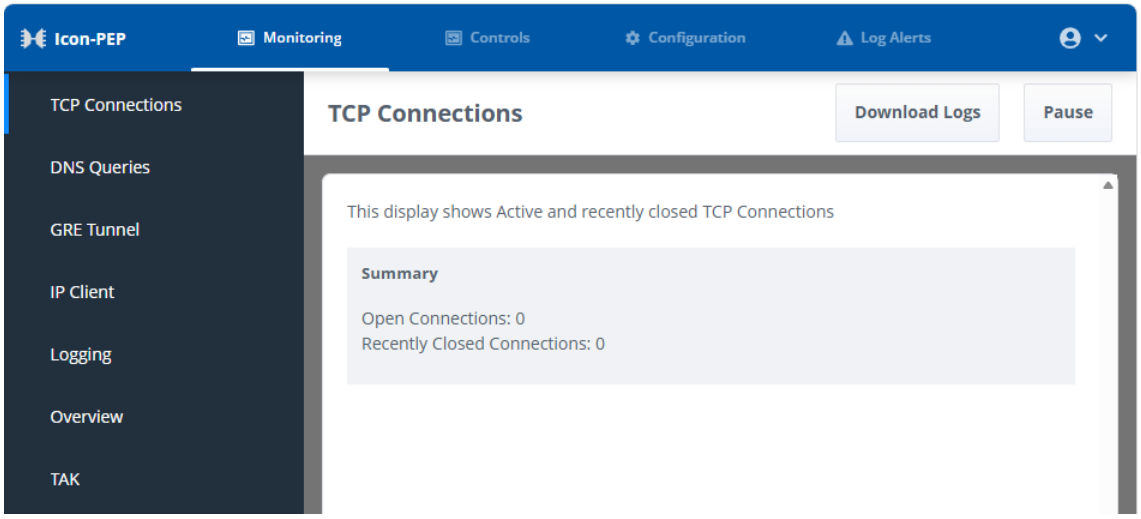
More information on Icon-PEP can be found on the Isode website at https://www.isode.com/product/performance-enhancing-proxy/.

Detailed configuration and operational information on Icon-PEP can be found in the Admin Guide available from the Isode website at

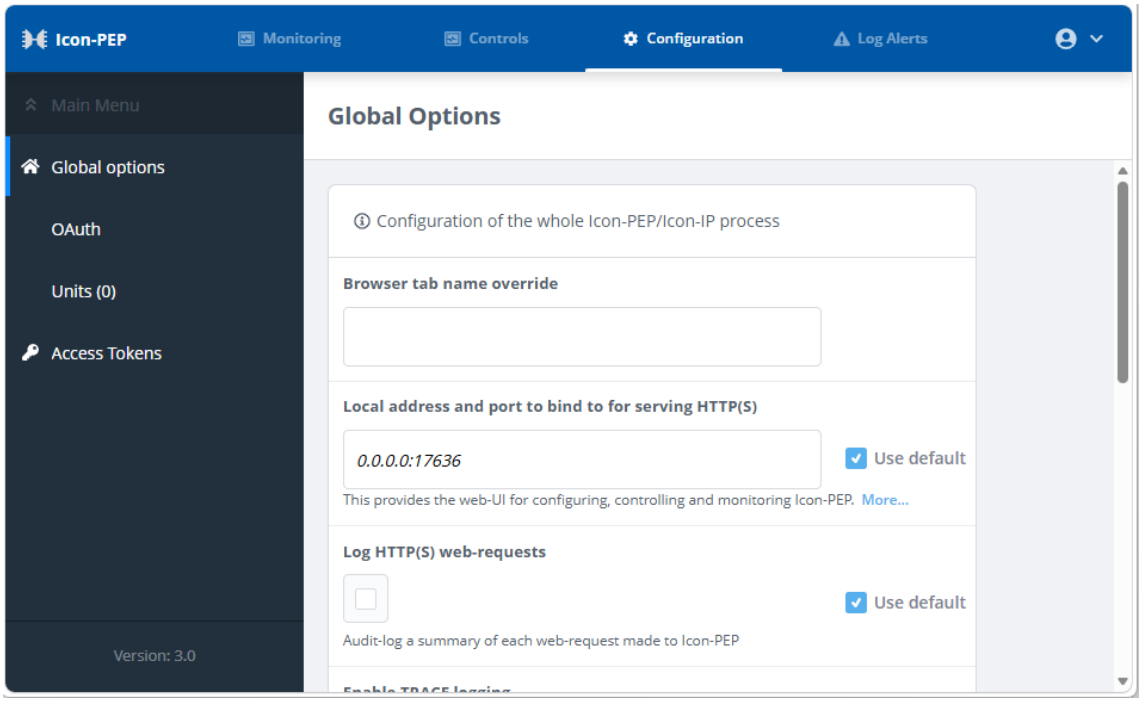
https://www.isode.com/wp-content/uploads/2023/08/Icon-PEP-3.0-Admin-Guide.pdf

Icon-PEP is configured using a Web GUI that is accessed at https://ip-address-or-hostname:17636. I will show screens from the USS Enterprise below with notes on what should be different on the USPF HQ.

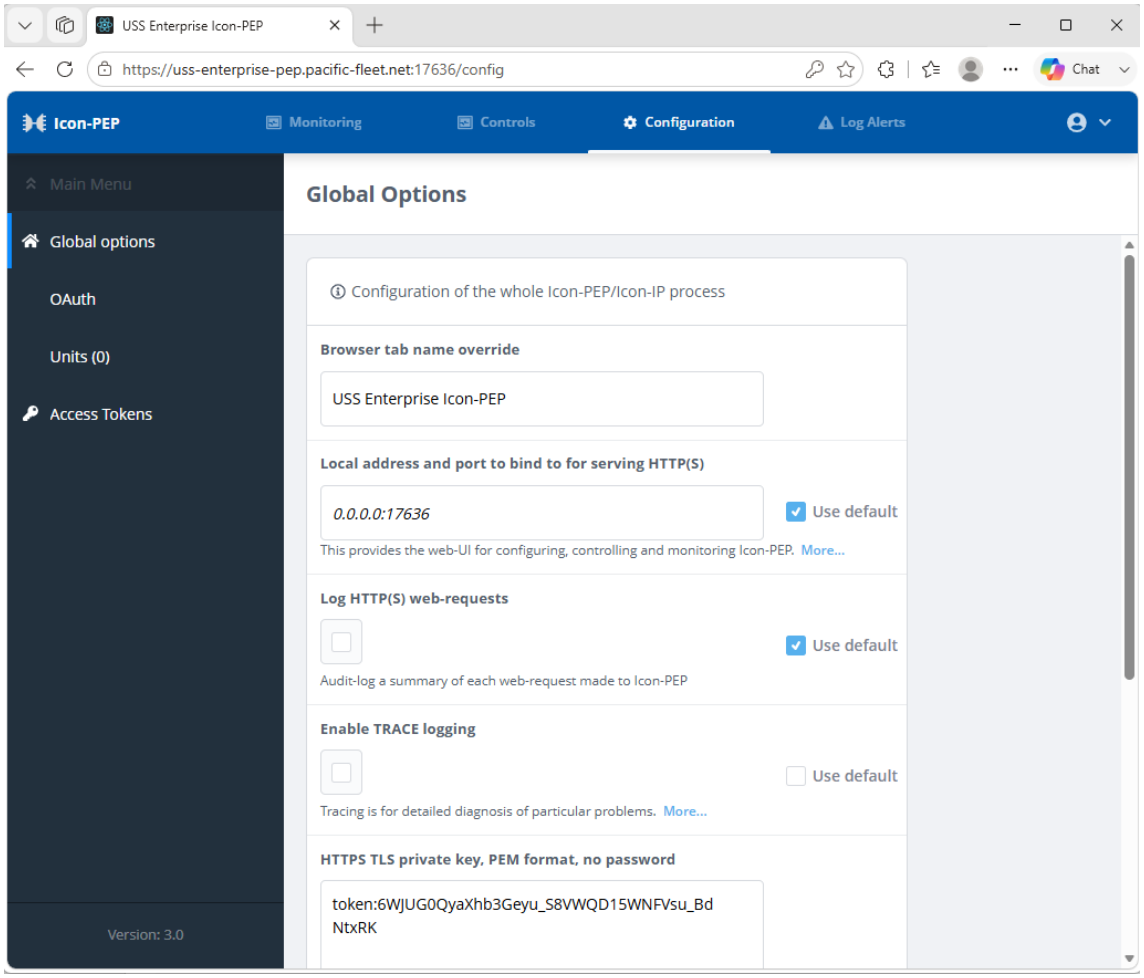
Below is the initial screen.



Select Configuration.



The server comes with an “Autogenerated TLS Certificate”, hence the warnings on the initial screen after installation. If you want a certificate that matches the fully qualified hostname of the server then you need to use some tools to generate a Private Key with no Password and Certificate Chain, both in .pem format. That you load into this initial screen. Setting the “Browser tab name override” is useful if you have multiple Icon-PEP servers so you can see which one you are on. We have configured both the TLS and “Browser tab name override”, as you can see below.

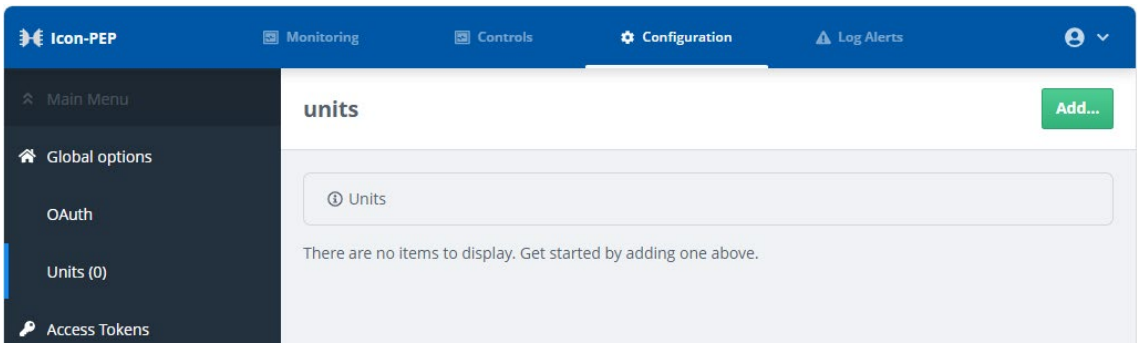


For the USPF HQ you would likely give it a “Browser tab name override” of “USPF HQ Icon-PEP” and load appropriate TLS configuration.

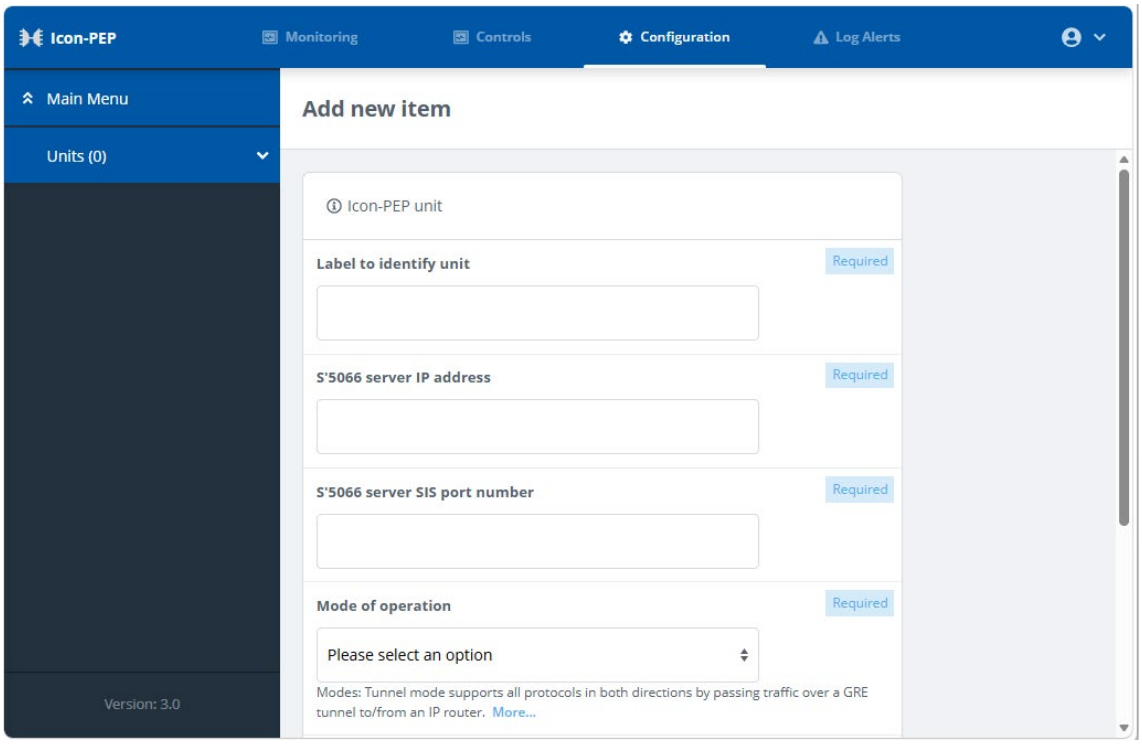
Click the Submit button after all changes have been made.

