Isode

M-Link EDGE R19.3 Evaluation Guide

Installing and configuring R19.3 of M-Link EDGE, Isode's XMPP Gateway Server.

Contents

Introduction

This guide demonstrates how to get up and running with M-Link EDGE R19.3.

Objectives

By the end of this evaluation you will have:

- Installed M-Link EDGE R19.3
- Requested a Product Activation Key (PAK)
- Receive and Installed the PAK.
- Connected to two External XMPP Servers.

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 *support@isode.com*. Please note that access to the Self-Service Portal for web-based ticket submission and tracking is not available to evaluators.

Preparation

You should visit *www.isode.com/products/supported-platforms.html* 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 10 for simple evaluations and demonstrations.

Isode supports the use of the latest versions of Google Chrome, Mozilla Firefox and Microsoft Edge browsers with the Harrier web client. Internet Explorer is not supported.

External Dependencies

You will need a Chrome Browser installed on the Server and set as the default browser.

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 *www.isode.com/evaluate/evalrequest.html*.

*****TBC Download information***.

Product Activation Key

M-Link EDGE requires a valid Product Activation Key from Isode before it will run correctly. Keys are issued by Isode Customer Services. You will be show in this guide how to copy and send the Product Activation Key request to support@isode.com.

External XMPP Server Details

This guide assumes that you already have access to an external XMPP server and an XMPP Guard, which this installation will interact with.

Installing M-Link

Linux

Run the following commands.

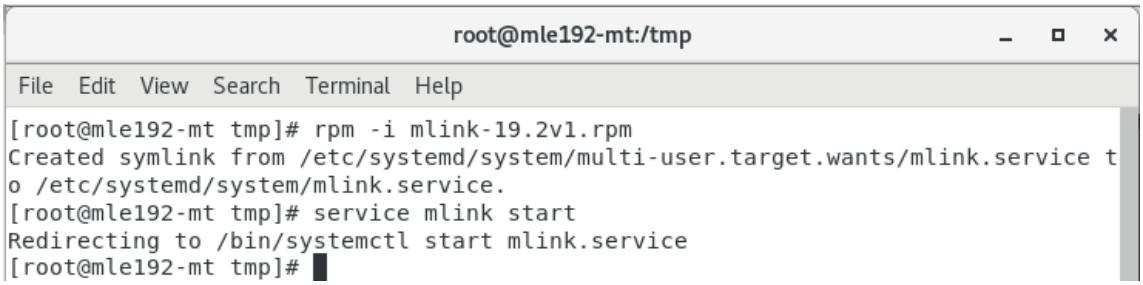

Figure 1: Installing M-Link R19.3 Step 1 (Linux)

Then jump to the browser screen of the Windows Install (on Page 8) and point your browser at https://localhost:5221 .

Windows

Double-click the .msi file that you downloaded earlier and follow the instructions for a fresh install.

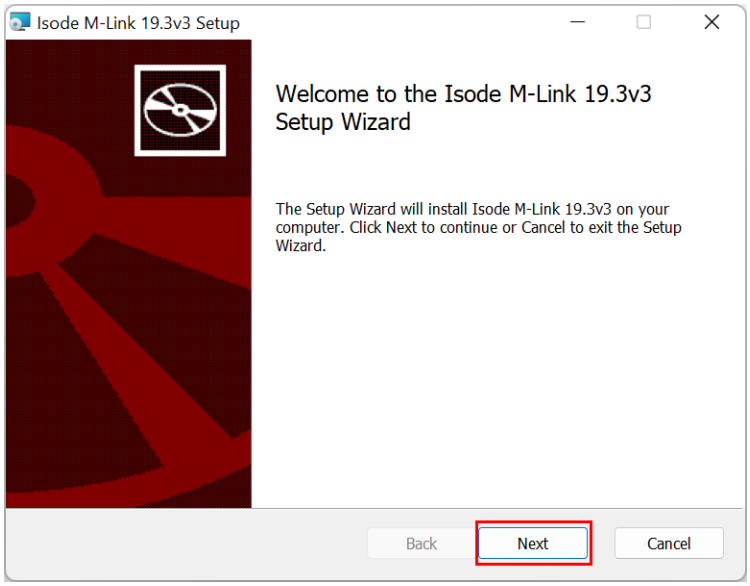

Figure 1a: Installing M-Link R19.3 Step 1

Click "Next".

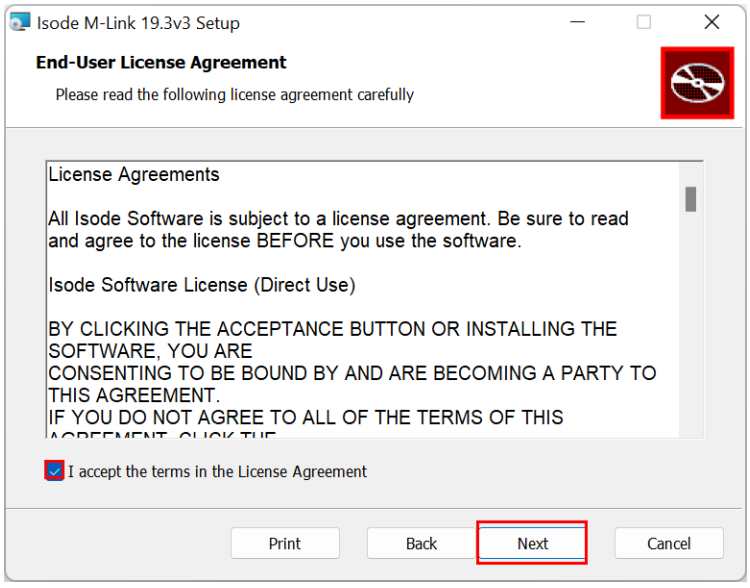

Figure 2: Installing M-Link R19.3 Step 2

Check the checkbox to accept the terms of the license and click "Next".

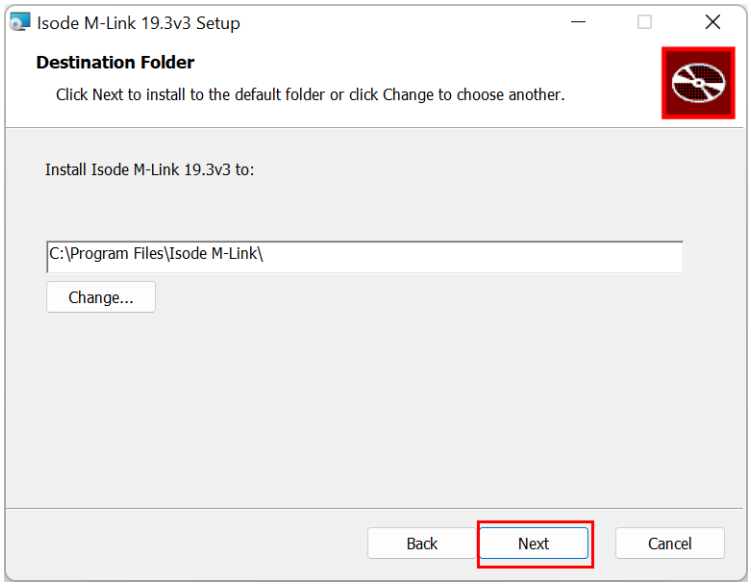

Figure 3: Installing M-Link R19.3 Step 3

Click "Next".

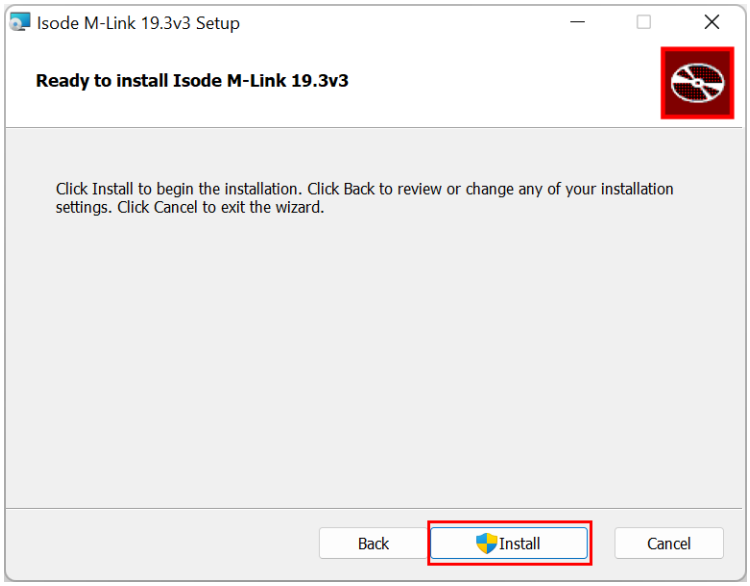

Figure 4: Installing M-Link R19.3 Step 4

Click "Install".

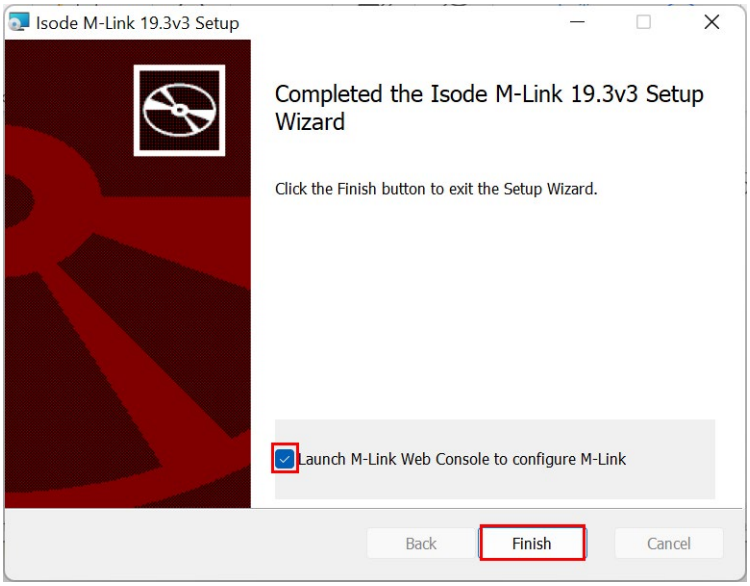

Figure 5: Installing M-Link R19.3 Step 5

Click "Finish" and the following Browser window opens.

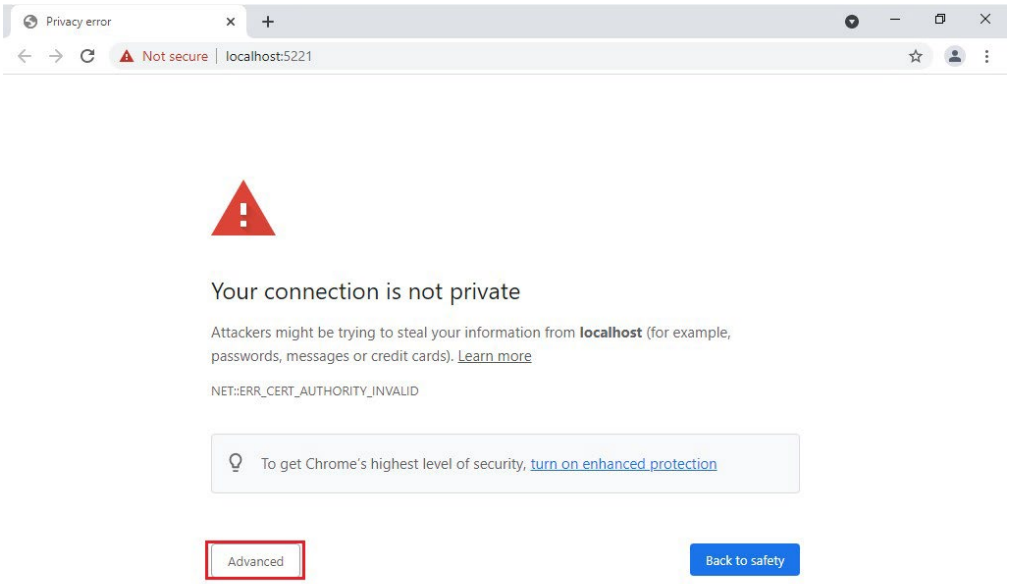

Figure 6: Initial M-Link R19.3 Configuration Step 1

Click "Advanced".

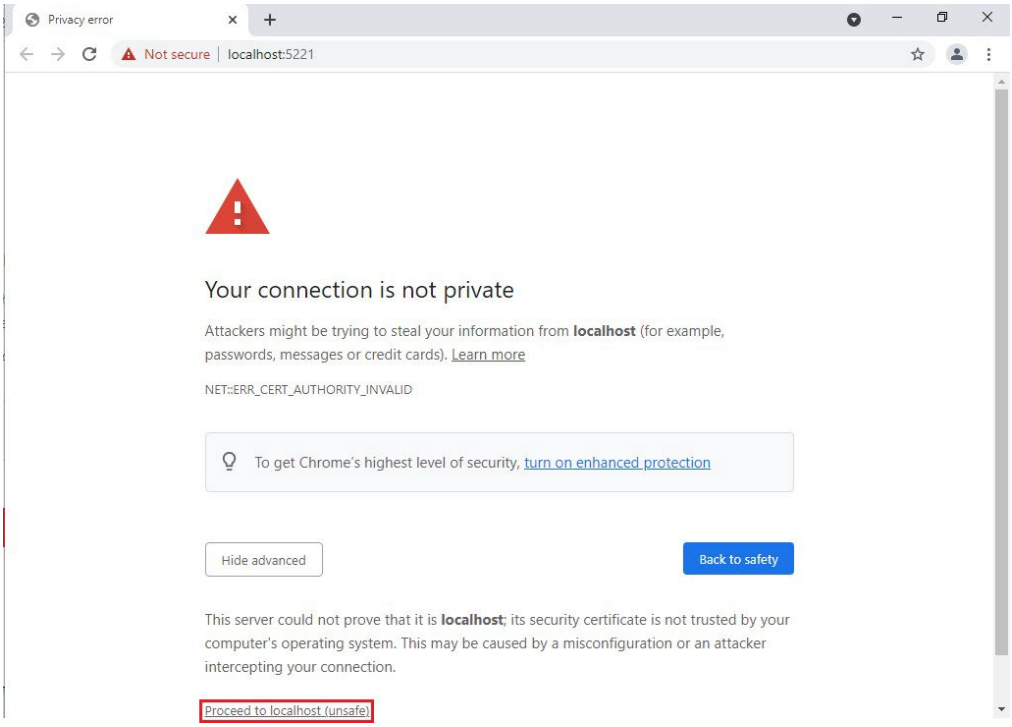

Figure 7: Initial M-Link R19.3 Configuration Step 2

Click "Proceed to localhost (unsafe)".

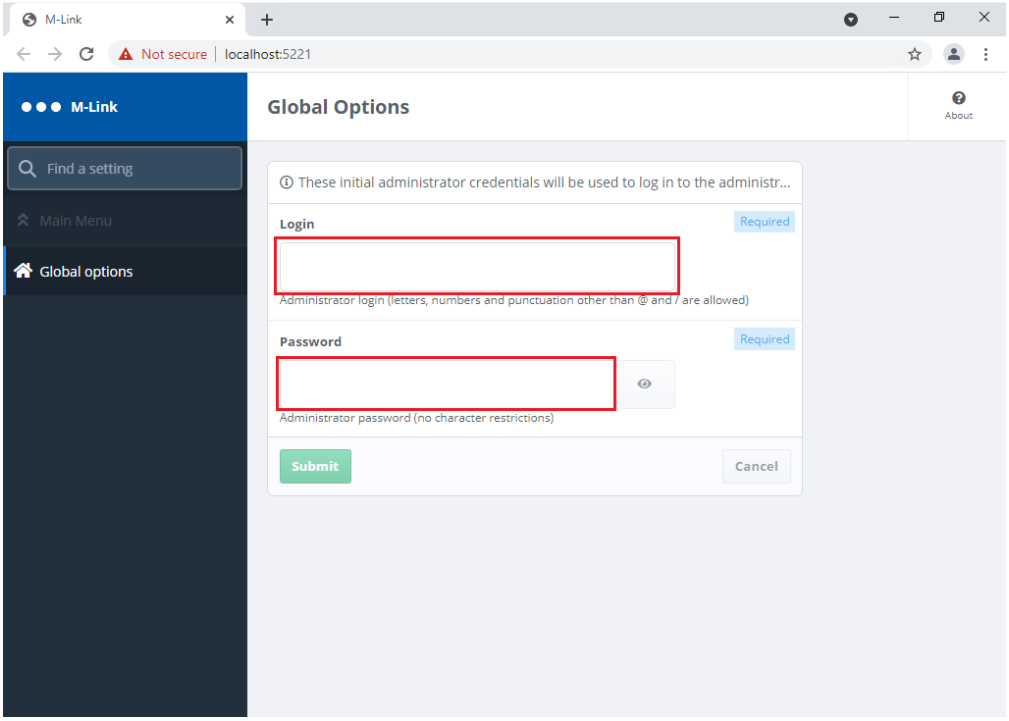

Figure 8: Initial M-Link R19.3 Configuration Step 3

Enter an Administrator Login Name of your choice and set a Password.

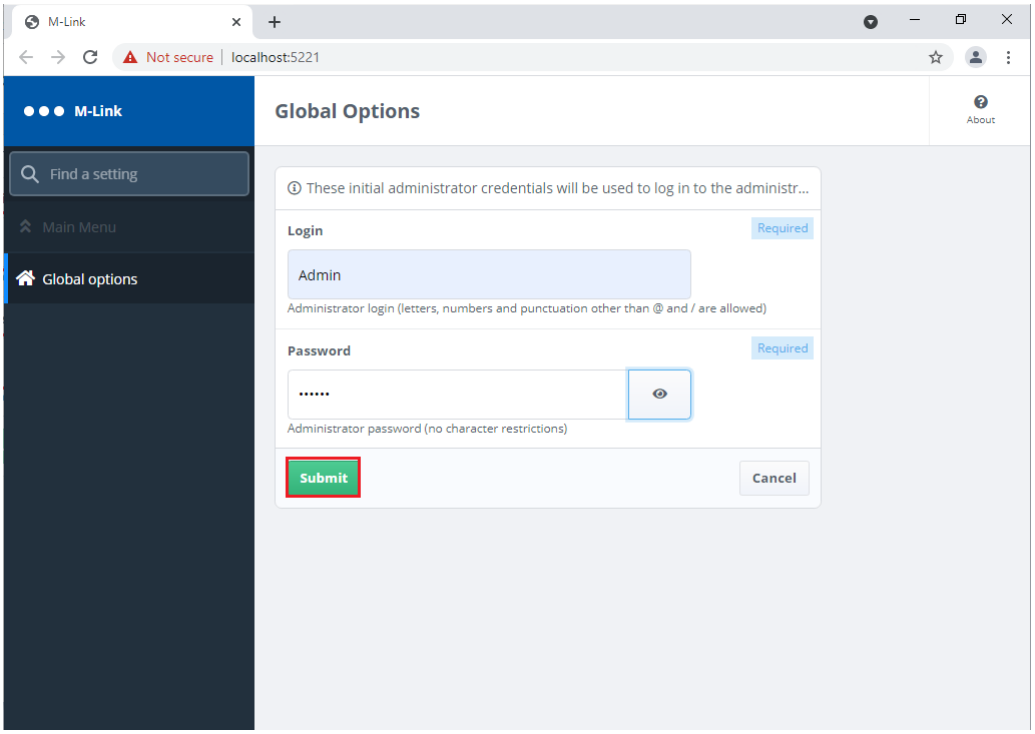

Figure 9: Initial M-Link R19.3 Configuration Step 4

Click "Submit".

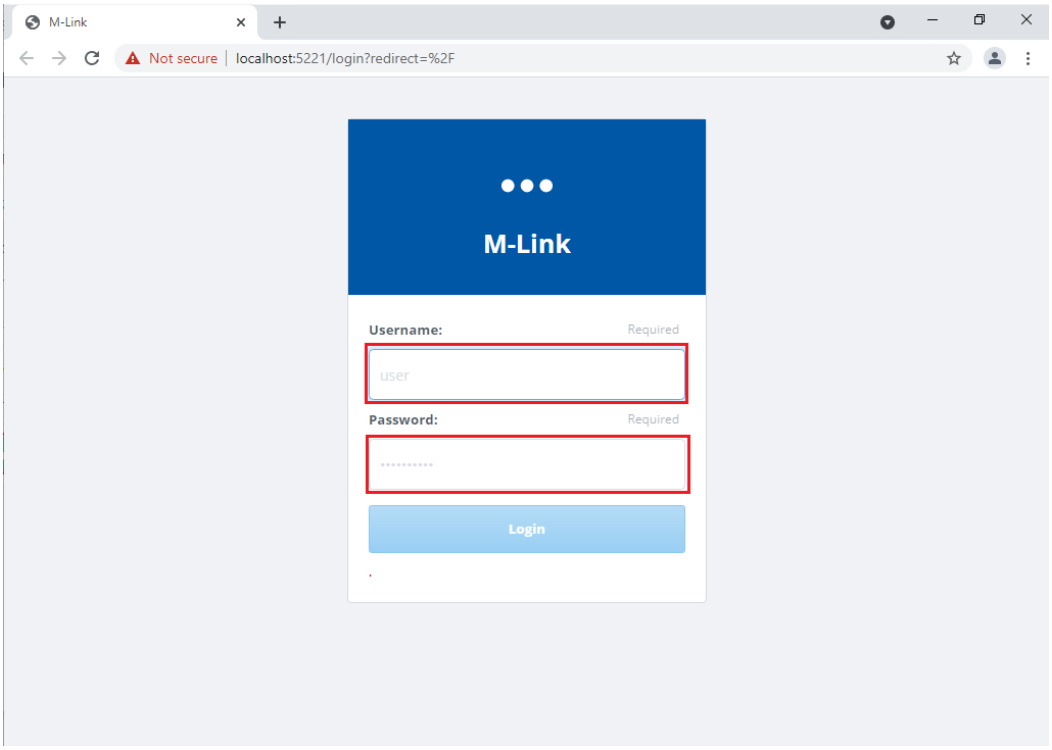

Figure 10: Initial M-Link R19.3 Configuration Step 5

Enter the Administrator Login Name and Password you created previously.

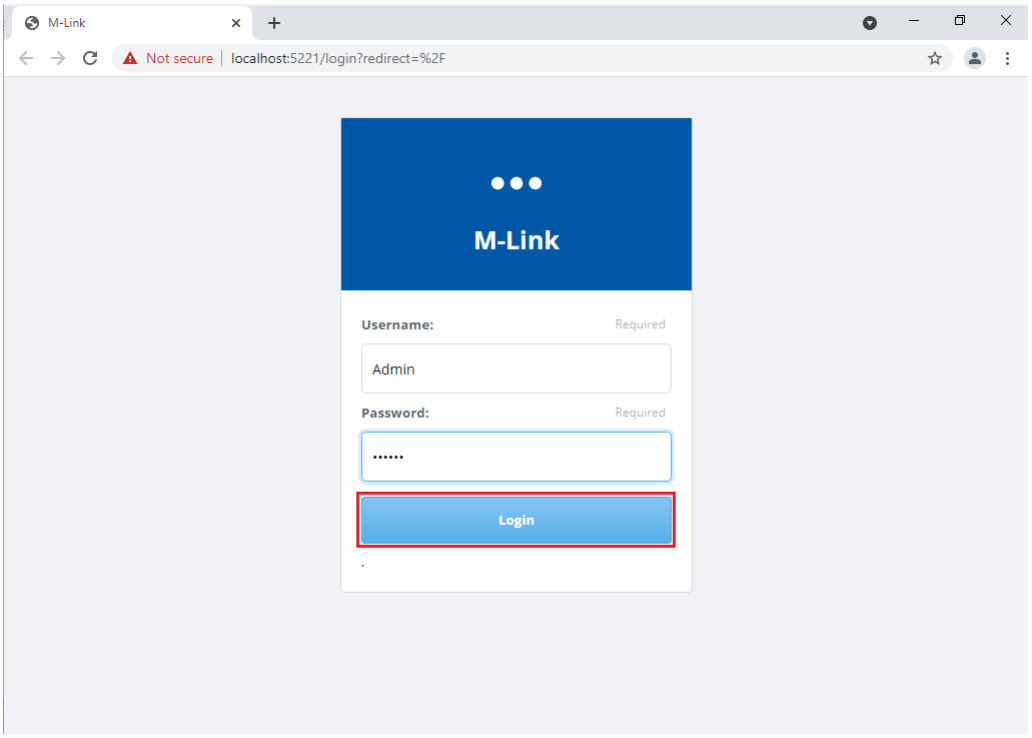

Figure 11: Initial M-Link R19.3 Configuration Step 6

Click "Login" and the following screen appears.

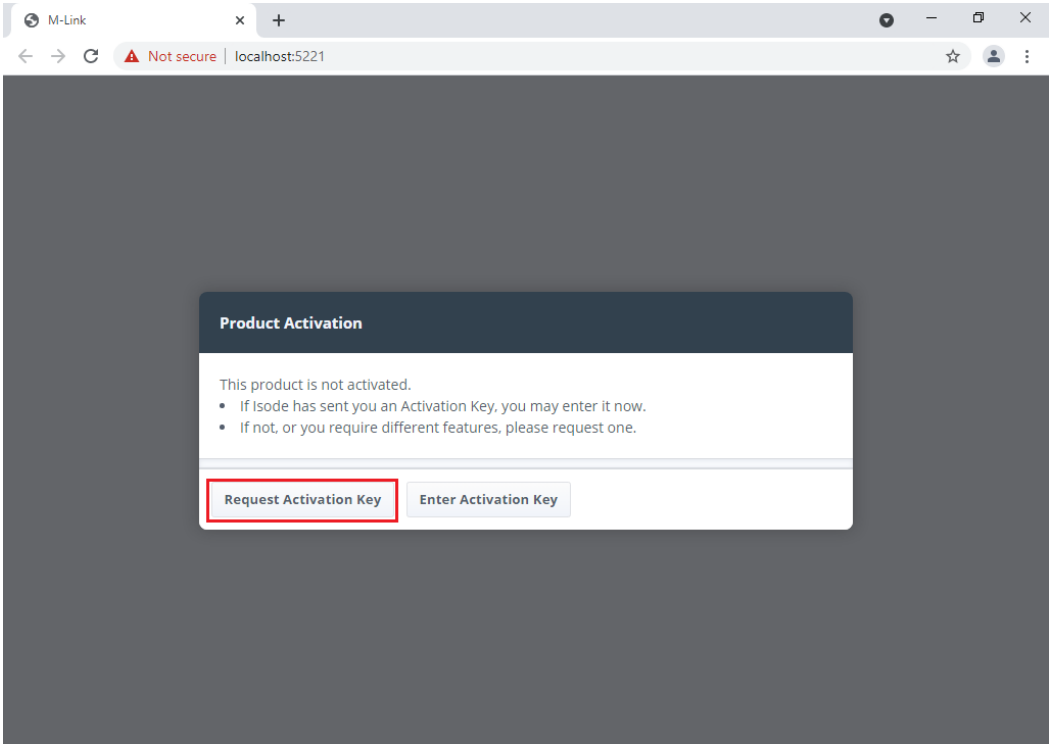

Figure 12: Initial M-Link R19.3 Configuration Step 7

Click "Request Activation Key".