Unit Configuration

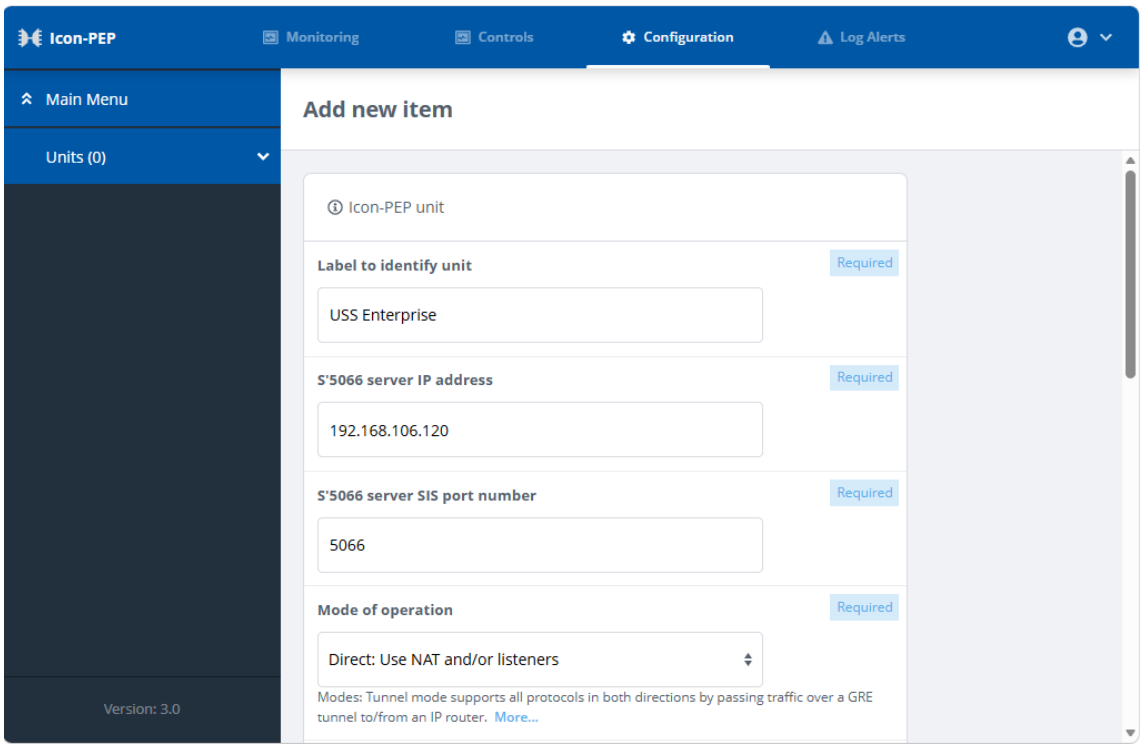
Select “Units”.

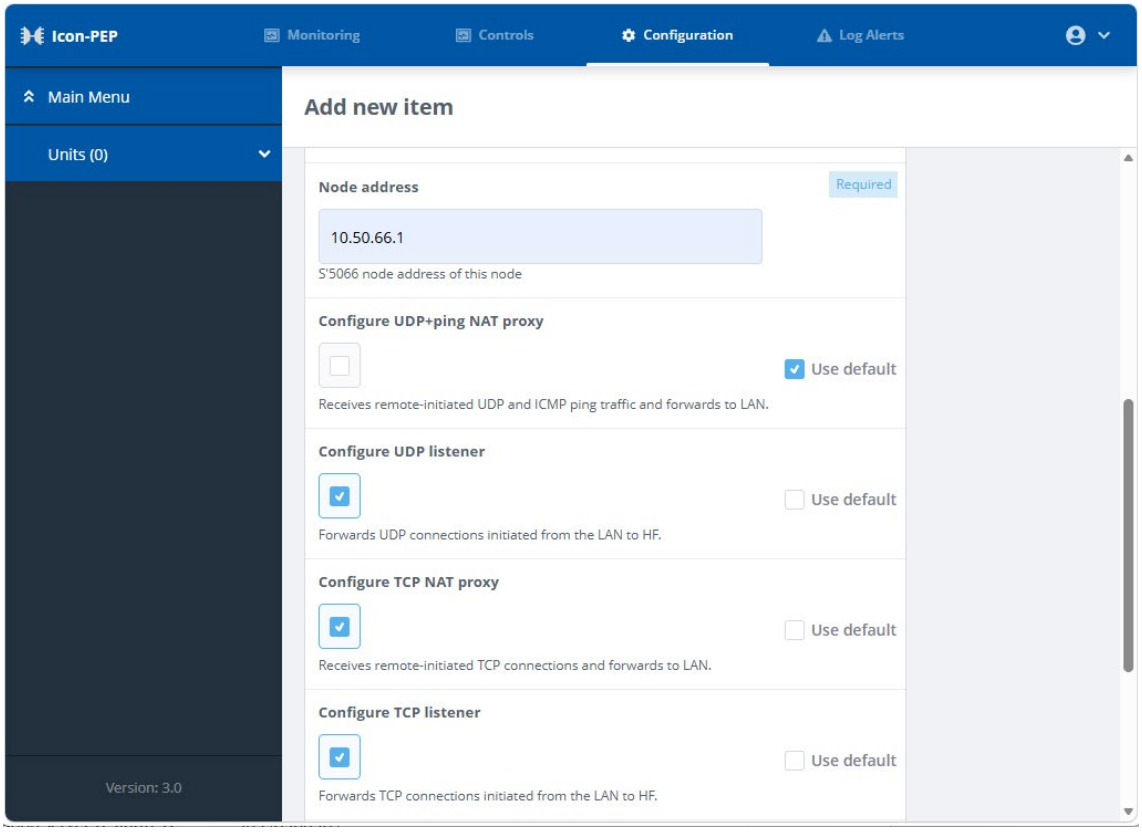


Click “Add...”

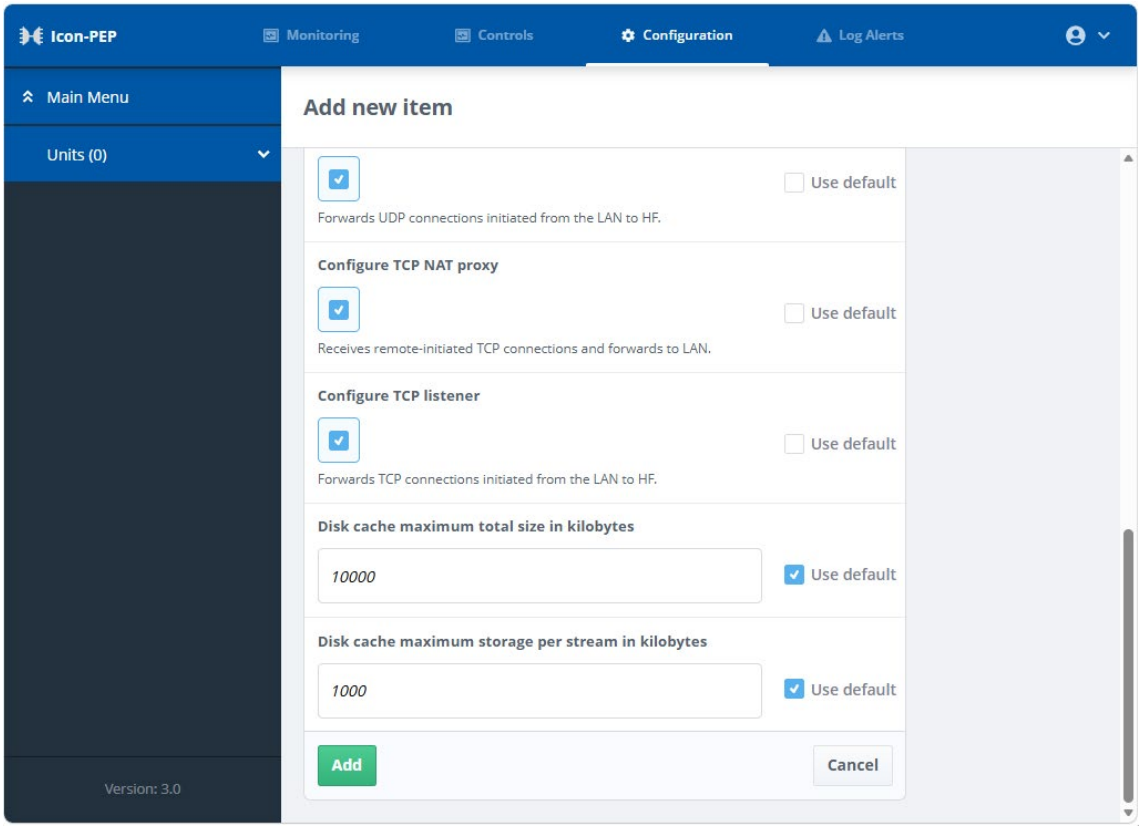


Enter the details below, selecting the “Mode of operation” from the drop down.





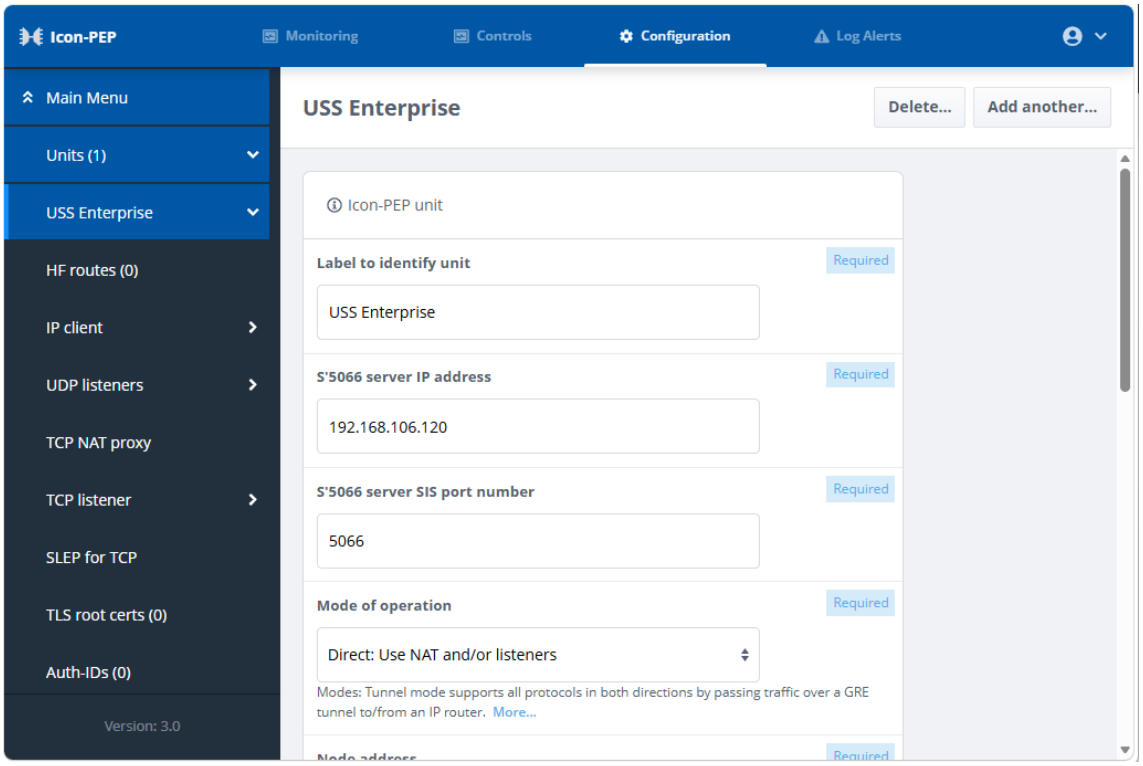
Continued on next page.



Click “Add”.

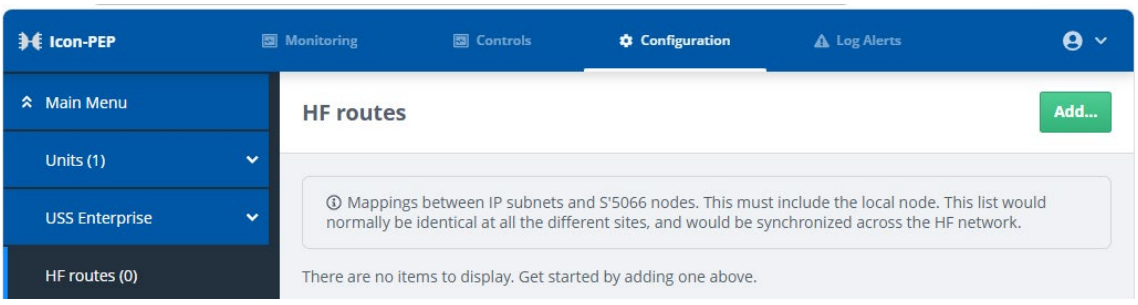
For the USPF HQ the following details are different.