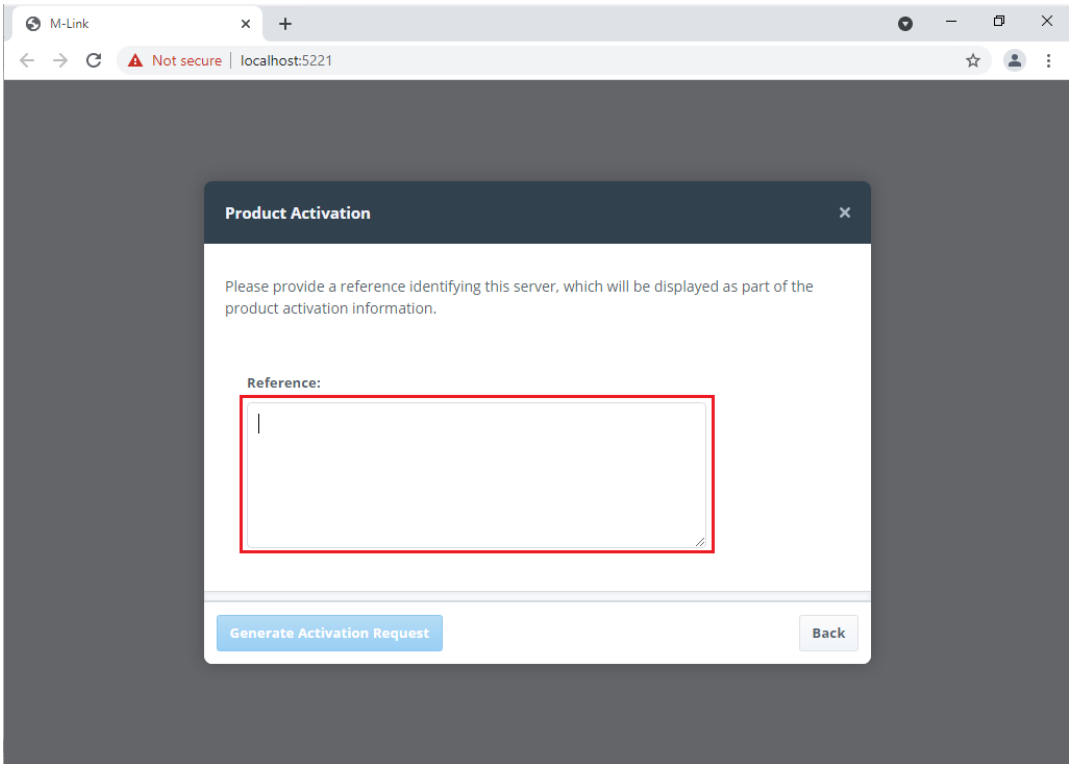

Figure 13: Initial M-Link R19.3 Configuration Step 8

Enter a reference for the Server.

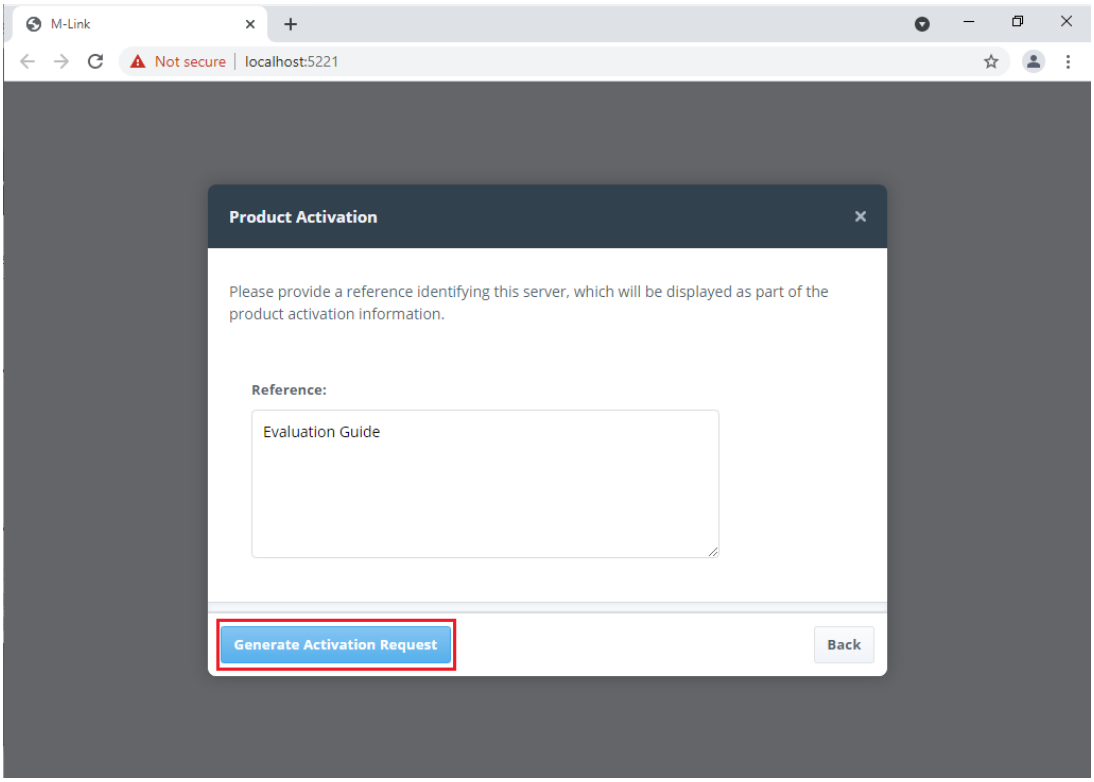

Figure 14: Initial M-Link R19.3 Configuration Step 9

Click "Generate Activation Request".

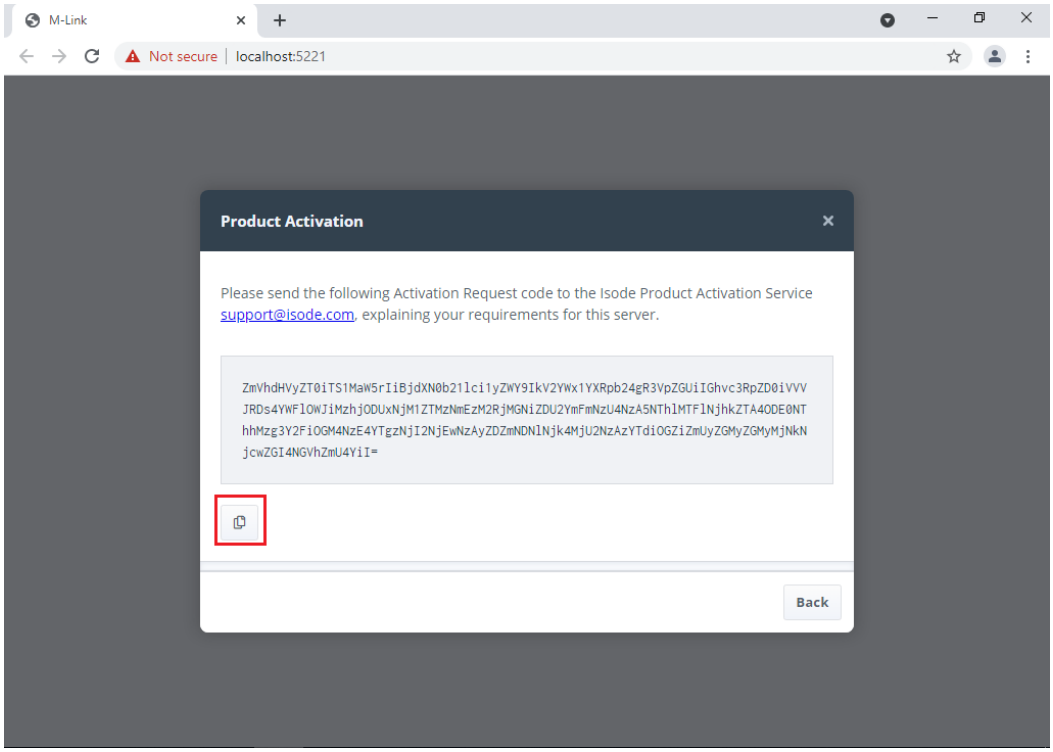

Figure 15: Initial M-Link R19.3 Configuration Step 10

Use the "Copy" button (bottom left) to copy this "Activation Request" and then email it to support@isode.com .

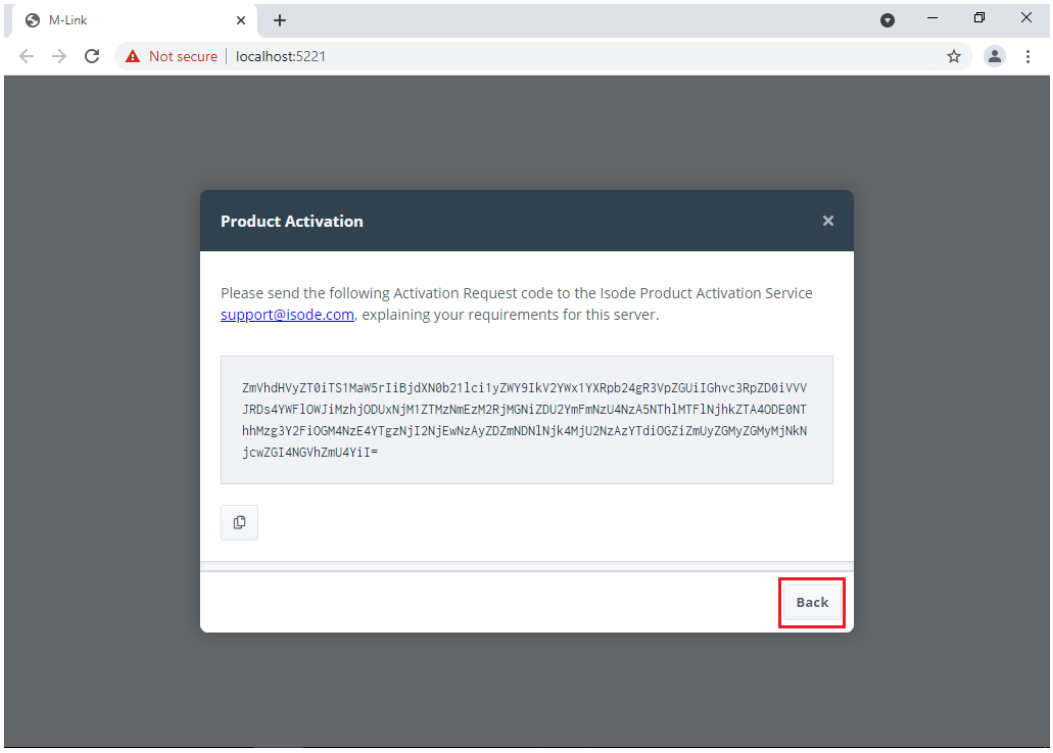

Figure 16: Initial M-Link R19.3 Configuration Step 11

Click "Back"

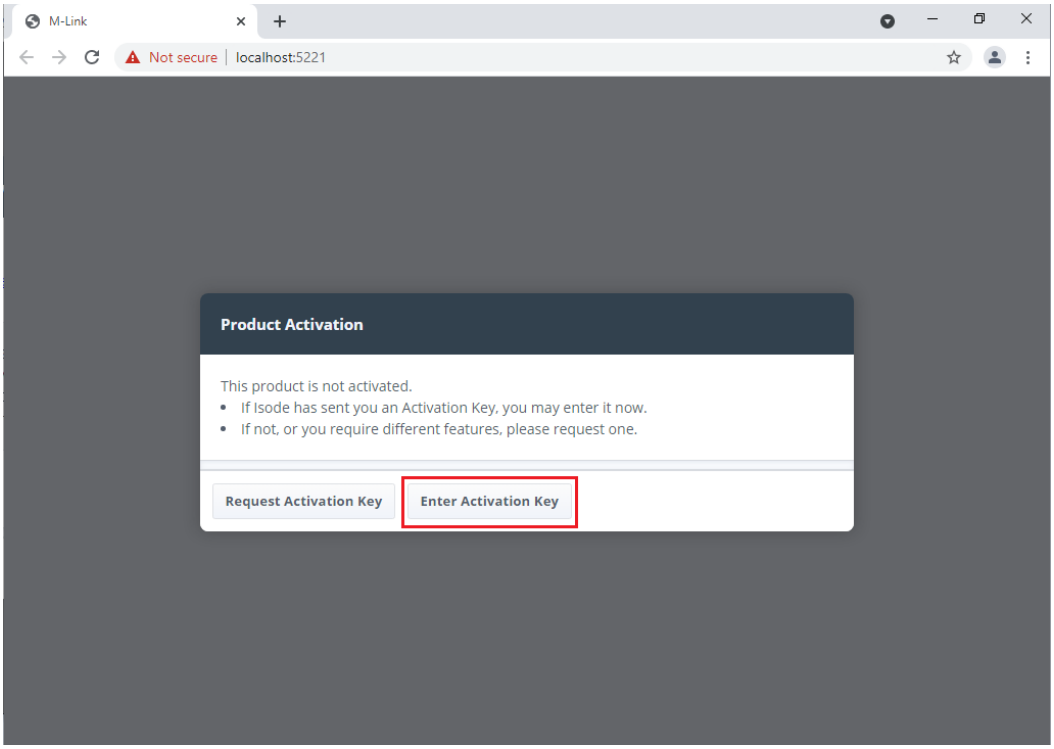

Figure 17: Initial M-Link R19.3 Configuration Step 12

You will receive the "Product Activation Key" from Isode Support and you should then Click "Enter Activation Key".

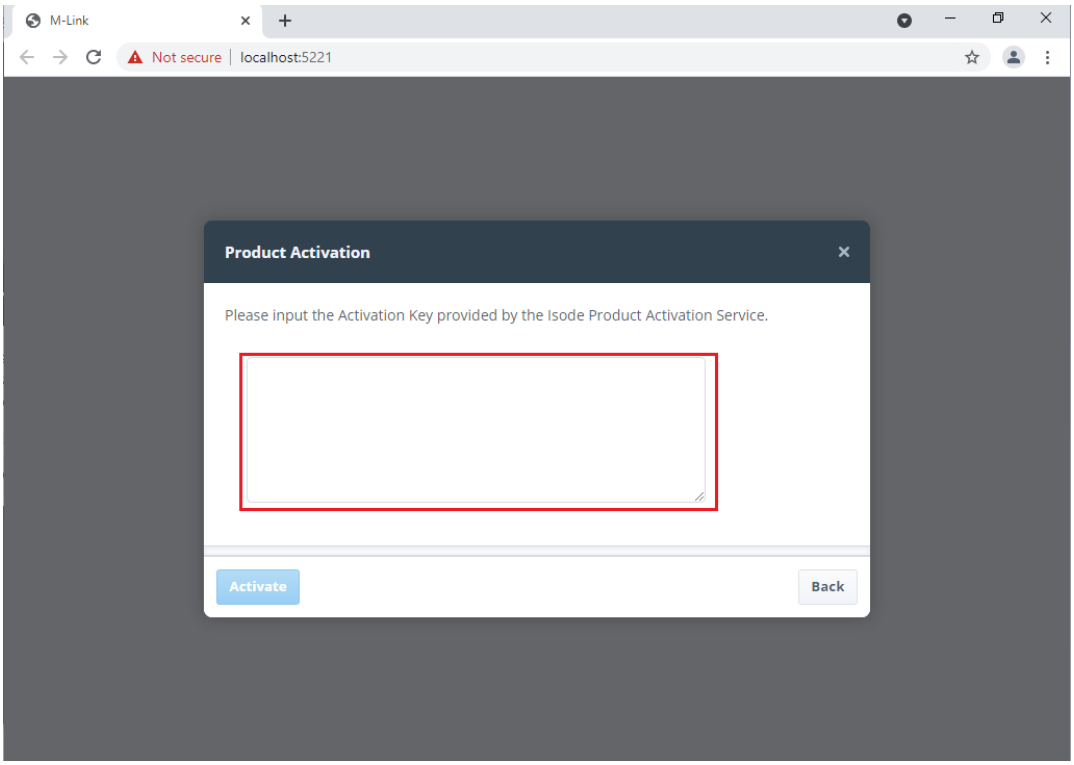

Figure 18: Initial M-Link R19.3 Configuration Step 13

Paste the "Product Activation Key" in the space provided.