Label to identify unit:	USPF HQ
S’5066 server IP address:	192.168.56.101
Node address:	10.50.66.0

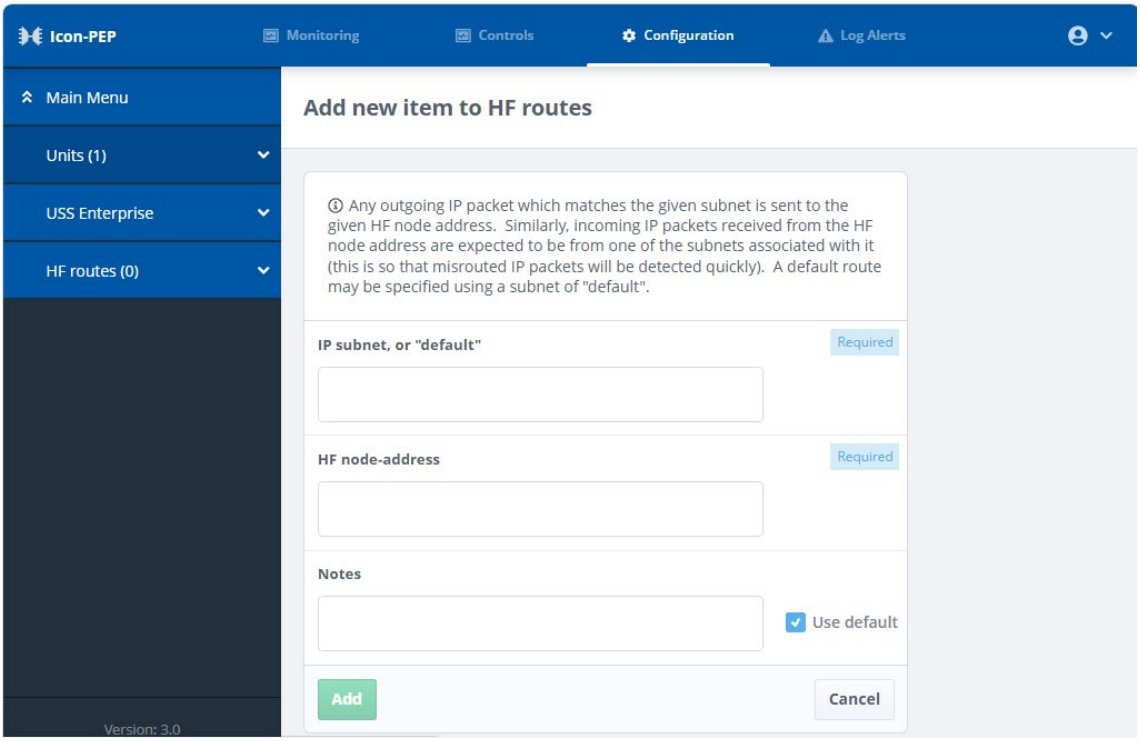


HF Routes Configuration

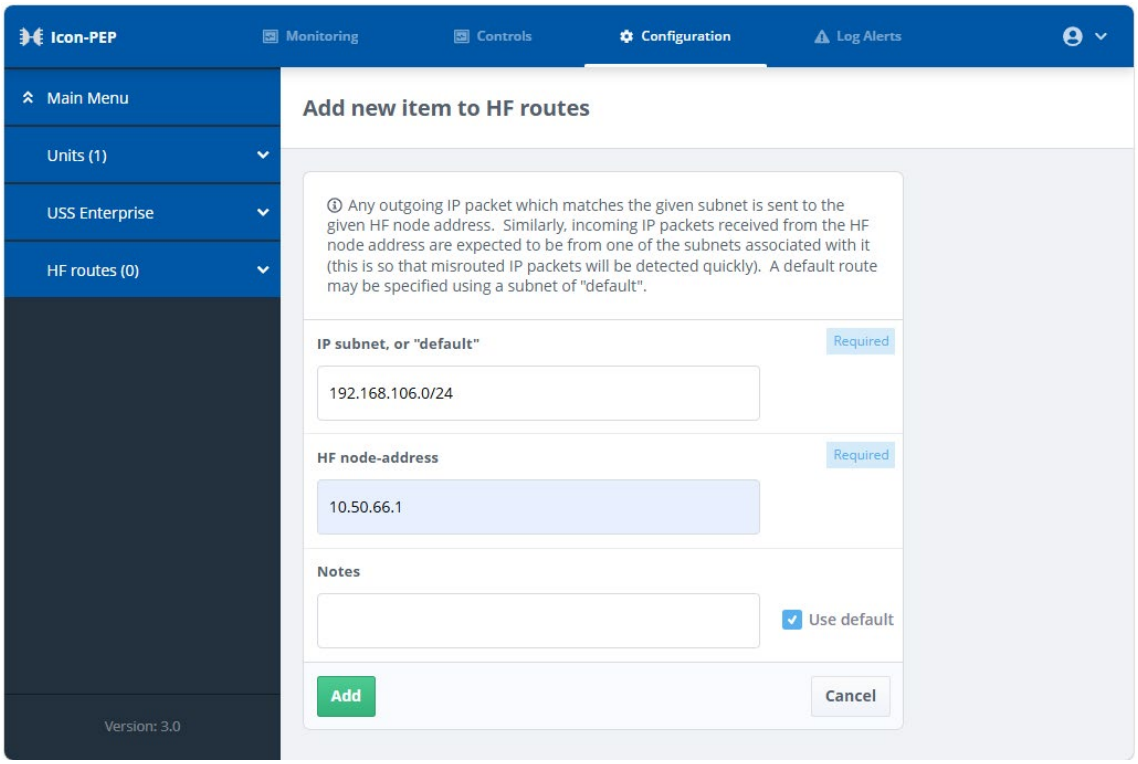
We now need to add two HF Routes, one for each subnet, these will be the same on both nodes. Select "HF Routes.



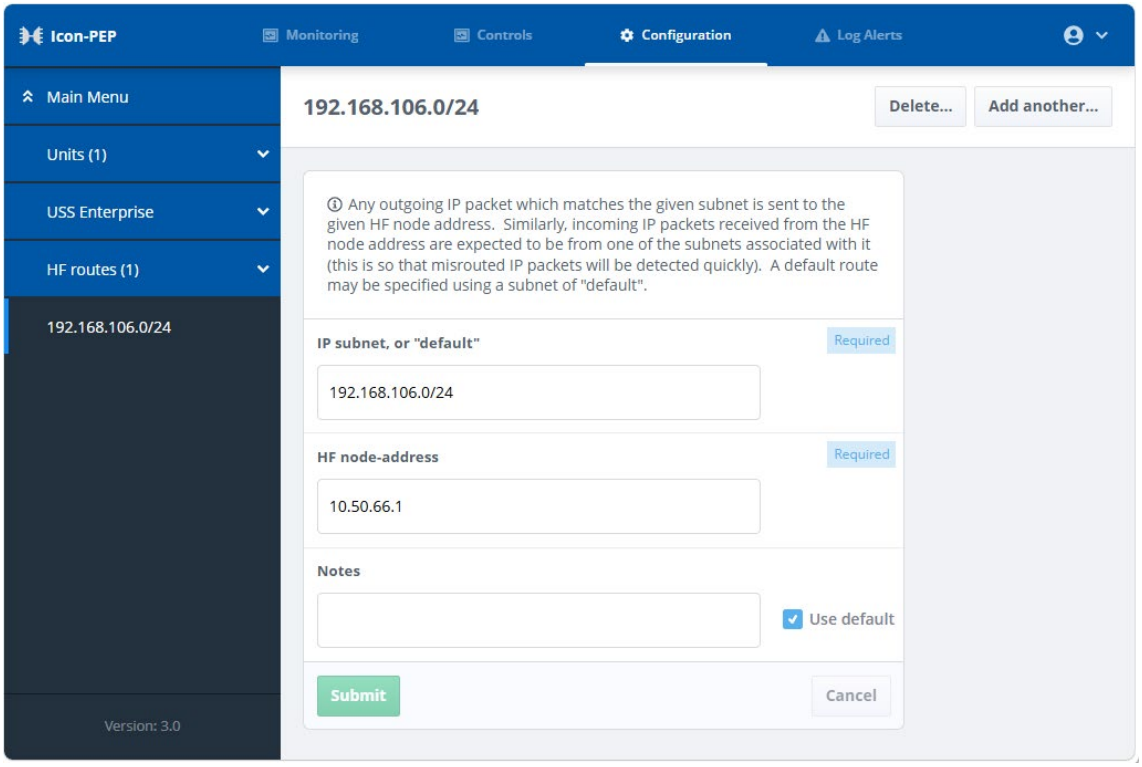
Click "Add..."



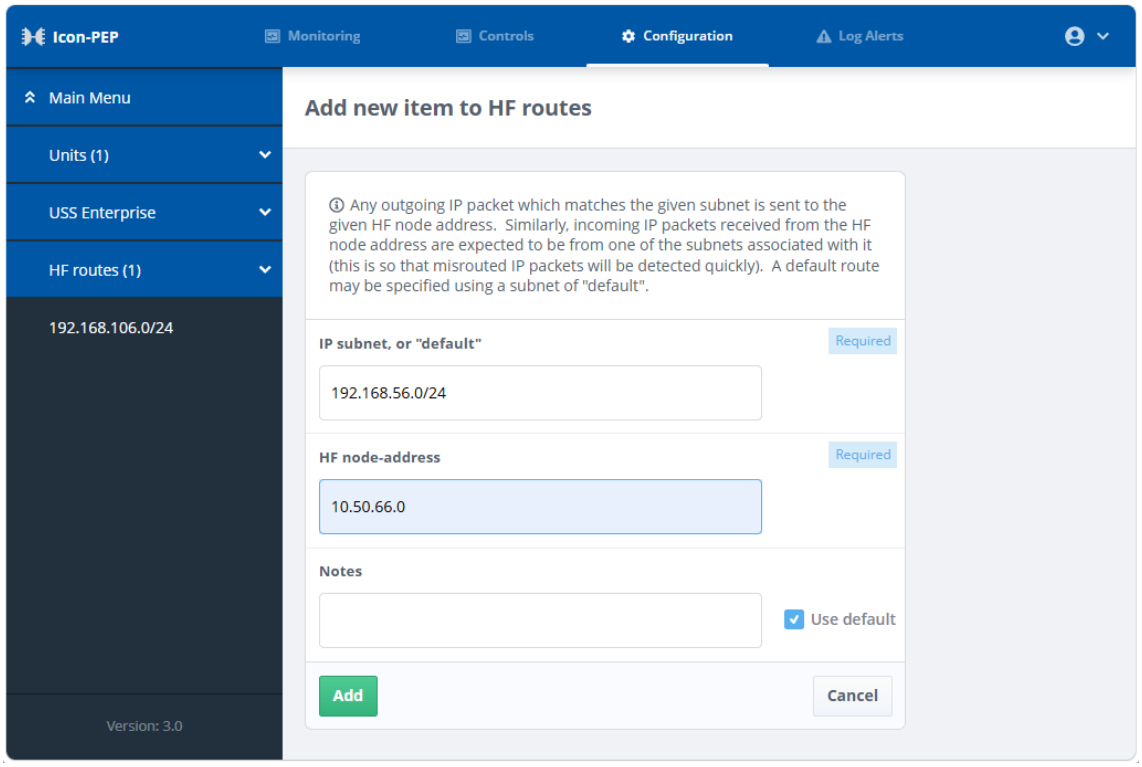
You should enter the Subnet associated with each S'5066 Node Address. The Notes section is optional, but in the example below you could have entered USPF HQ.



Click "Add..."



Click “Add another...” and enter the details below.

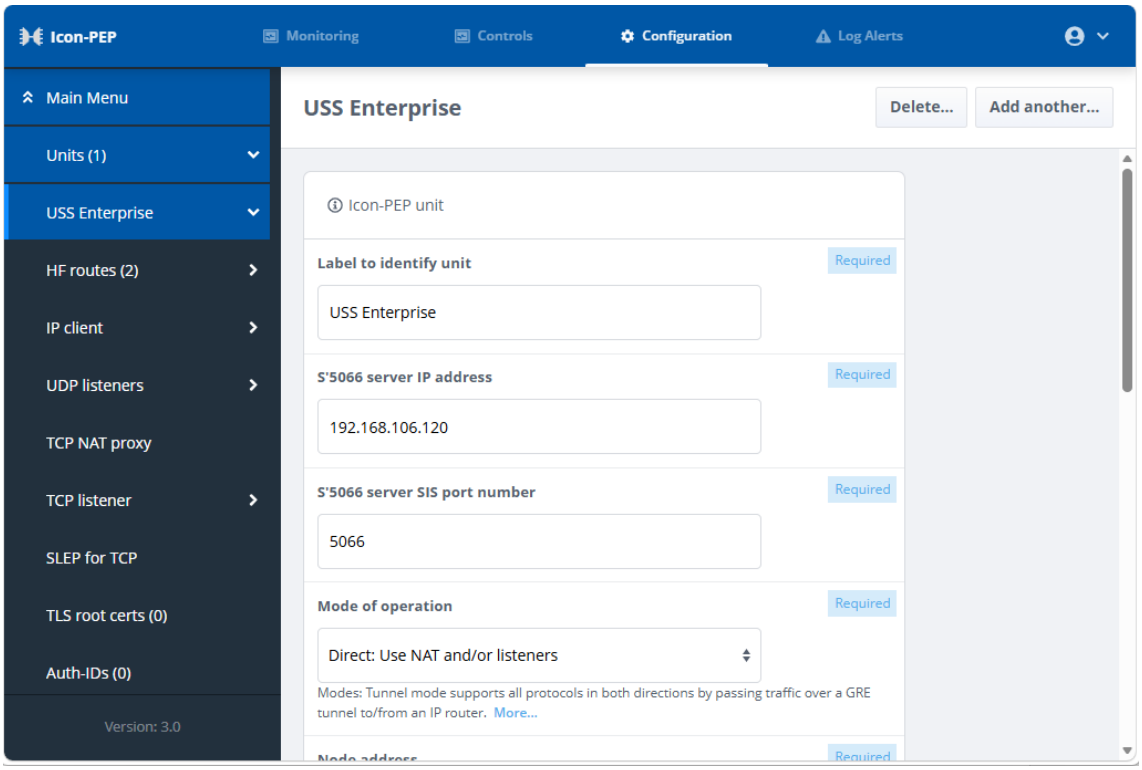


Click “Add”.

The new route will appear on the left-hand side.

You have now configured the Icon-PEP server such that any traffic it receives for either of the Subnets will be directed to the local S'5066 server. In the case of traffic it receives over the HF Network for the local Subnet this will be routed to the local LAN.

Now click on your "Unit" on the left-hand side, in this example USS Enterprise.



You will note that we now have a "2" next to "HF Routes".