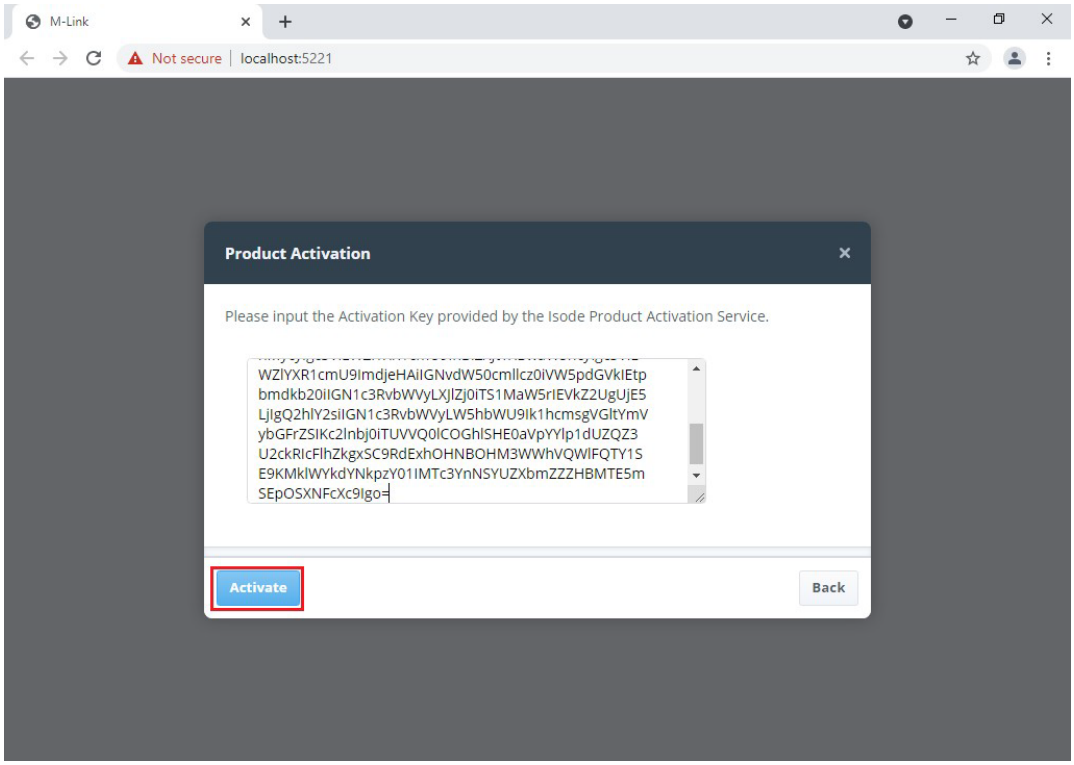

Figure 19: Initial M-Link R19.3 Configuration Step 14

Click “Activate”, and the following screen should appear.

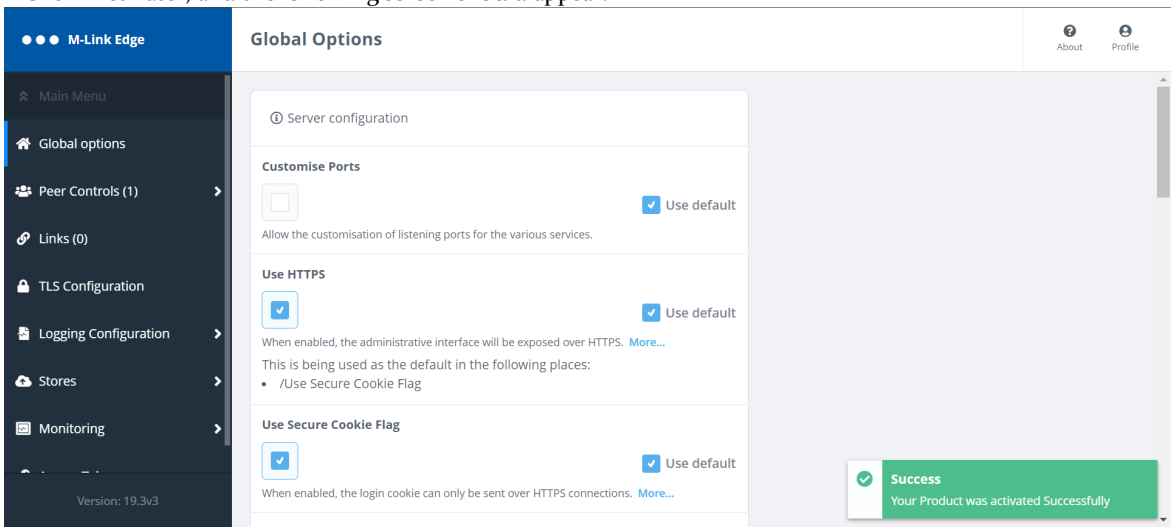

Figure 20: Initial M-Link R19.3 Configuration Complete

Your server is now ready for further configuration.

Configuring M-Link Edge

There are a number of configuration options and the intention of this guide is to give you an overview of the most used ones. The options detailed below will be configured in this guide.

1. TLS Configuration (Only shown if you have a TLS Product Activation Key)
2. GCXP Link Configuration – for use with Isode M-Guard
3. X2X Link Configuration – for use with some 3rd Party Guards and SATCOM Links
4. Peer Configuration

TLS Configuration

Before you start this you will need the following.

- A Certificate Chain file in PEM format containing your Server Certificate, CA Certificate and any Intermediate CA Certificates.
- A Private Key file in PEM format (you must know the passphrase for the Private Key).
- As a Minimum the Certificate Subject should be the hostname of the server, e.g. cn=hostname and have a Subject Alternative Name of DNS Name=Hostname.
- The issuing CA Certificate should either be either a Globally Trusted Root CA or in the Trusted Root CA Store.

From the "Home" – Global Options screen

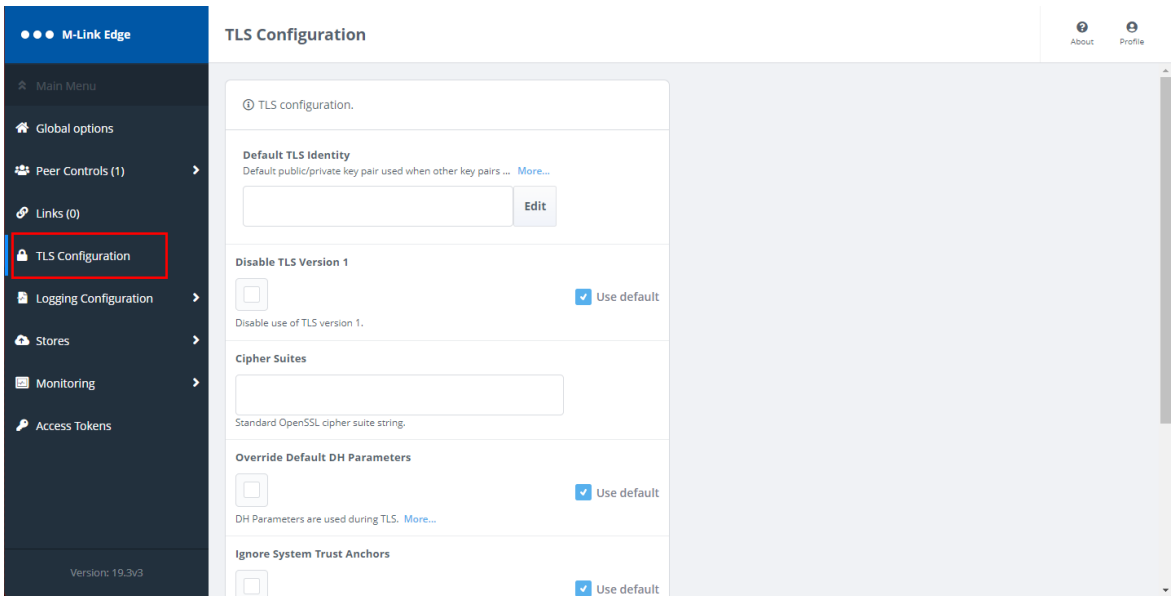

Figure 21: TLS Configuration Step 1

Click TLS Configuration.

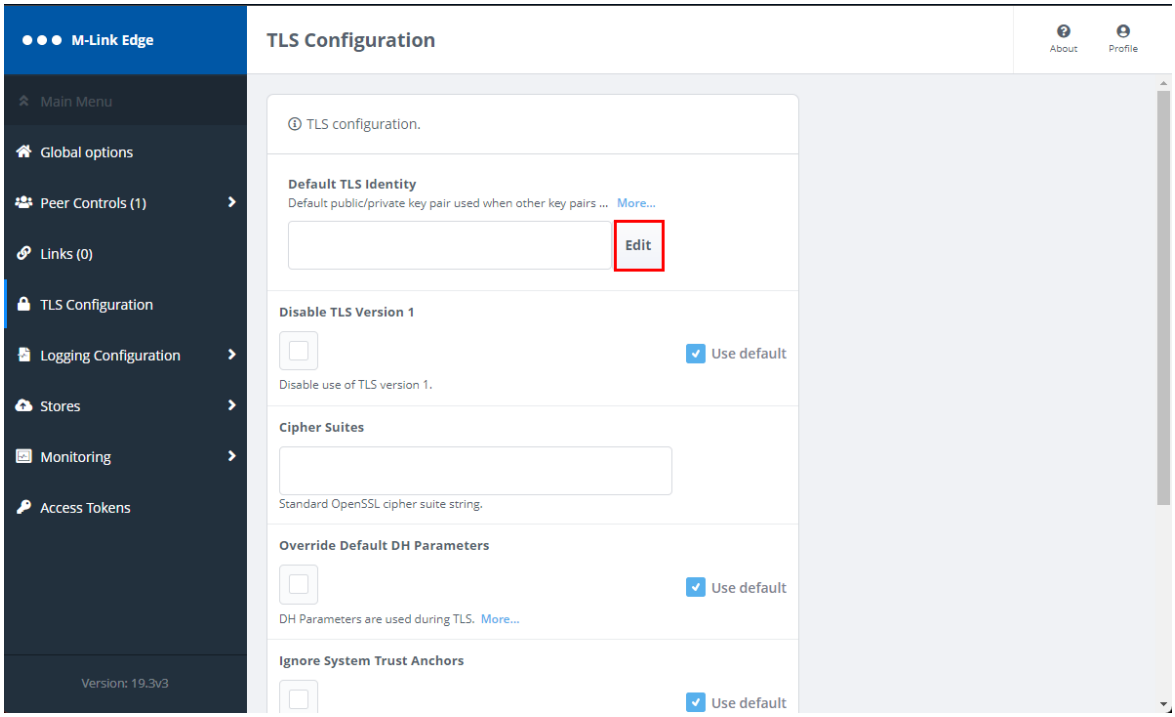

Figure 22: TLS Configuration Step 2

Select "Edit" next to "Default TLS Identity".

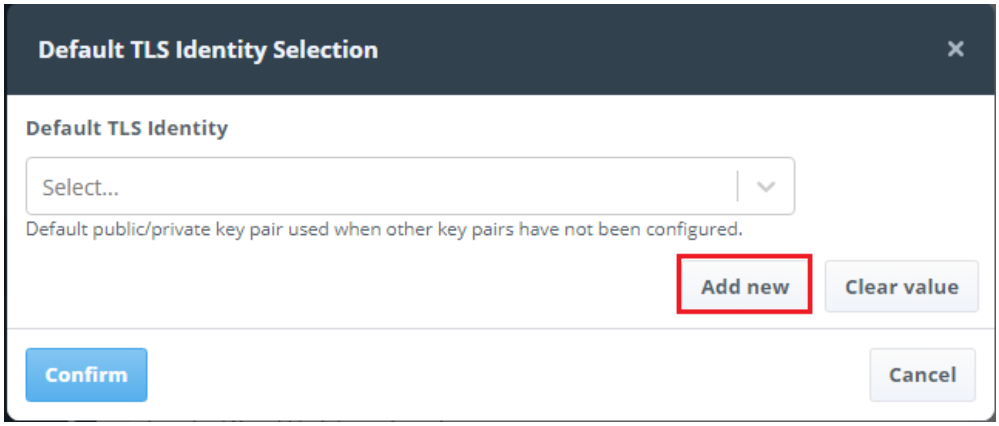

Figure 23: TLS Configuration Step 3

Click "Add new".

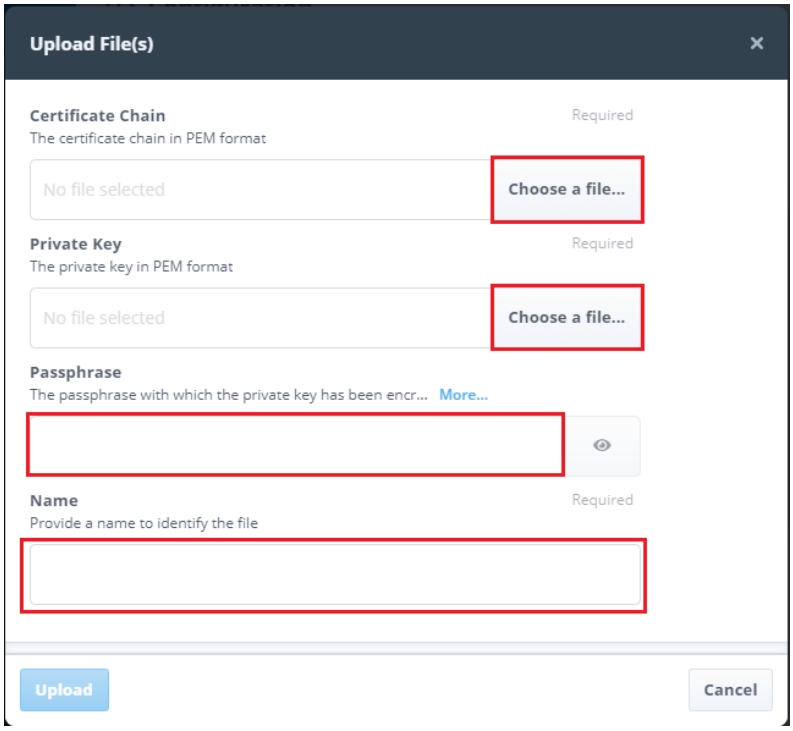

Figure 24: TLS Configuration Step 4

Use the "Choose a file…" buttons to load the Certificate chain and Private Key, enter the Private Key Passphrase and Provide and "Name" of your choice for the "Identity".