Configure TCP Listeners

The next thing we need to configure is the TCP Listeners for each protocol we want to send over HF. What you do is map the Icon-PEP IP Address to the actual IP Address on the Remote HF Subnet. The Local Client will have the Icon-PEP IP Address as that of the remote IP Address either by DNS or a local "hosts" file.

We will configure this for the "http" and "https" protocols. You can only configure this for one remote Website as Icon-PEP can only map it's IP Address to one Remote IP Address per Local Port.

Here is the relevant information for this Icon-PEP (USS Enterprise).

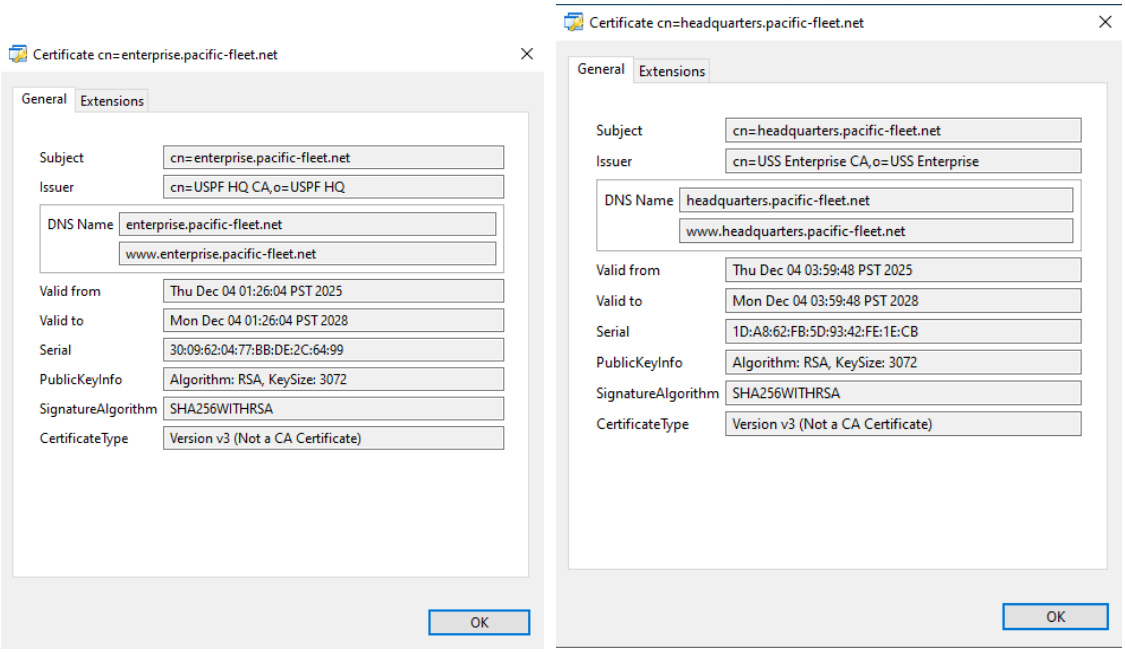
Client Hostname	Protocol	Local IP	Destination address	Remote Node
headquarters.pacific-fleet.net	http	192.168.156.189	192.168.56.100:80	10.50.66.0
headquarters.pacific-fleet.net	https	192.168.156.189	192.168.56.100:443	10.50.66.0

This is the relevant information for the USPF HQ Icon-PEP.

Client Hostname	Protocol	Local IP	Destination address	Remote Node
enterprise.pacific-fleet.net	http	192.168.56.183	192.168.156.100:80	10.50.66.1
enterprise.pacific-fleet.net	https	192.168.56.183	192.168.156.100:443	10.50.66.1

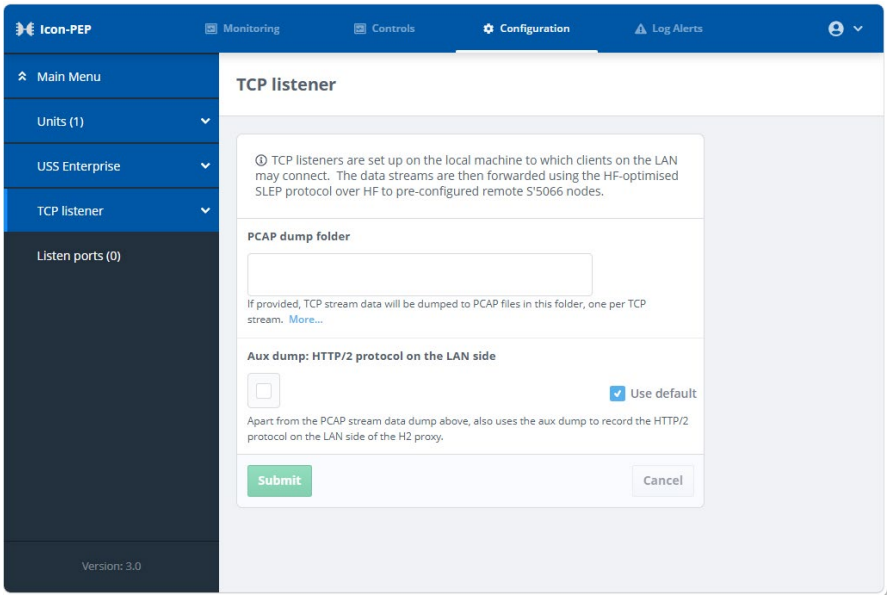
For any protocol requiring TLS you will need to create a Certificate representing that Remote Hostname and issued by a Certificate Authority accessible on the Local LAN. This considerably reduces the traffic over HF as the TLS handshaking is done over the local LAN. You will need both the Certificate Chain and Private key (with no password) for the TLS connection.

These are examples of the Certificates.

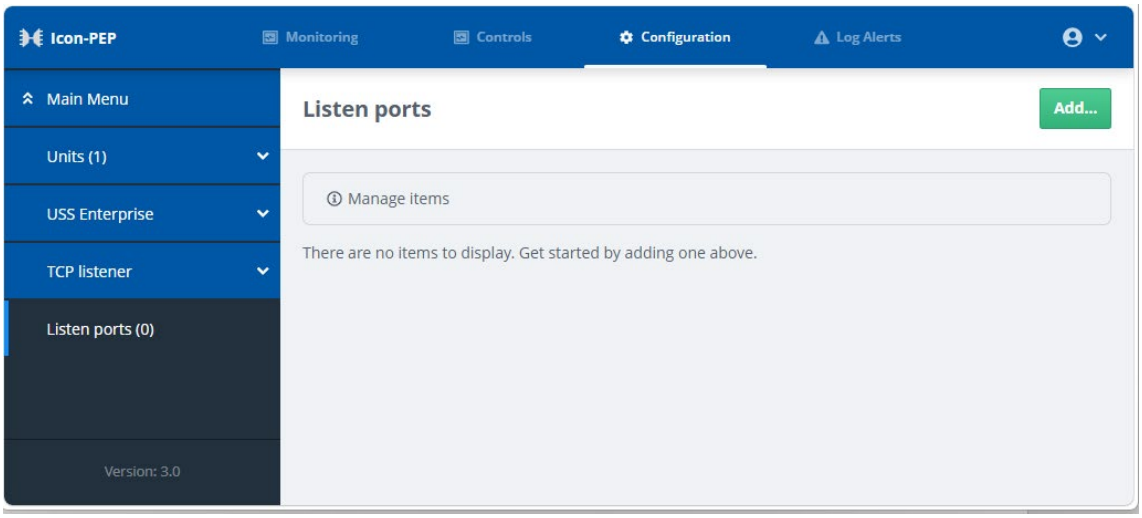


We will start with the http protocol.

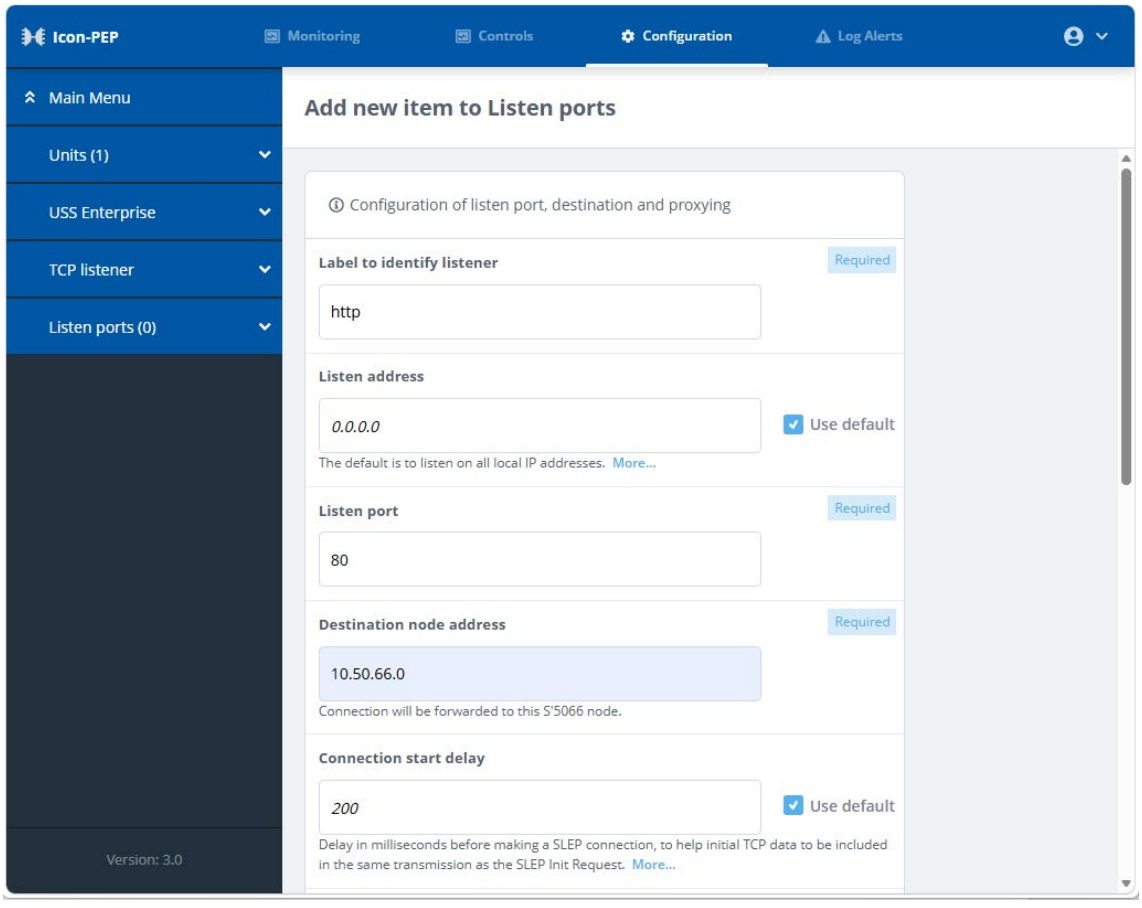
Click “TCP listener”.



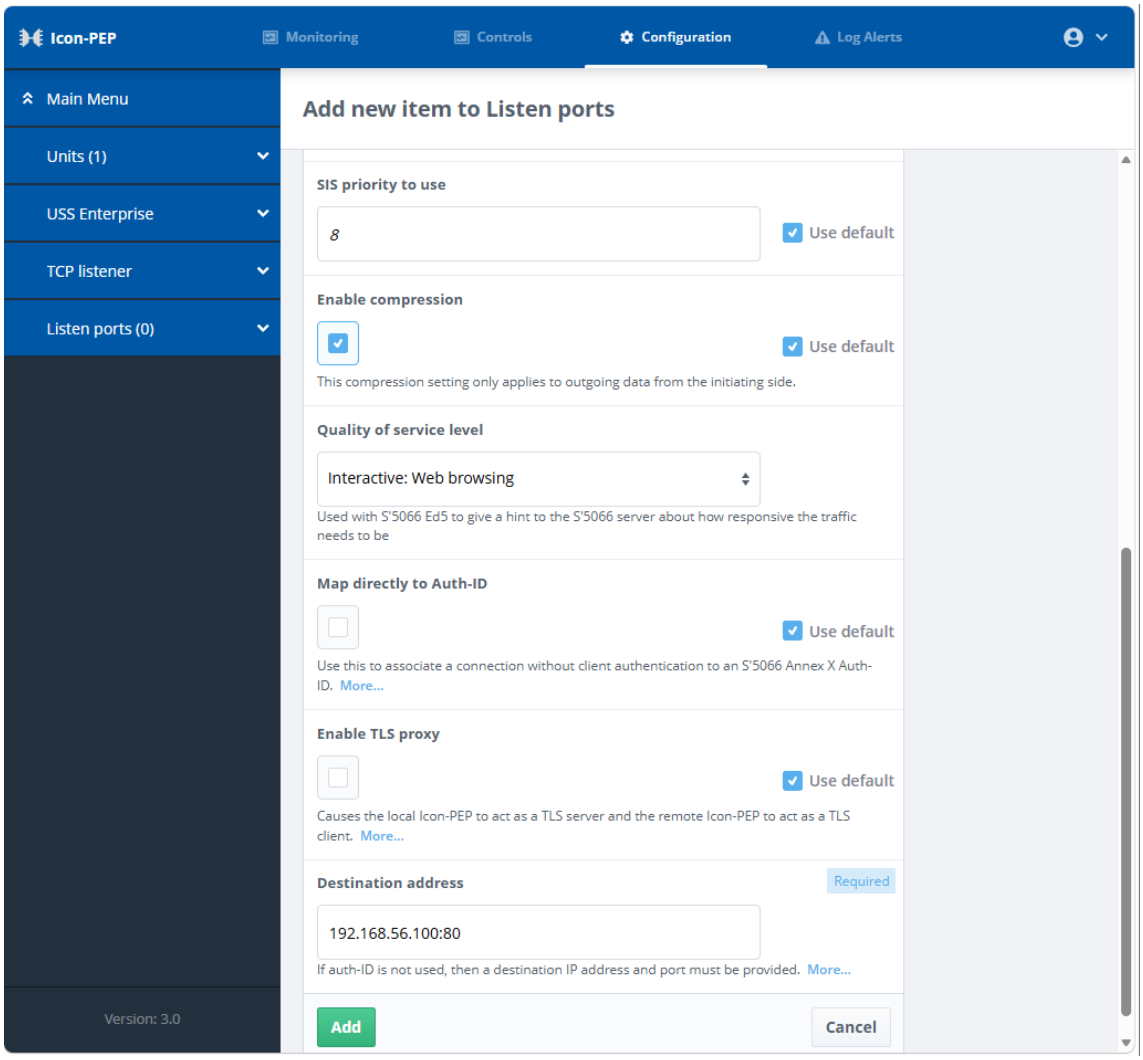
Click “Listen Ports”.



Click “Add...”, for the USS Enterprise Complete as follows.



...continued on next page.

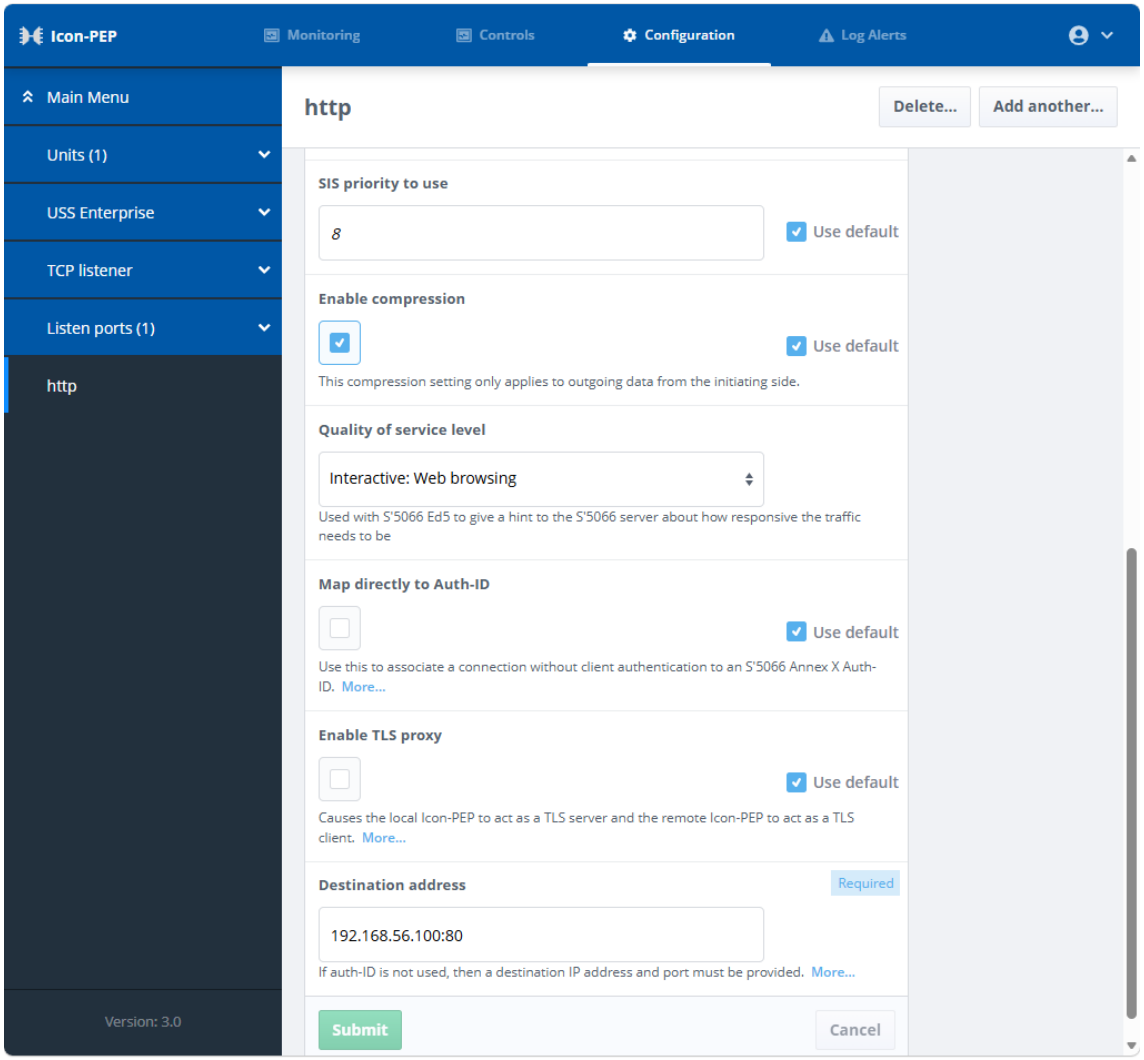


Click Add.

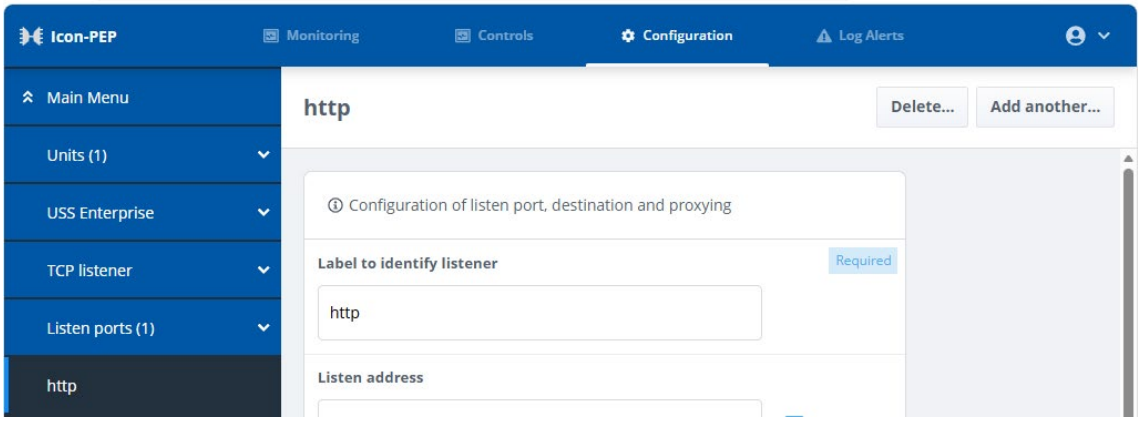
Use the following Values for USPF HQ.

Label to identify listener:	http
Listen port:	80
Destination node address:	10.50.66.1
Destination address:	192.168.106.120:80

When you have entered this information click “Add” and you will see this.



Note the "1" next to the "listen ports".



Before you Click "Add another..." make sure you have the ".pem" files, examples are shown on the next pages.

Click “Add another…”

Use the following Values for USS Enterprise.

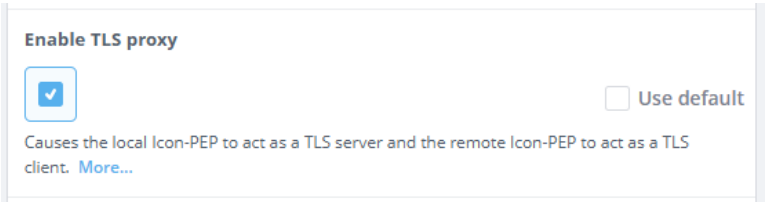
Label to identify listener:	https
Listen port:	443
Destination node address:	10.50.66.0
Destination address:	192.168.56.100:443

Use the following Values for USPF HQ.

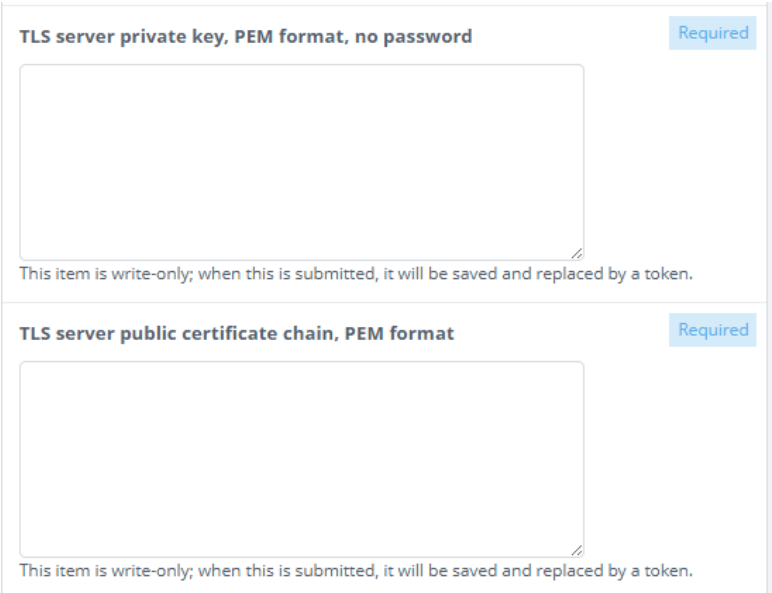
Label to identify listener:	https
Listen port:	443
Destination node address:	10.50.66.1
Destination address:	192.168.106.120::443

When you have entered this information click “Add” and you will see this.

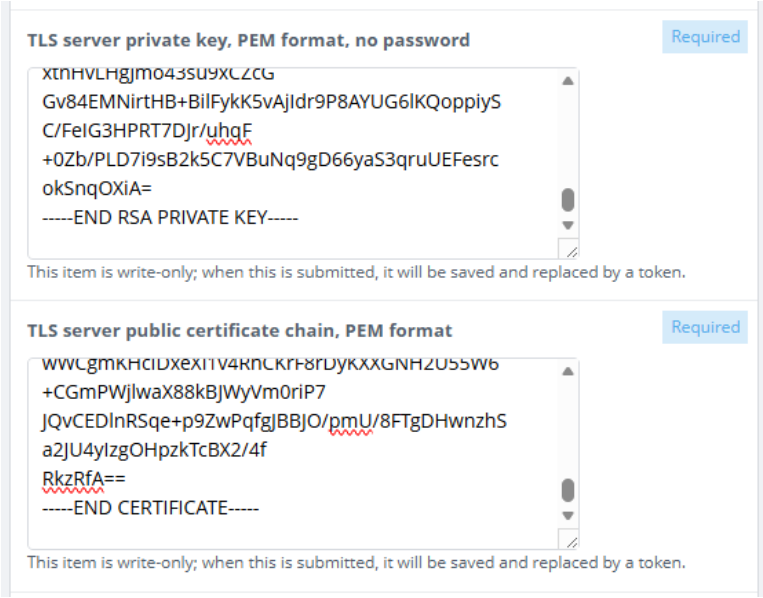
You will also need to check the “Enable TLS proxy”



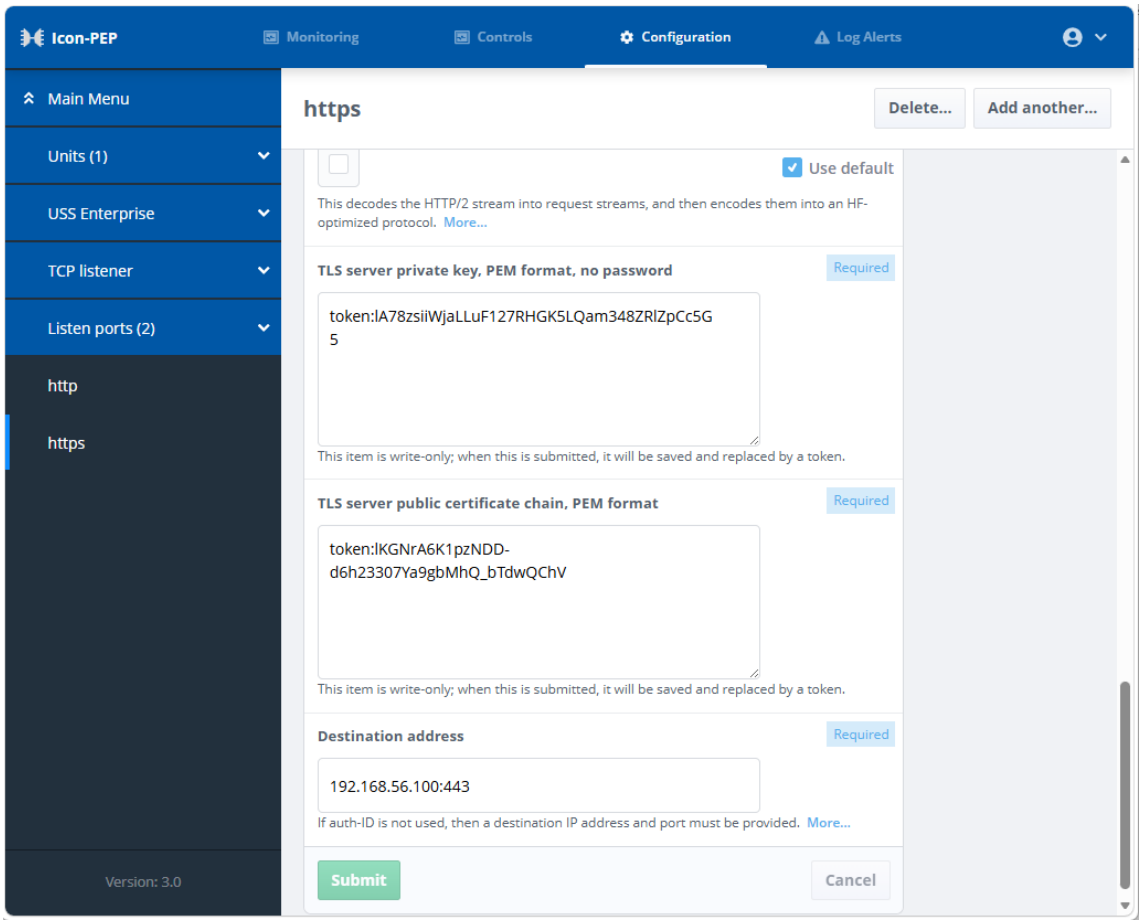
This will expose these Fields.