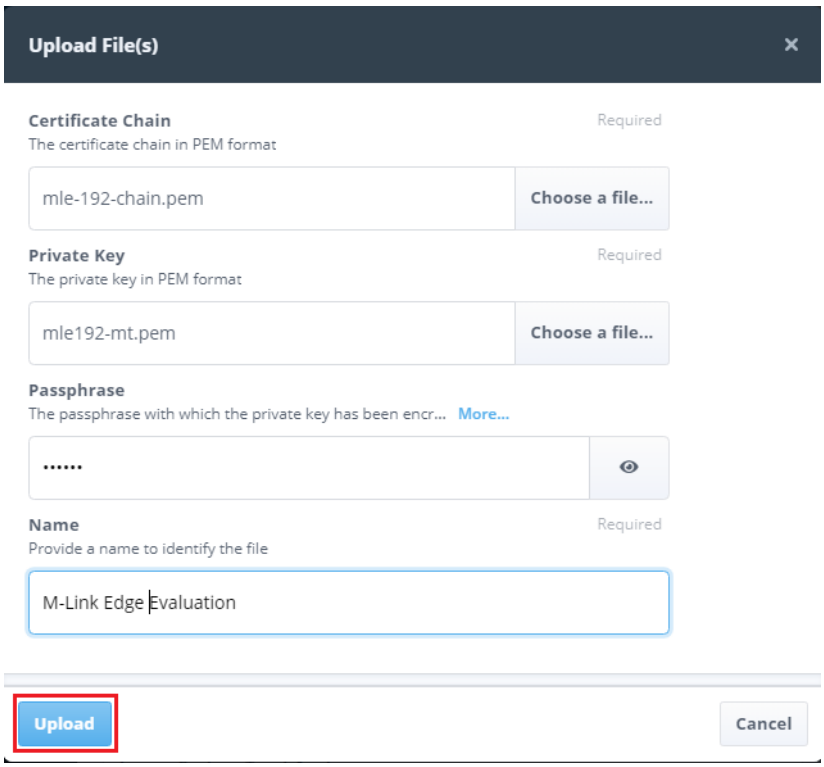

Figure 25: TLS Configuration Step 5

Click "Upload".

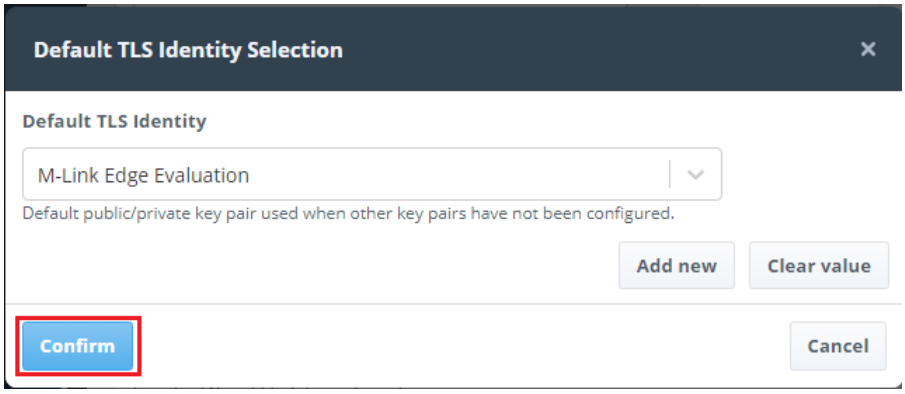

Figure 26: TLS Configuration Step 6

Click "Confirm".

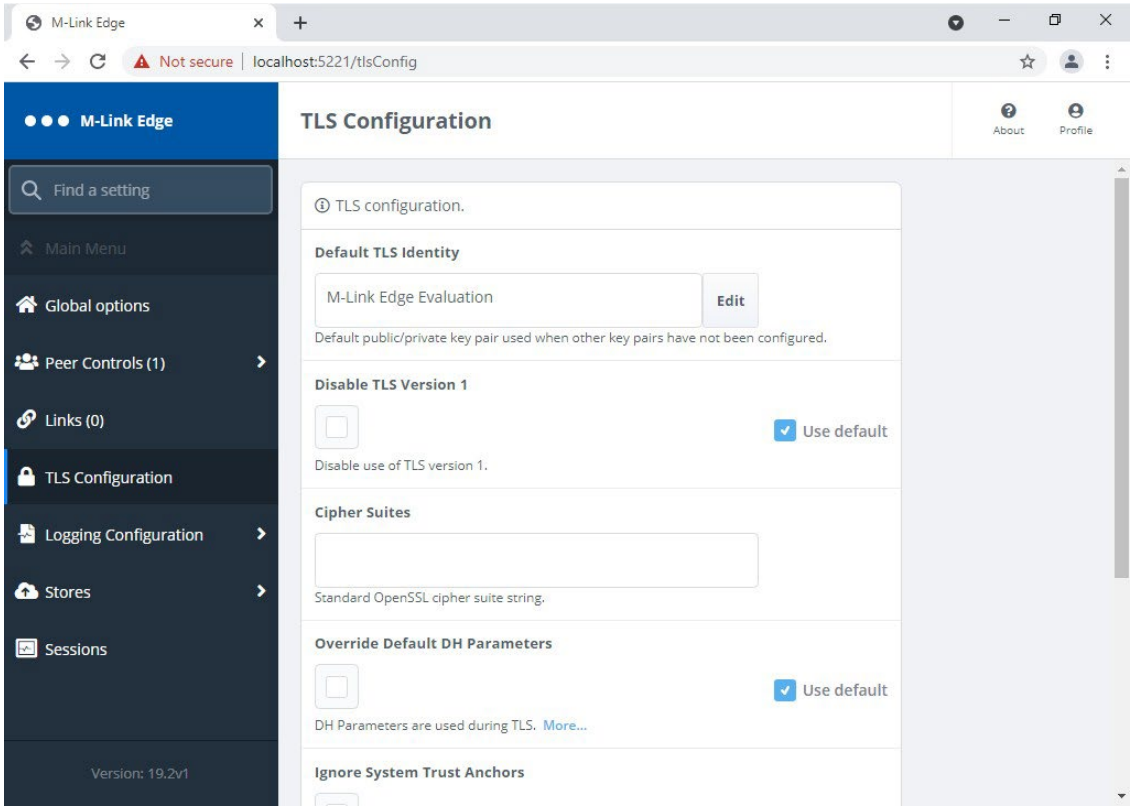

Figure 27: TLS Configuration Step 7

Scroll down to the bottom of the screen.

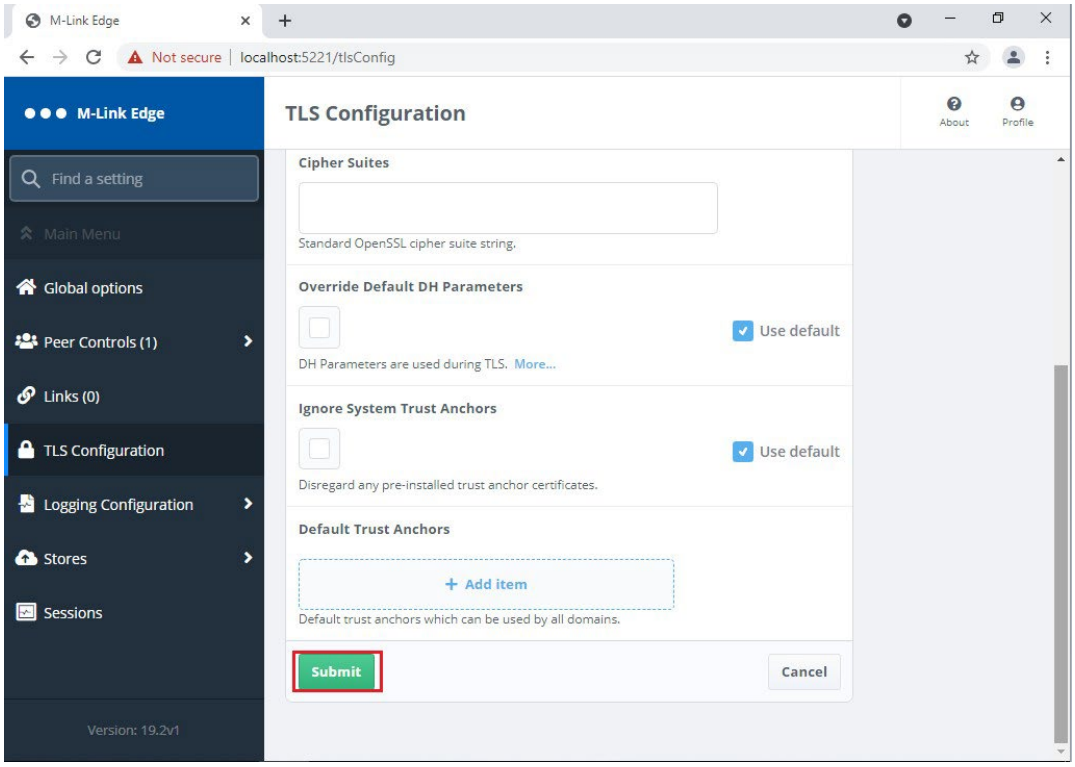

Figure 28: TLS Configuration Step 8

Click "Submit".

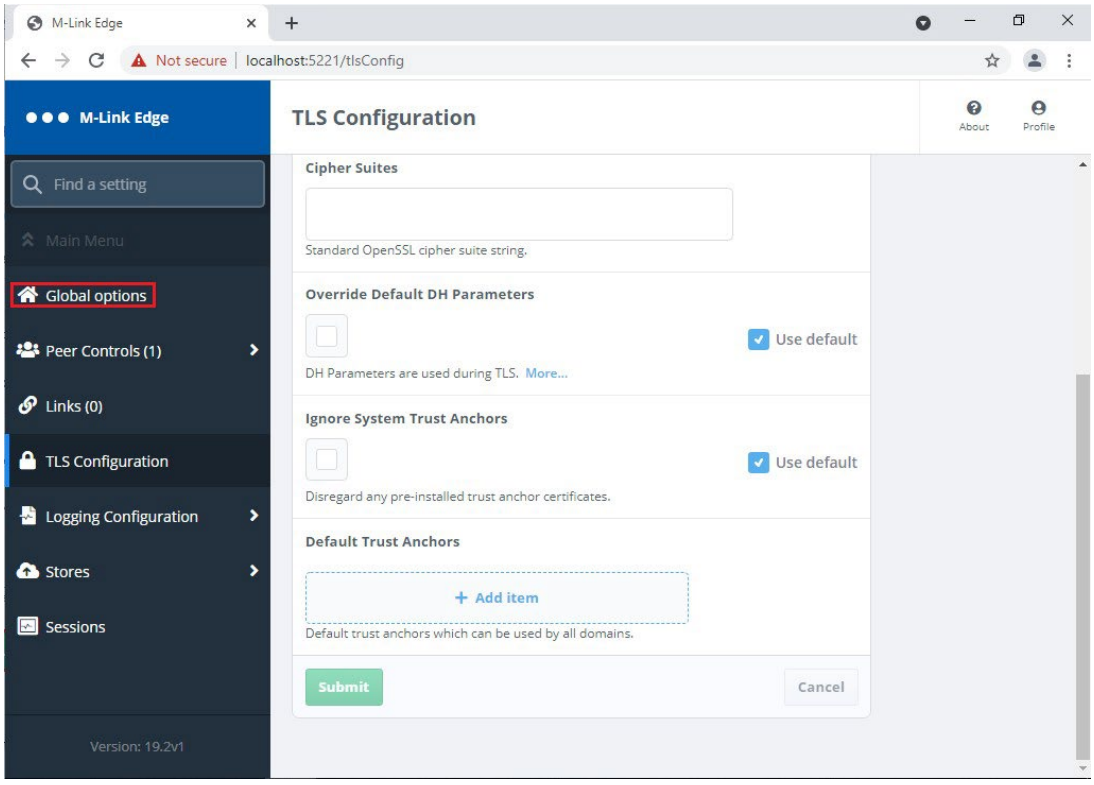

Figure 29: TLS Configuration Step 9

Click "Global options", the following screen is displayed.