Paste in your Private Key and Certificate Chain .pem files.



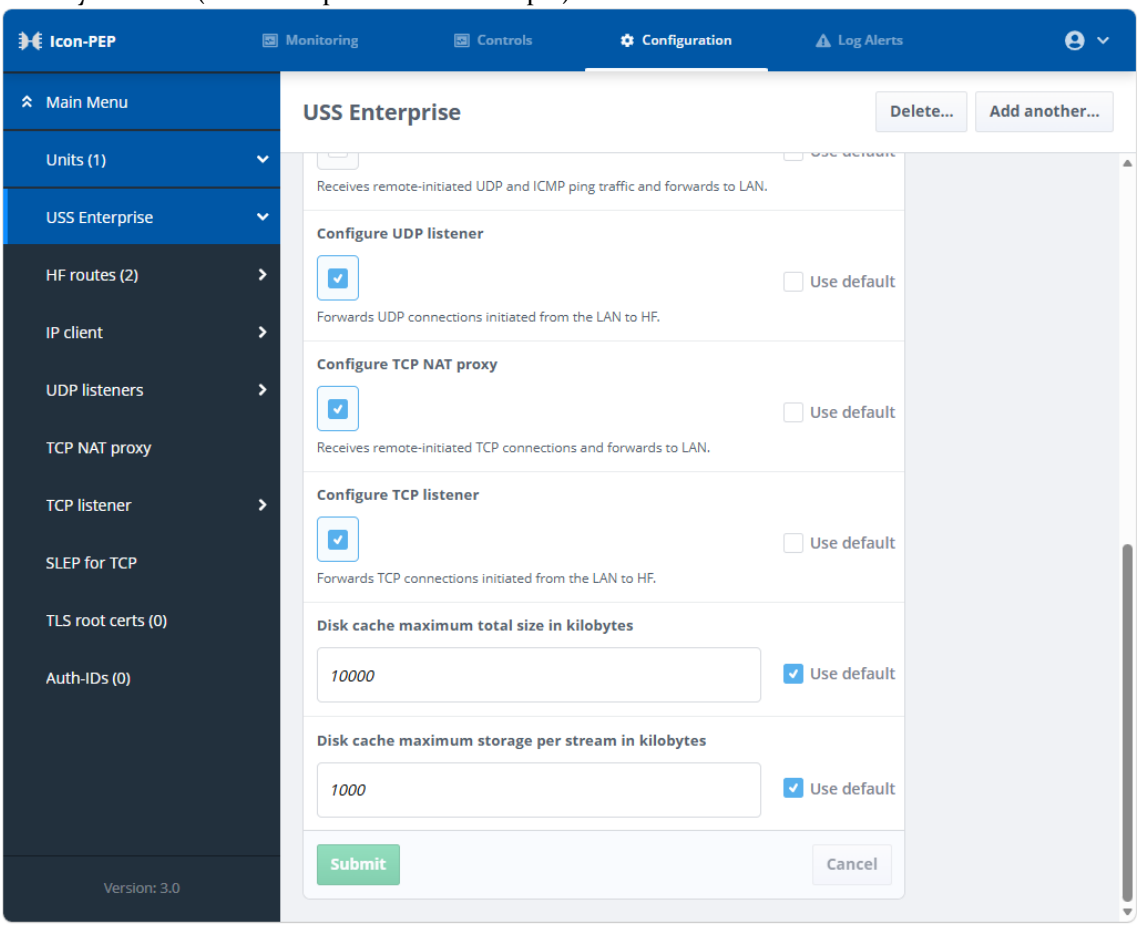
Click “Add”.



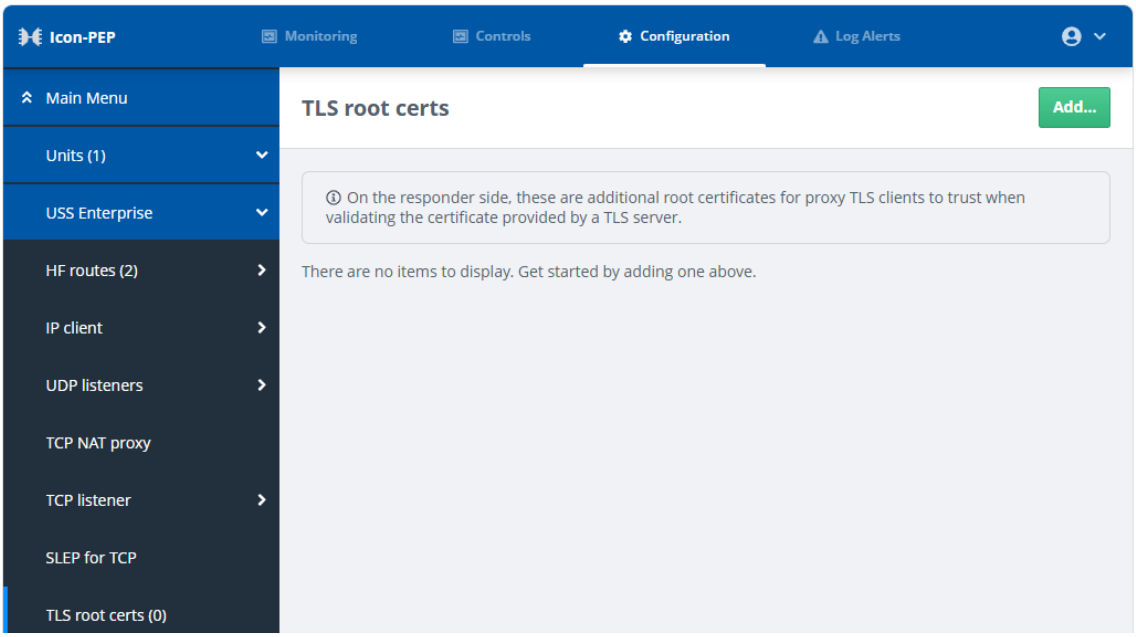
Note you now have “Listen ports” as “2” and the Private Key and Certificate Chain have been replaced with a “token”, this is correct behaviour.

Add TLS root certs

Select your Unit (USS Enterprise in this example).

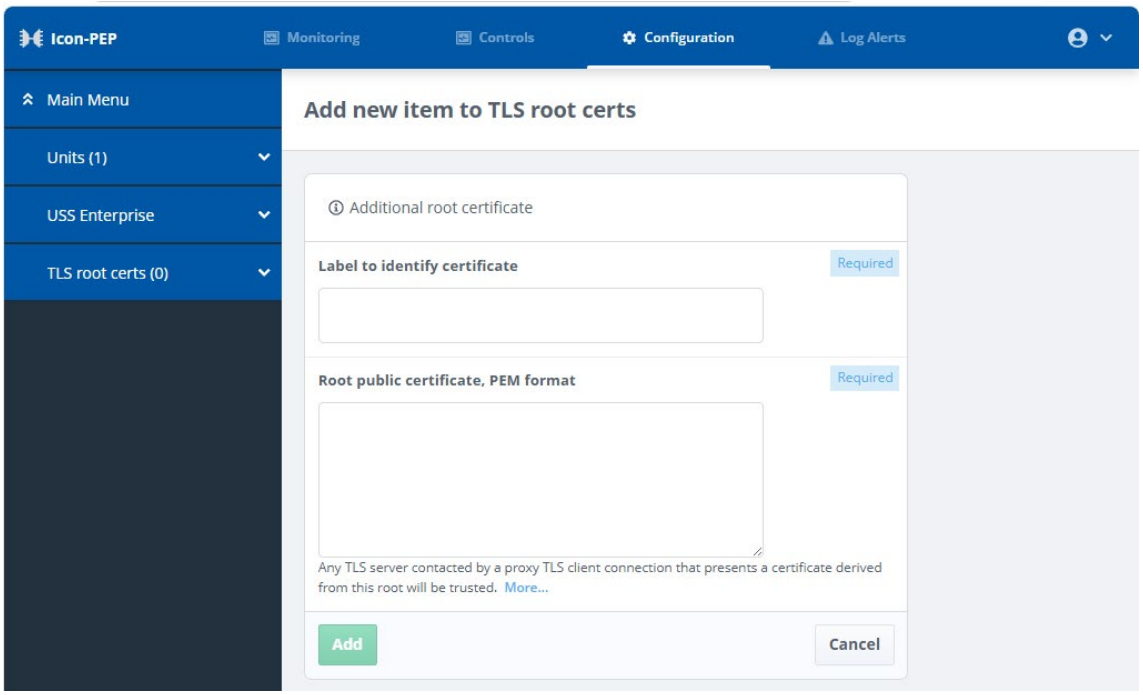


Click “TLS root certs (o)”.

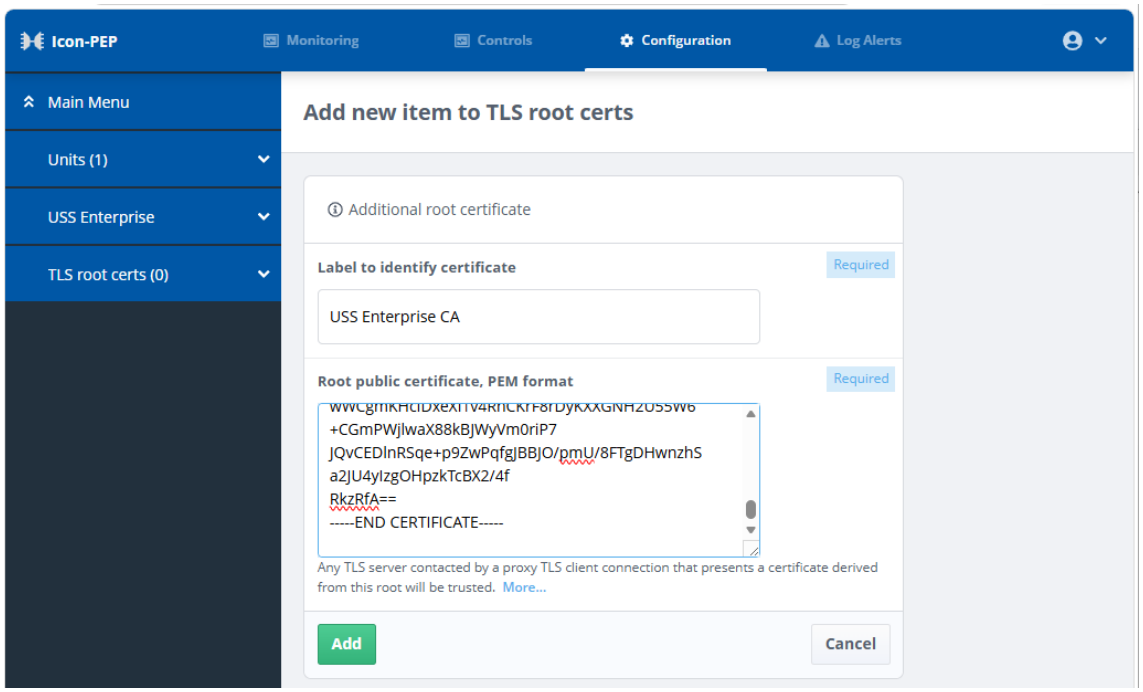


Here you need to add the CA Certificate that issued the Certificate of the Website on your local LAN, in our example (USS Enterprise) this is the enterprise.pacific-fleet.net CA and on the USPF HQ the headquarters.pacific-fleet.net CA.

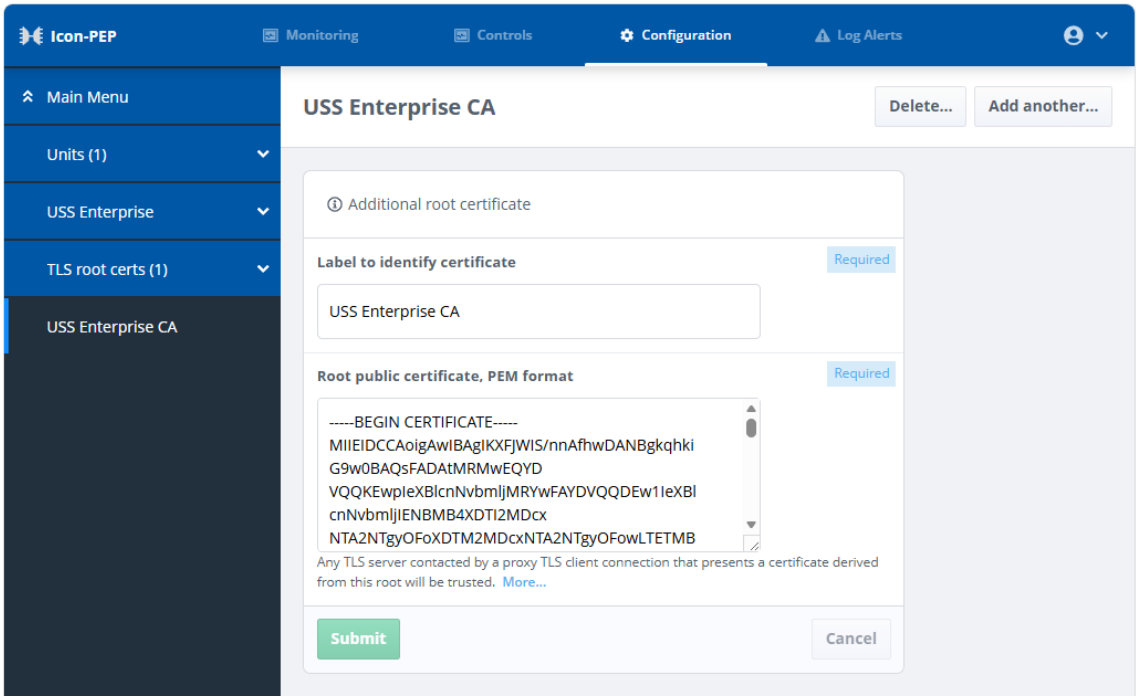
Click “Add...”



Give it a Label e.g. “USS Enterprise CA” and paste in the .pem of that Certificate.

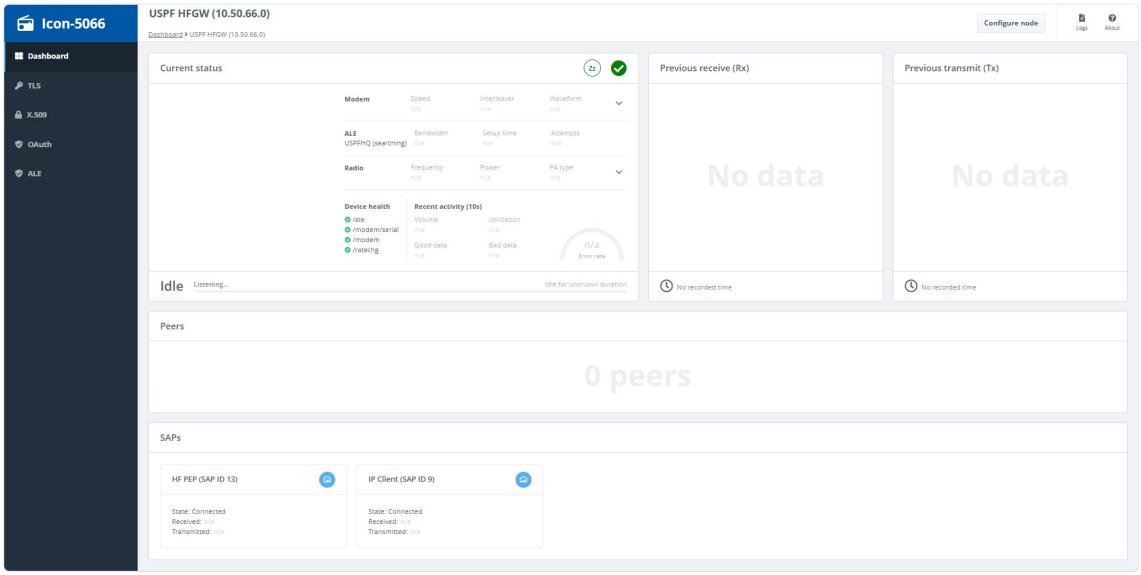


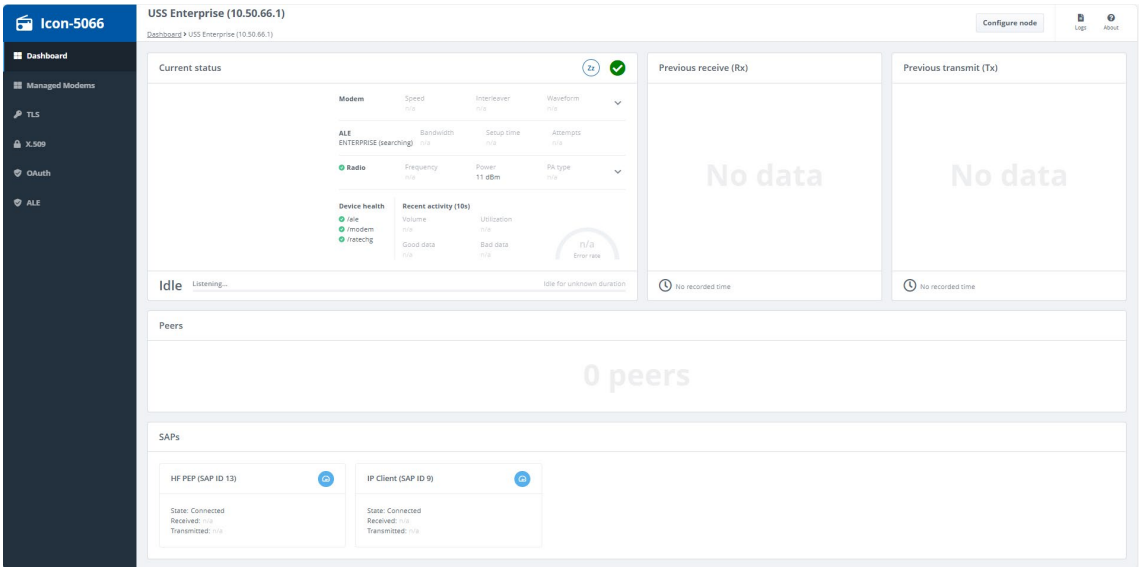
Click “Add”.


Icon-PEP
Monitoring
Controls
Configuration
Log Alerts
Main Menu
Units (1)
USS Enterprise
TLS root certs (1)
USS Enterprise CA
USS Enterprise CA
Delete...
Add another...
Additional root certificate
Label to identify certificate
Required
USS Enterprise CA
Root public certificate, PEM format
Required
-----BEGIN CERTIFICATE-----
MIIEIDCCAoigAwIBAgIKXFJWIS/nnAfhwDANBgkqhki
G9w0BAQsFADAtMRMwEQYD
VQQKEwpIeXBlcnNvbmljMRYwFAYDVQQDEw1IeXBl
cnNvbmljIENBMB4XDTI2MDcx
NTA2NTgyOFoXDTM2MDcxNTA2NTgyOFowLTETMB
Any TLS server contacted by a proxy TLS client connection that presents a certificate derived from this root will be trusted. More...
Submit
Cancel

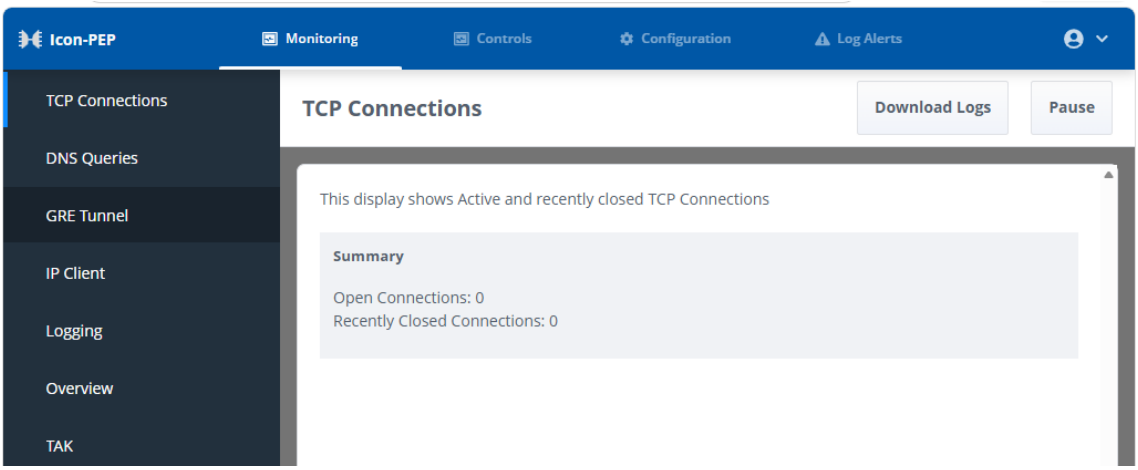
Testing

First check that both your S5066 servers are showing the IP Client and HF PEP connected as below.

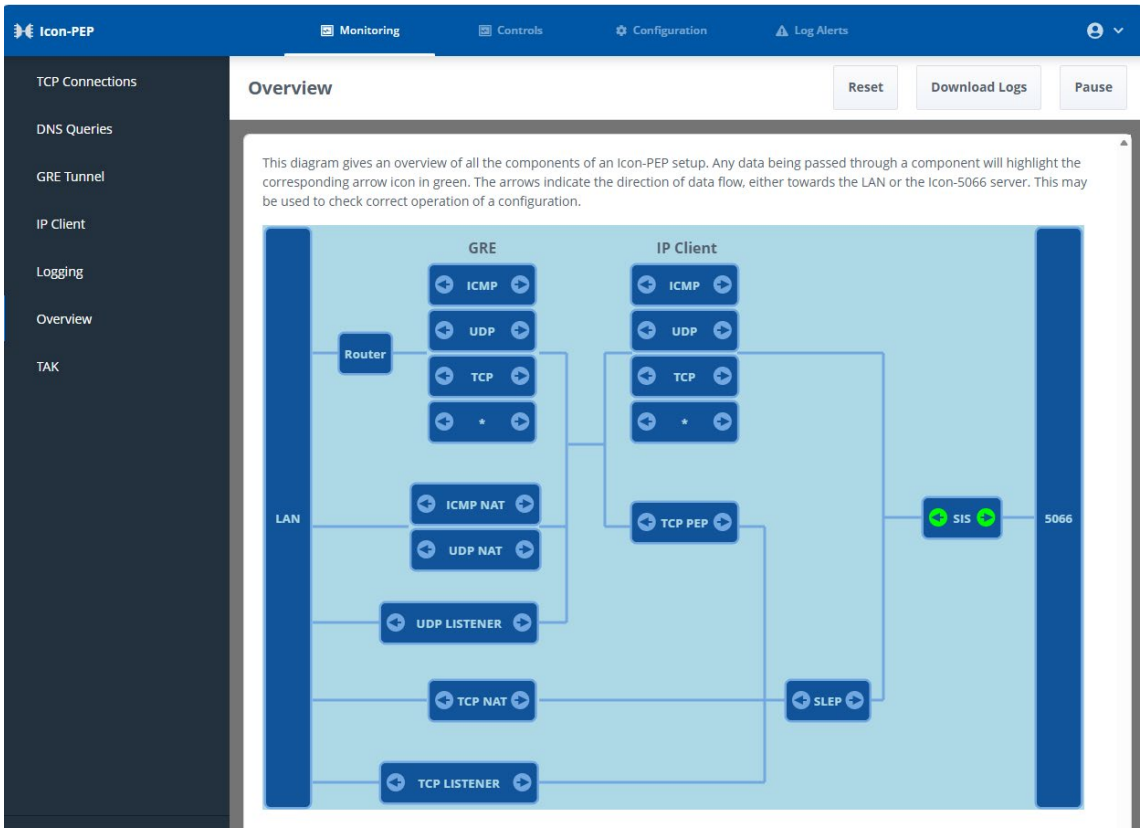




Now look at the Monitoring on your Icon-PEP servers.

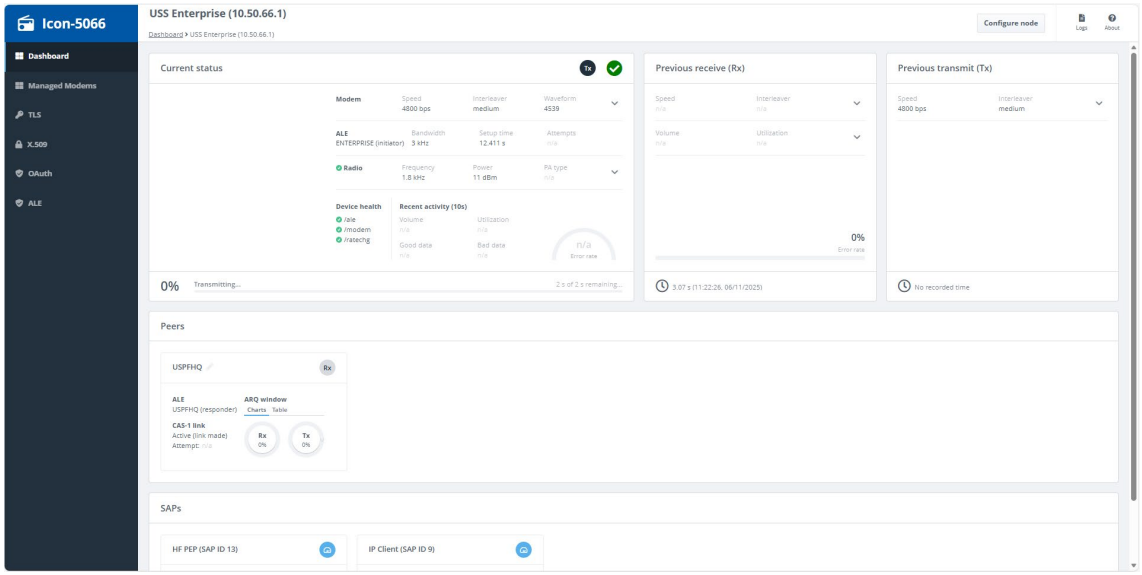


Initially there should be nothing showing for the TCP Connections on either, the "Overview" should show this.