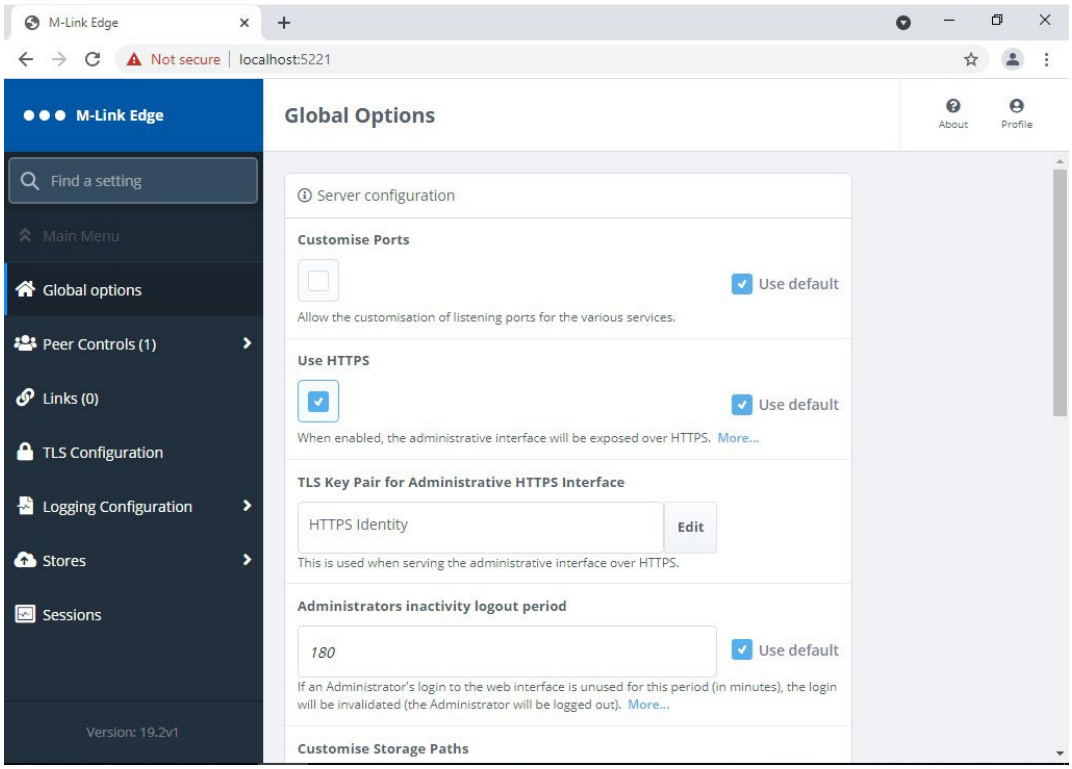

Figure 30: TLS Configuration Step 10

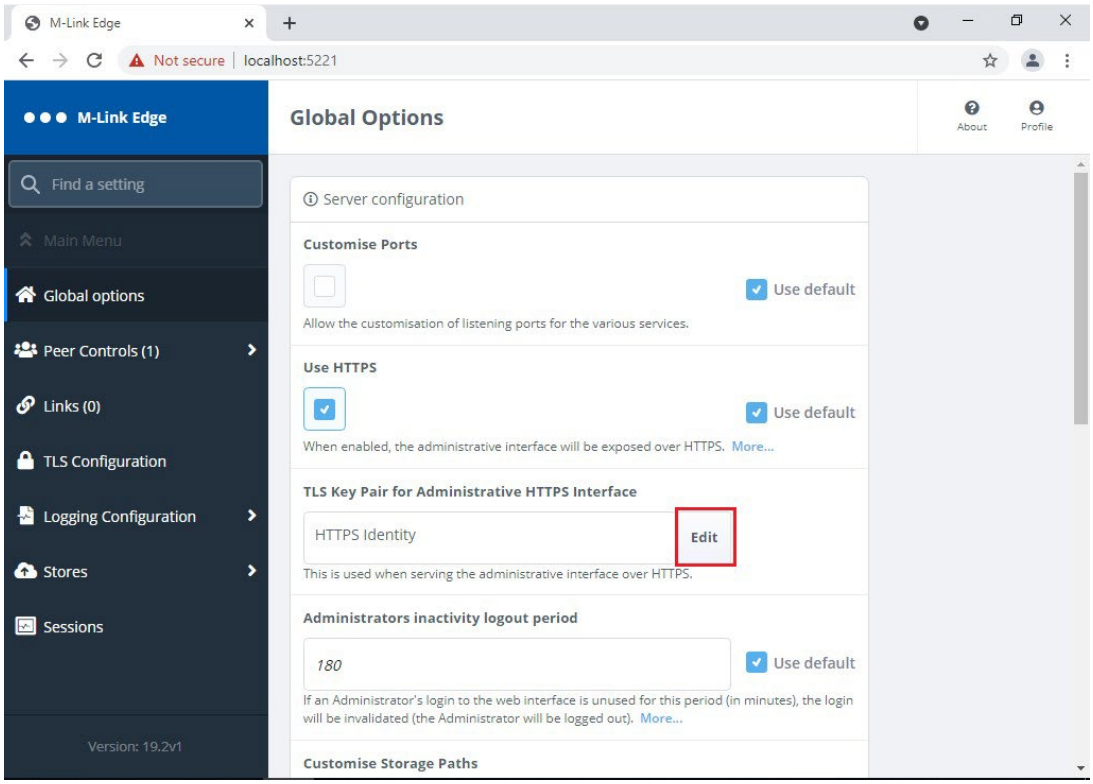

Figure 31: TLS Configuration Step 11

Click "Edit" on the "TLS Key Pair for Administrative HTTPS Interface".

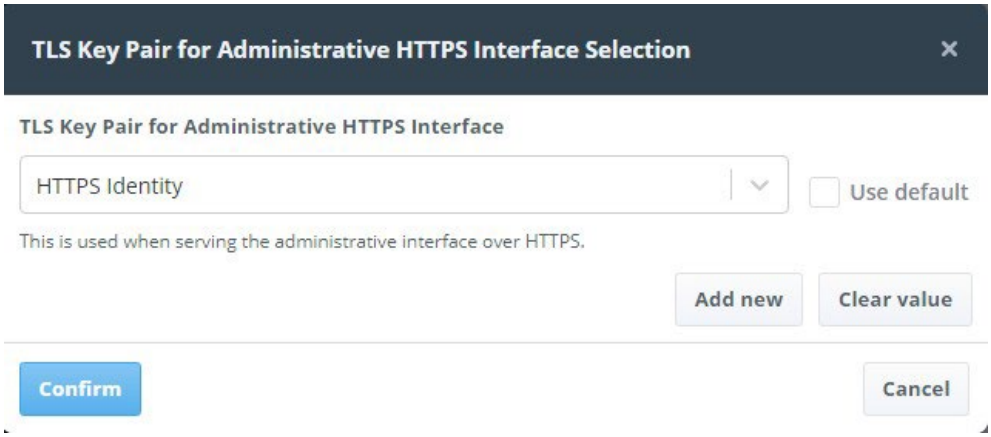

Figure 32: TLS Configuration Step 12

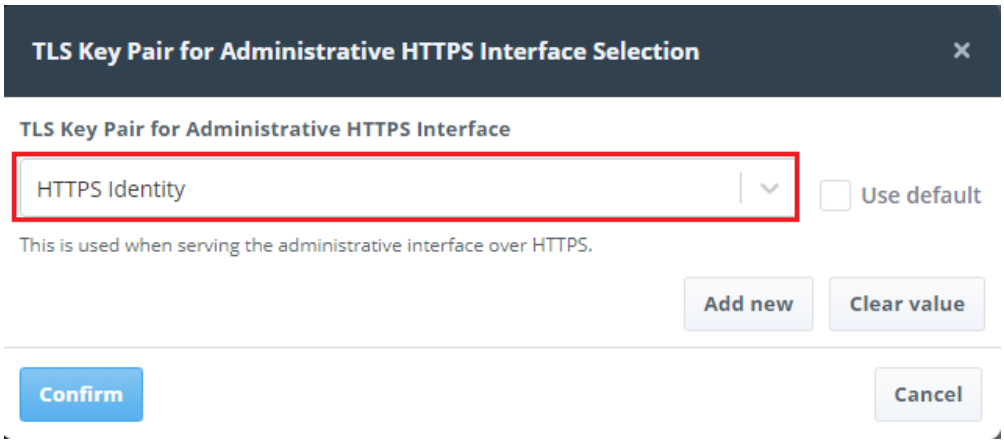

Figure 33: TLS Configuration Step 13

Select the "Dropdown".

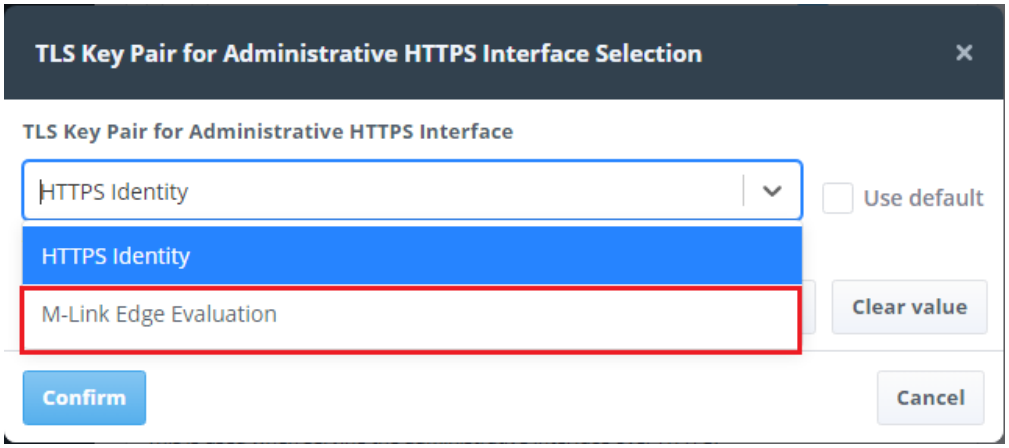

Figure 34: TLS Configuration Step 14

Select the Identity you just loaded.

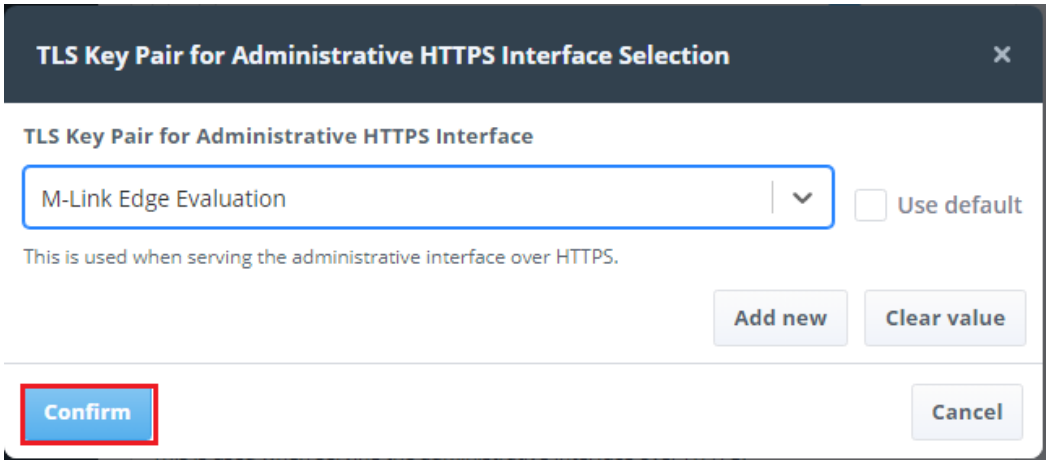

Figure 35: TLS Configuration Step 15

Click "Confirm".

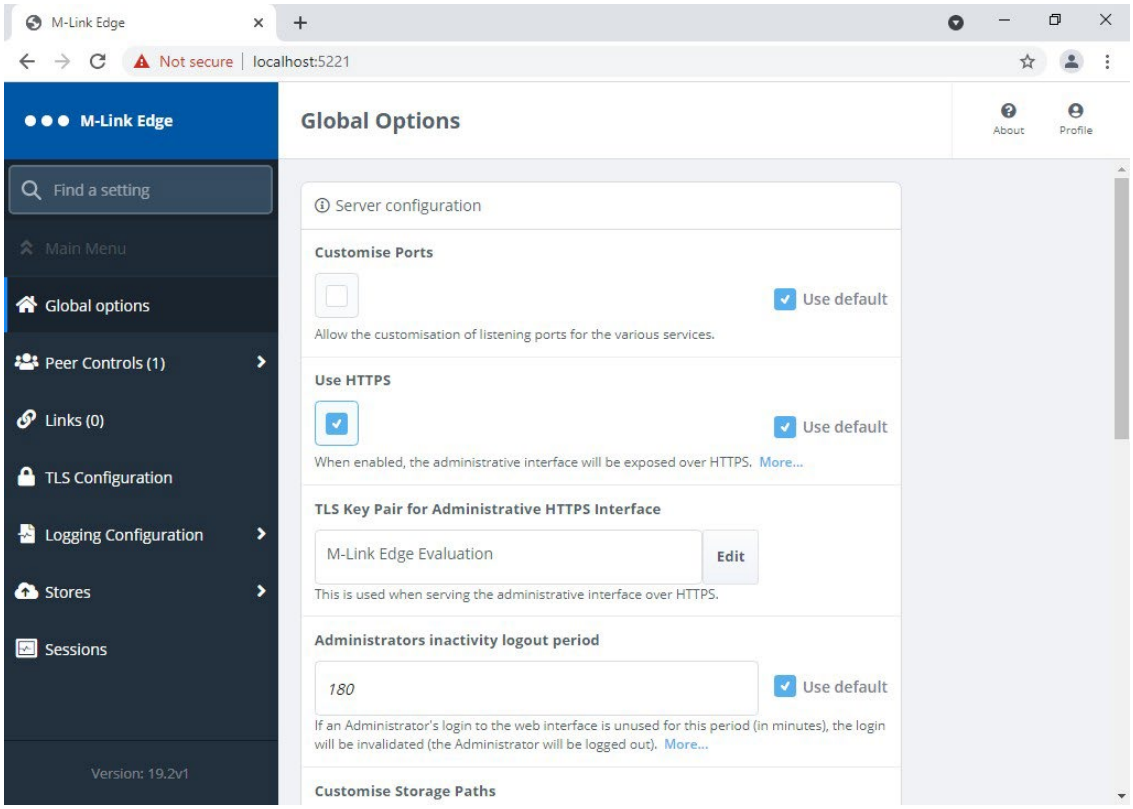

Figure 36: TLS Configuration Step 16

Scroll down to the bottom of the screen.