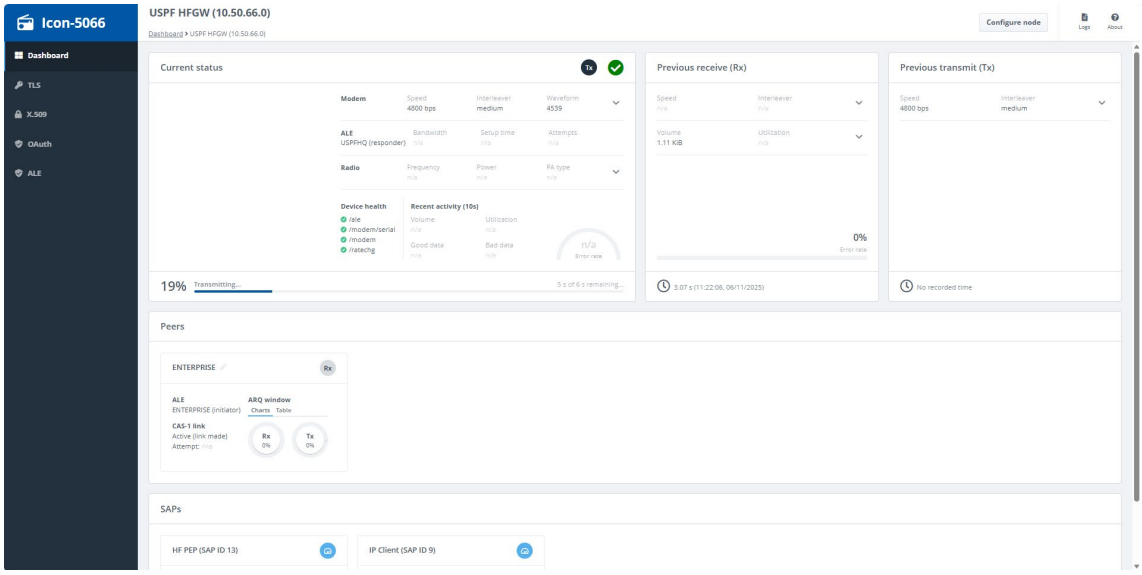


We are now going to browse from the USS Enterprise to the USPF HQ using the URL https://headquarters.pacific-fleet.net .

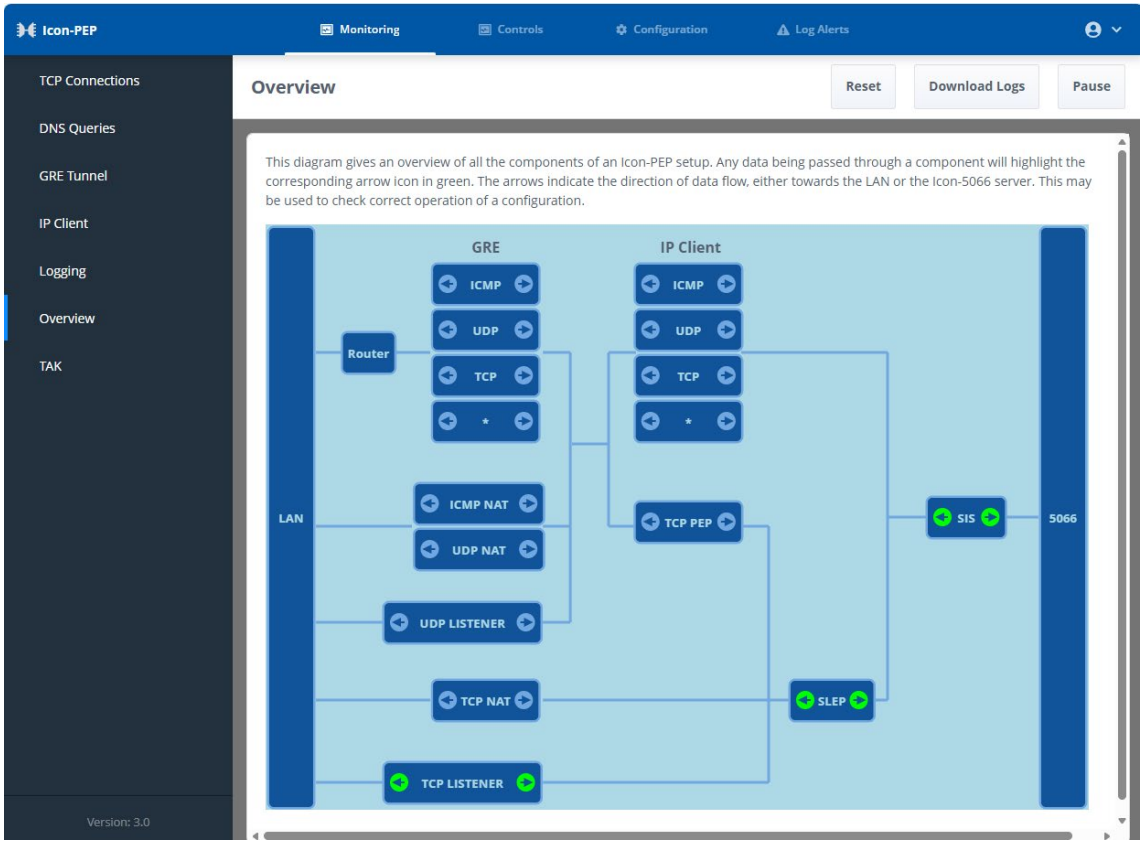
The USS Enterprise Icon-5066 Server will “Initiate” a connection.

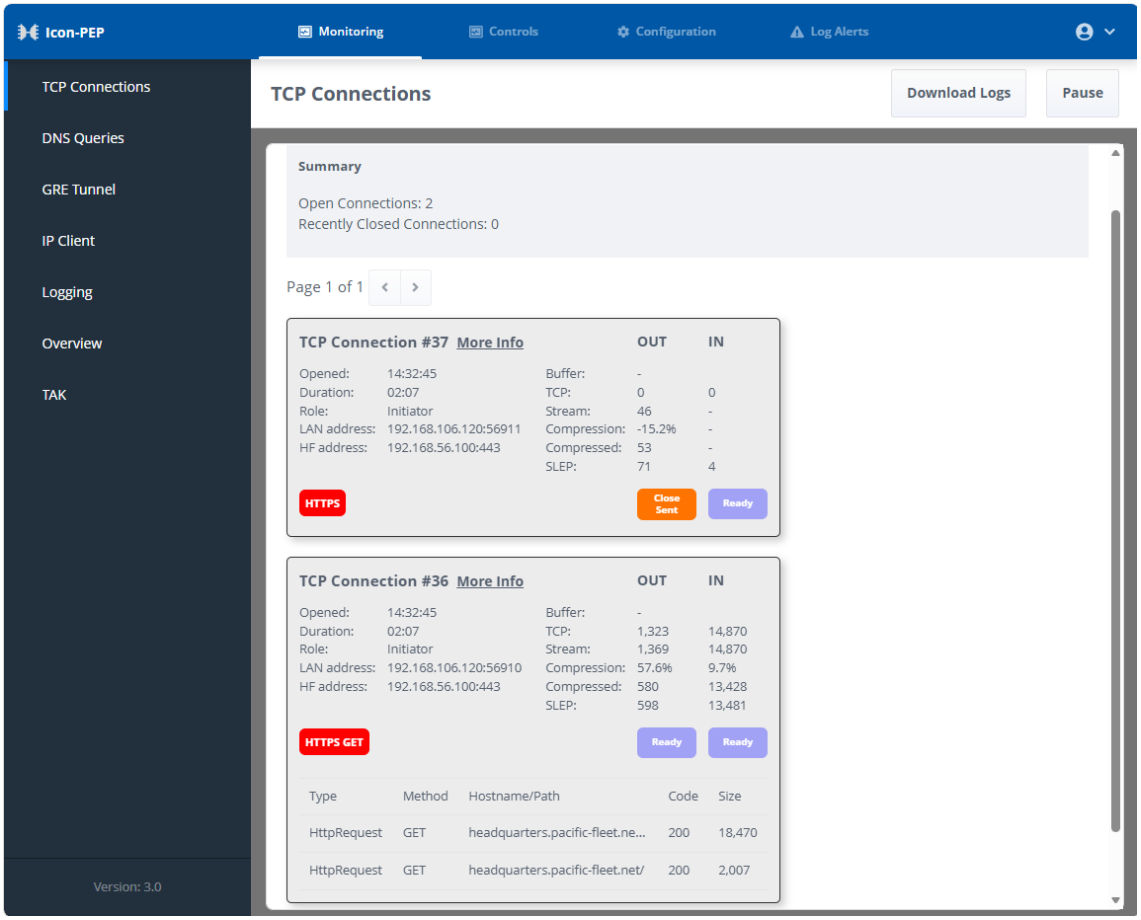


The USPF HQ Icon-5066 Server will “Respond”.



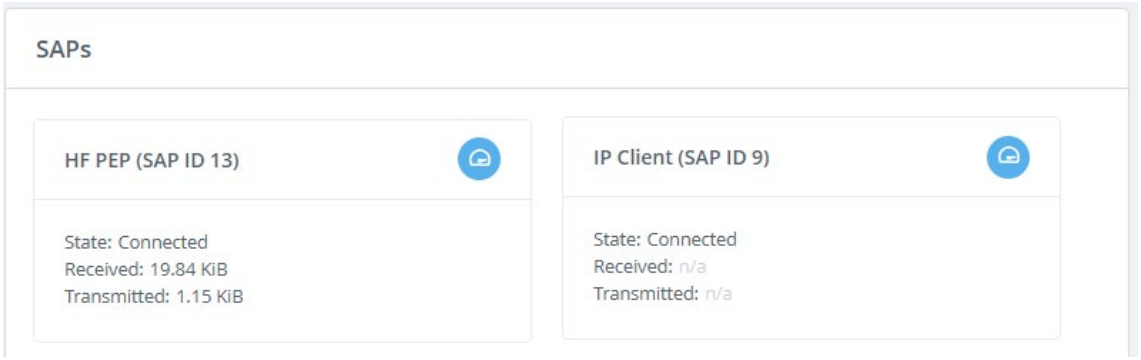
Here are the “Monitoring” Views



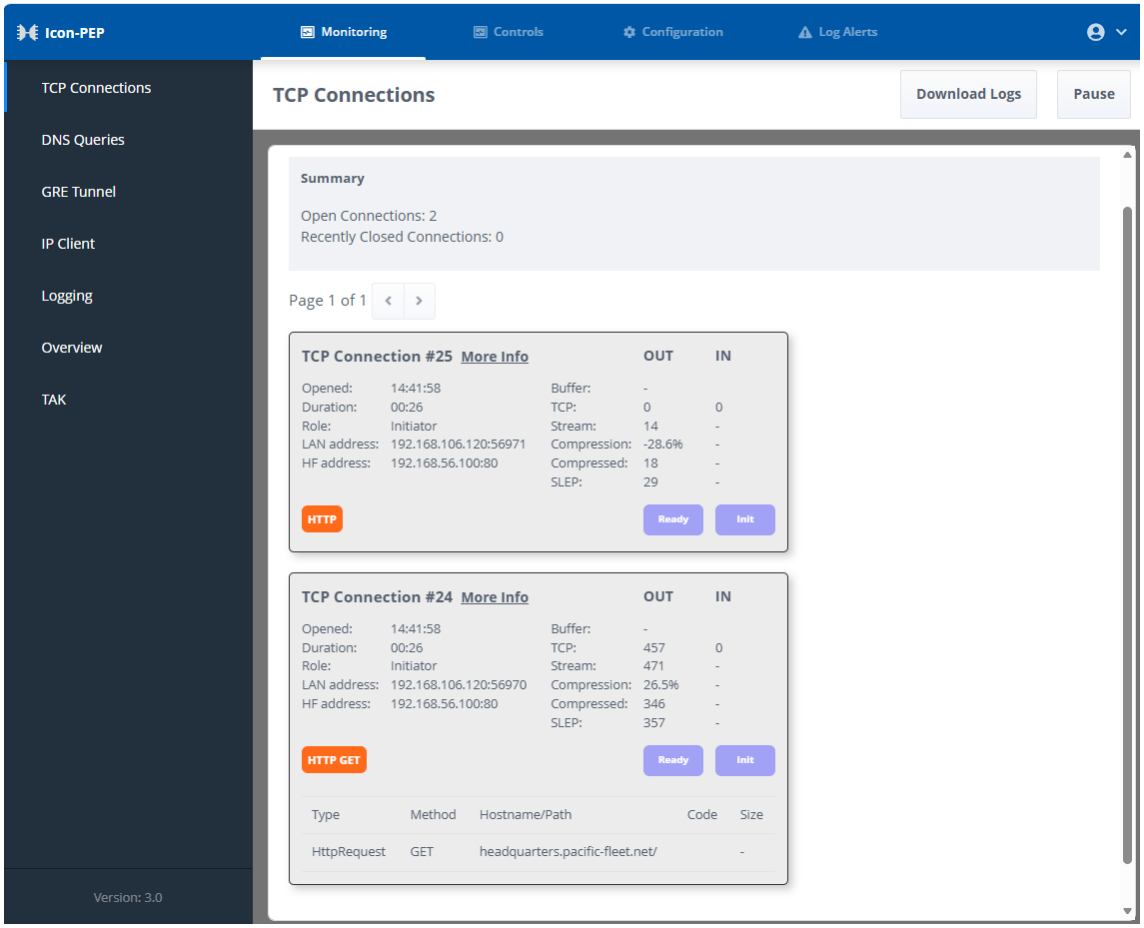


This is the page now displayed.

Icon-5066 also shows the data transferred.



Now repeat the process using the URL http://headquarters.pacific-fleet.net .



Note we are now on Port 80 not Port 443.

You will notice in the above screenshot on the left panel the word “TAK”. This is because Icon-PEP can support TAK (*https://www.civtak.org/community-tak-server/*) Server Federation over HF. If you are interested in this please contact Isode Support *isode.support@isode.com* detailing what you would like to achieve

Other Evaluations

This guide is one two relating to Isode's HF Products, the other guide is:

- Icon-5066

Information on all of this evaluation can be found at *https://www.isode.com/evaluations/*.

Whitepapers

Isode regularly publishes whitepapers on technical and market topics related to its products. A full list of these can be found at *www.isode.com/whitepapers/*.

Copyright