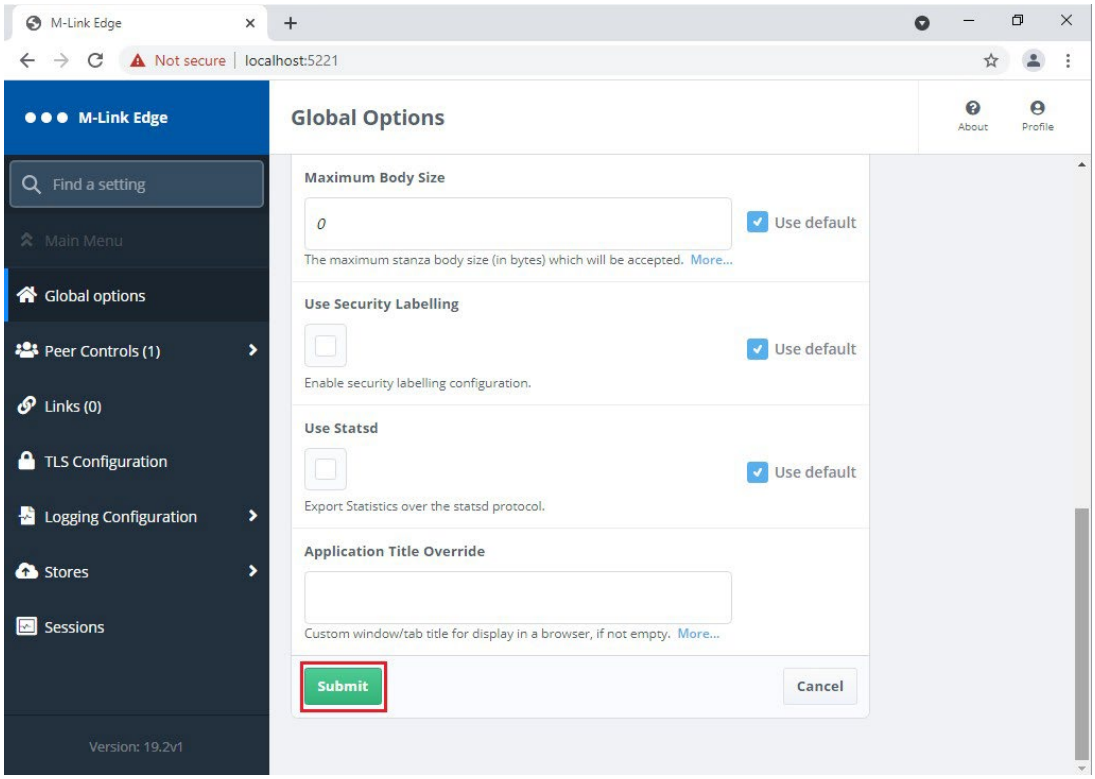

Figure 37: TLS Configuration Step 17

Click "Submit", the following screen is displayed – this is normal.

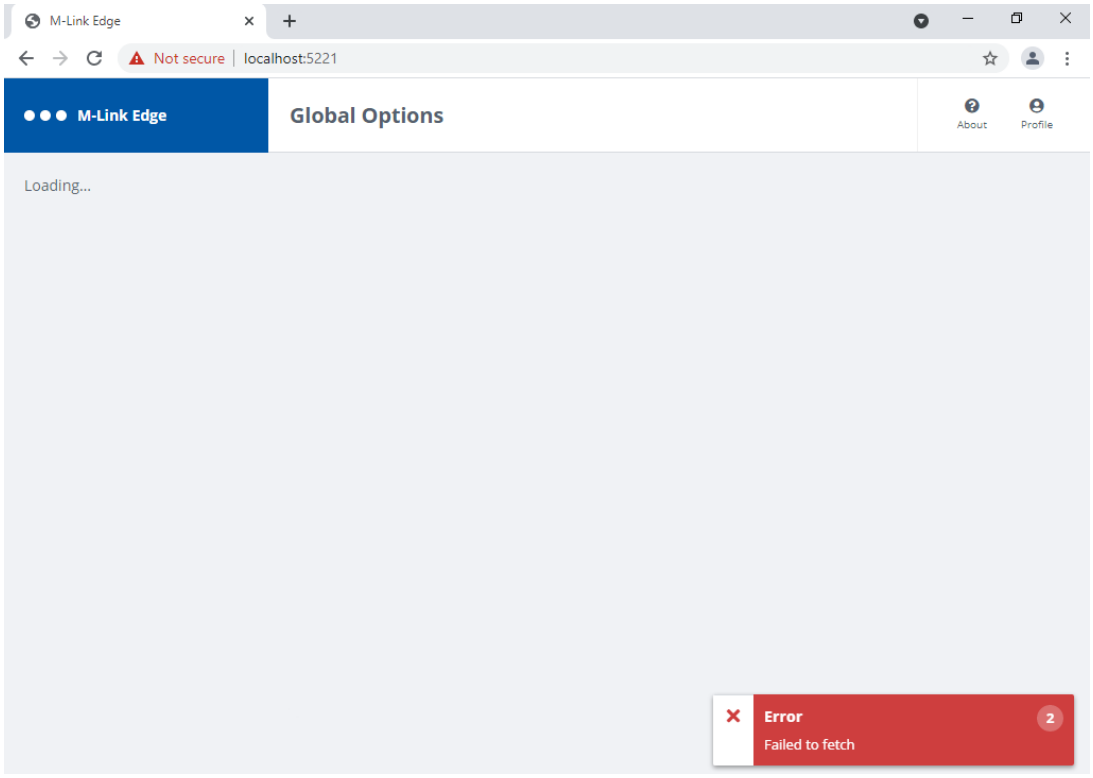

Figure 38: TLS Configuration Step 18

Now point your browser at https://hostname:5221 .

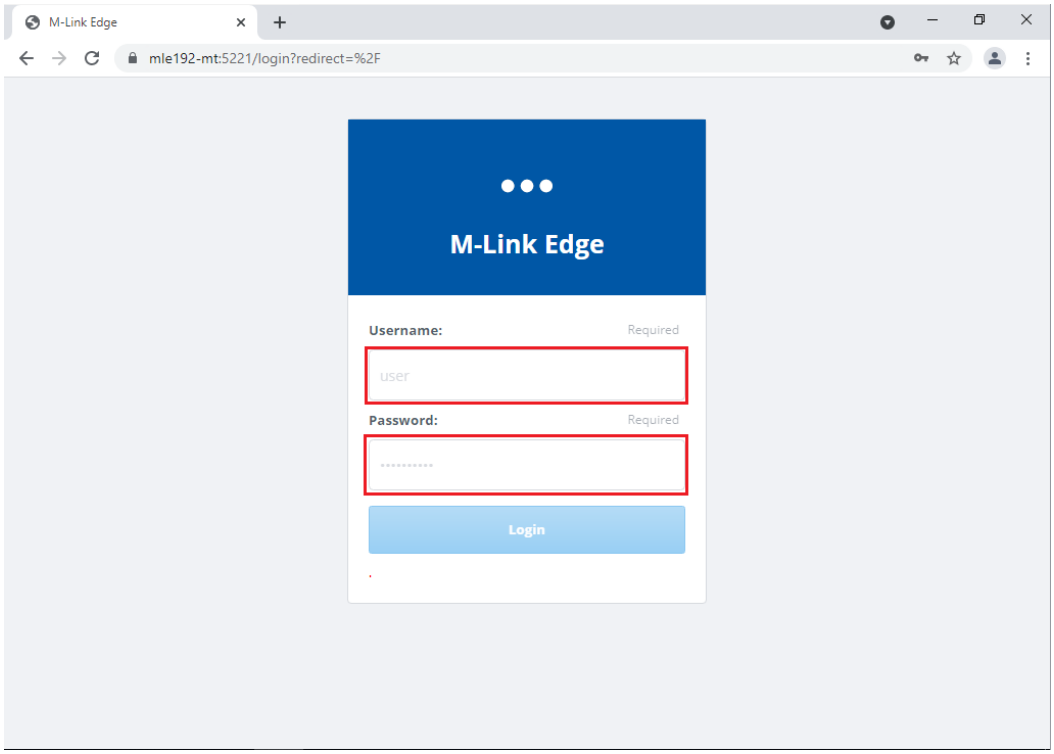

Figure 39: TLS Configuration Step 19

Enter the "Admin" Username and Password you previously configured.

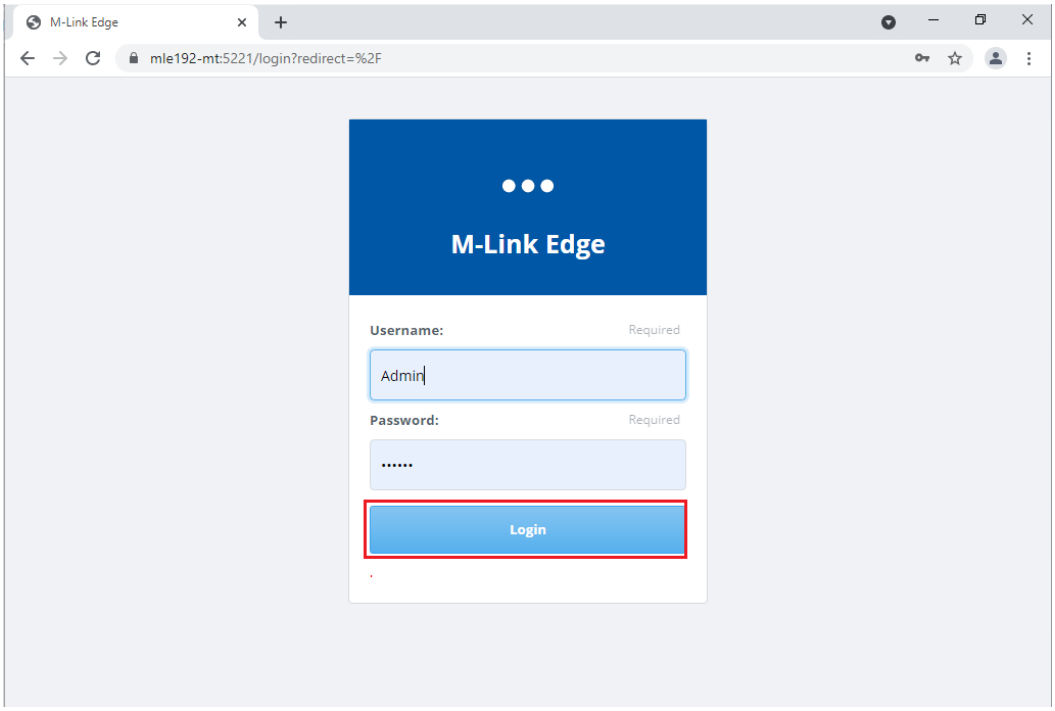

Figure 40: TLS Configuration Step 20

Click "Login".

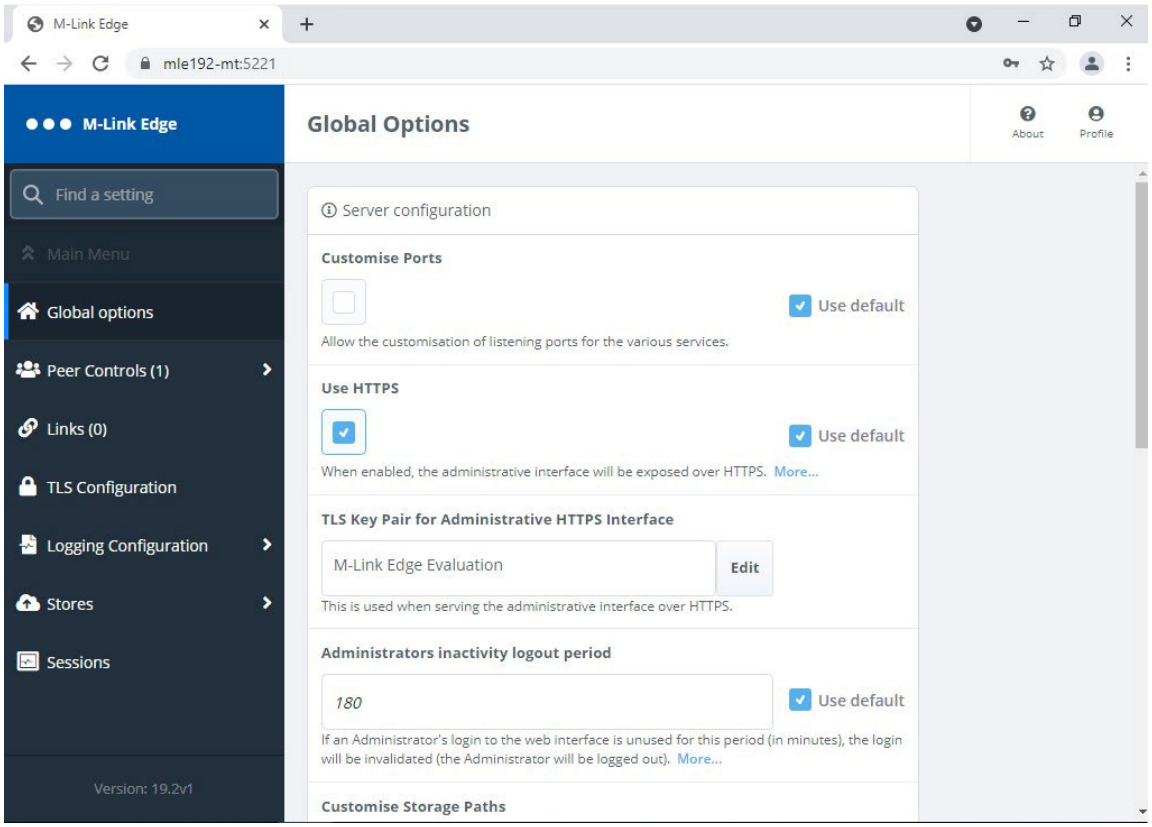

Figure 41: TLS Configuration Complete

Your TLS configuration is now complete and you can proceed to configuring other options.

Configuring a GCXP Link

A GCXP Link is typically used for connecting to Isode's M-Guard product but is a published standard so could be used by other vendors. M-Guard requires a TLS connection so M-Link EDGE will need to import the M-Guard Certificate Chain (CA Certificate and Server Certificate) in PEM format before configuring the Link. These steps will be the same for any Link that requires TLS.

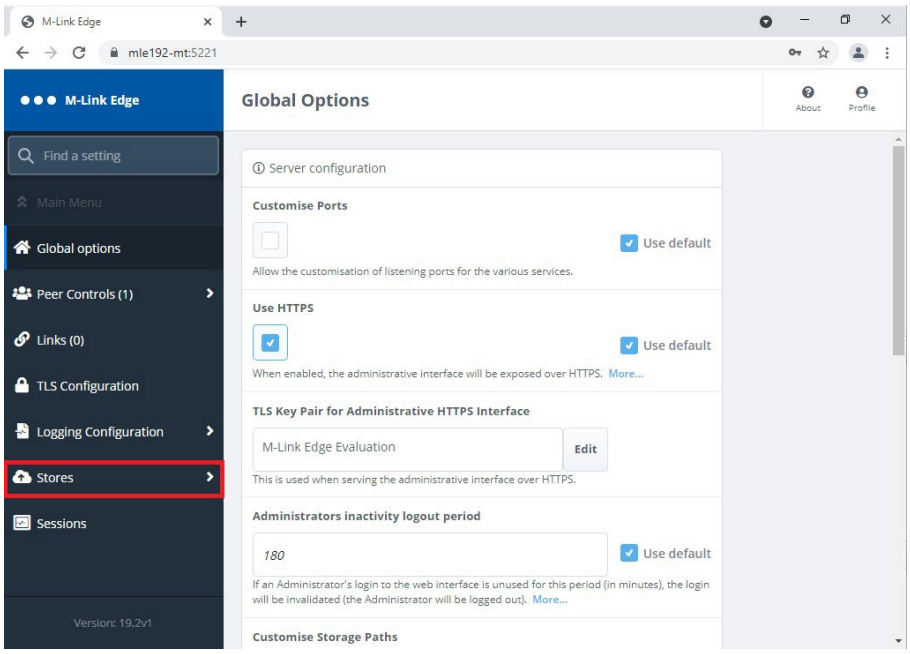

Figure 42: Adding M-Guard Certificate Chain in PEM format Step 1.

Click "Stores".

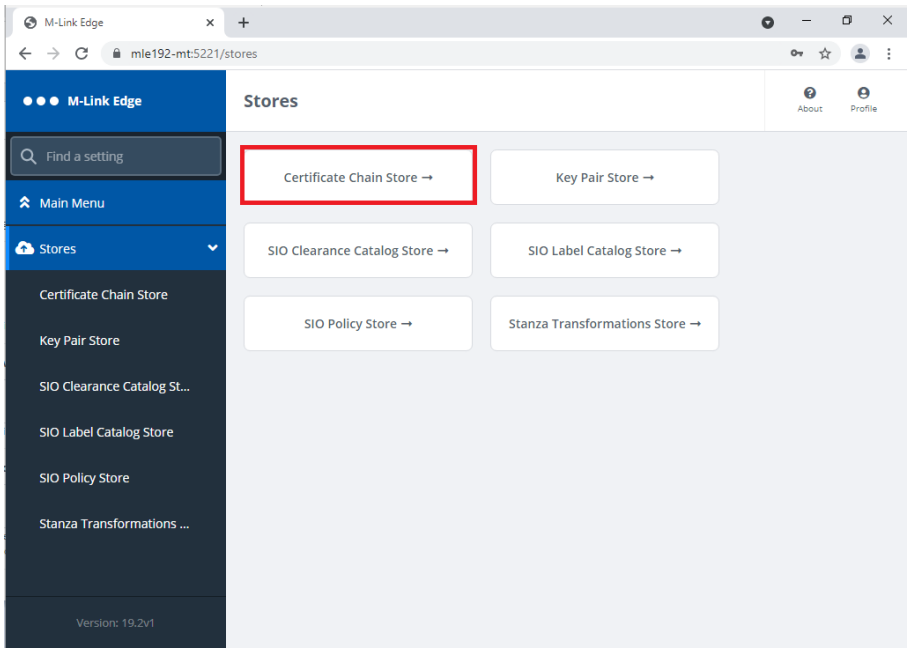

Figure 43: Adding M-Guard Certificate Chain in PEM format Step 2.

Click "Certificate Chain Store".

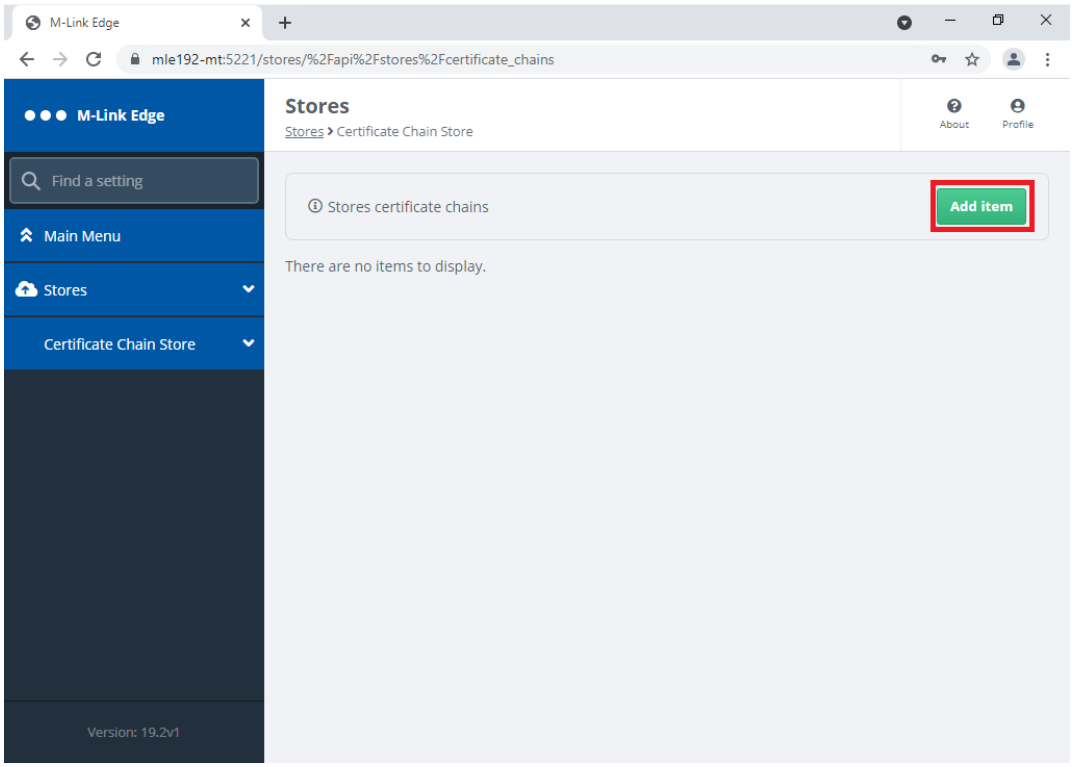

Figure 44: Adding M-Guard Certificate Chain in PEM format Step 3.

Click "Add item".

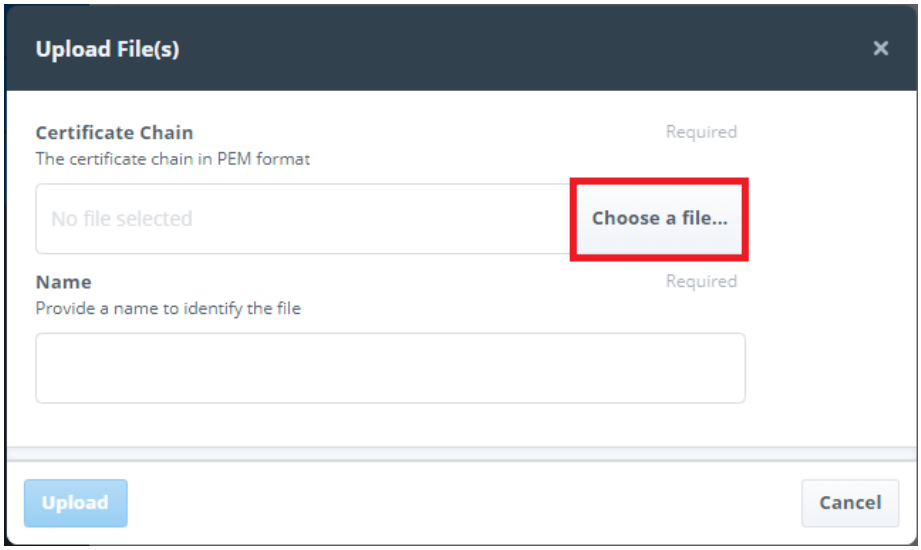

Figure 45: Adding M-Guard Certificate Chain in PEM format Step 4.

Click "Choose a file…", then select the PEM file containing the Certificate Chain from the File Explorer.

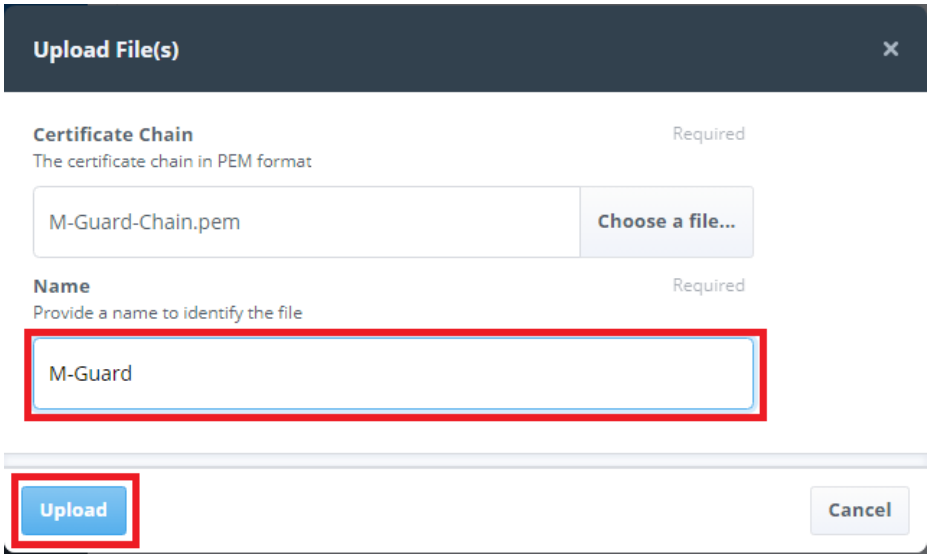

Figure 46: Adding M-Guard Certificate Chain in PEM format Step 5.

Enter a "Friendly Name for the Certificate and Click "Upload".

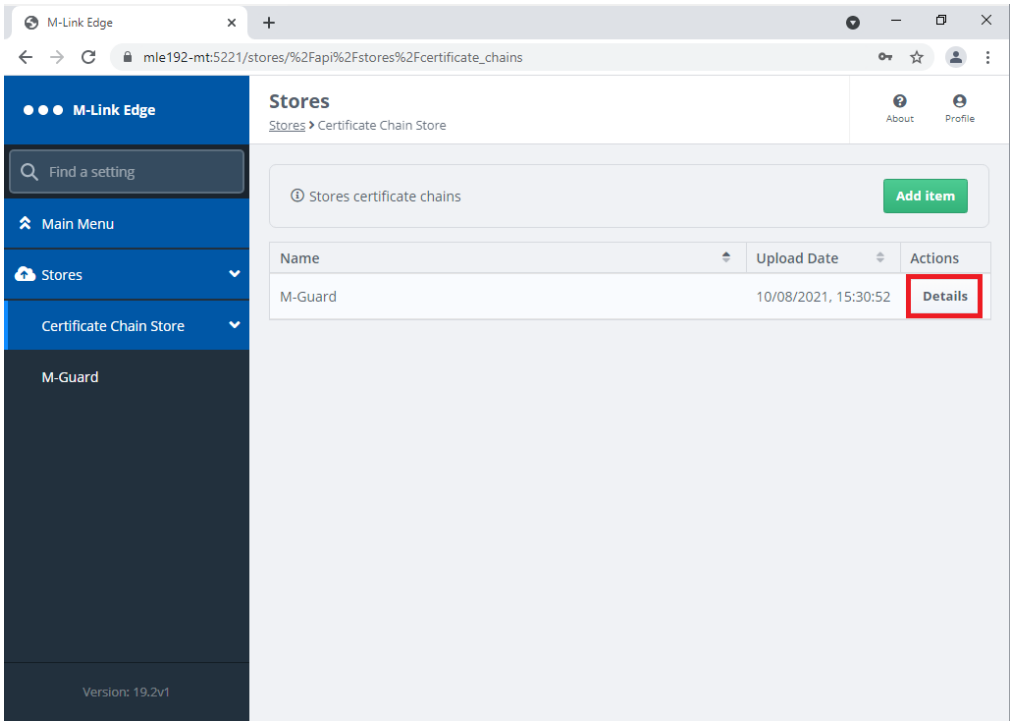

Figure 47: Adding M-Guard Certificate Chain in PEM format Step 6.

To check the details of the Certificate, Click "Details".

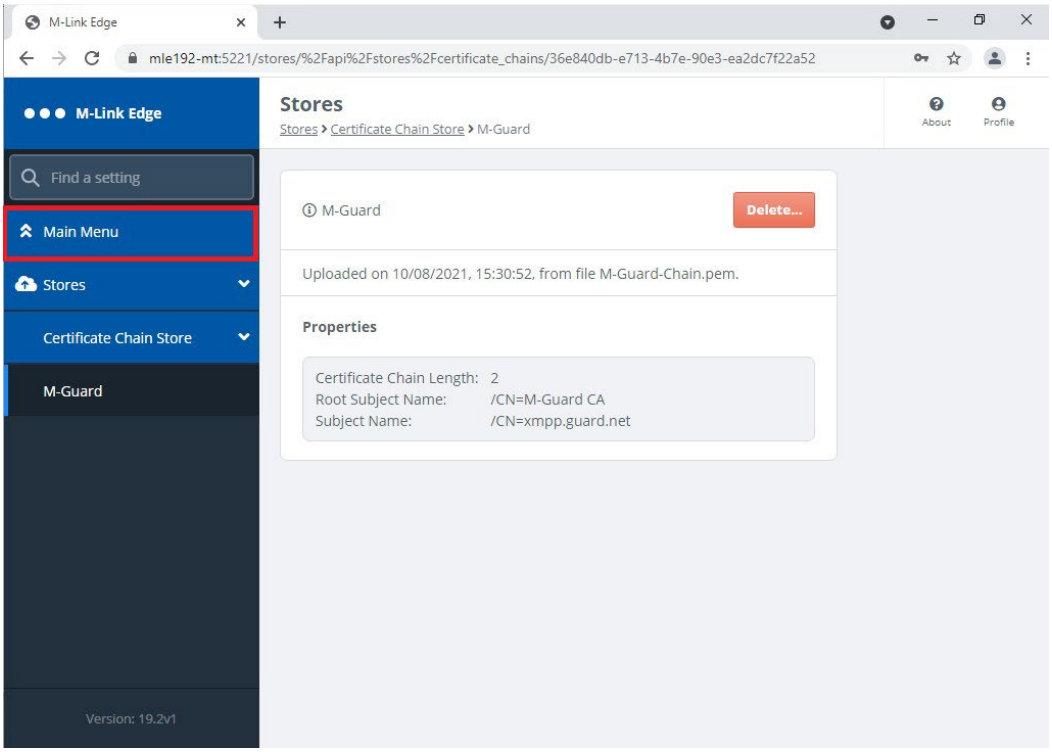

Figure 48: Adding M-Guard Certificate Chain in PEM format Step 7.

You can optionally delete the Certificate here if it is wrong, we will now continue with the configuration of the GCXP Link so Click, "Main Menu".

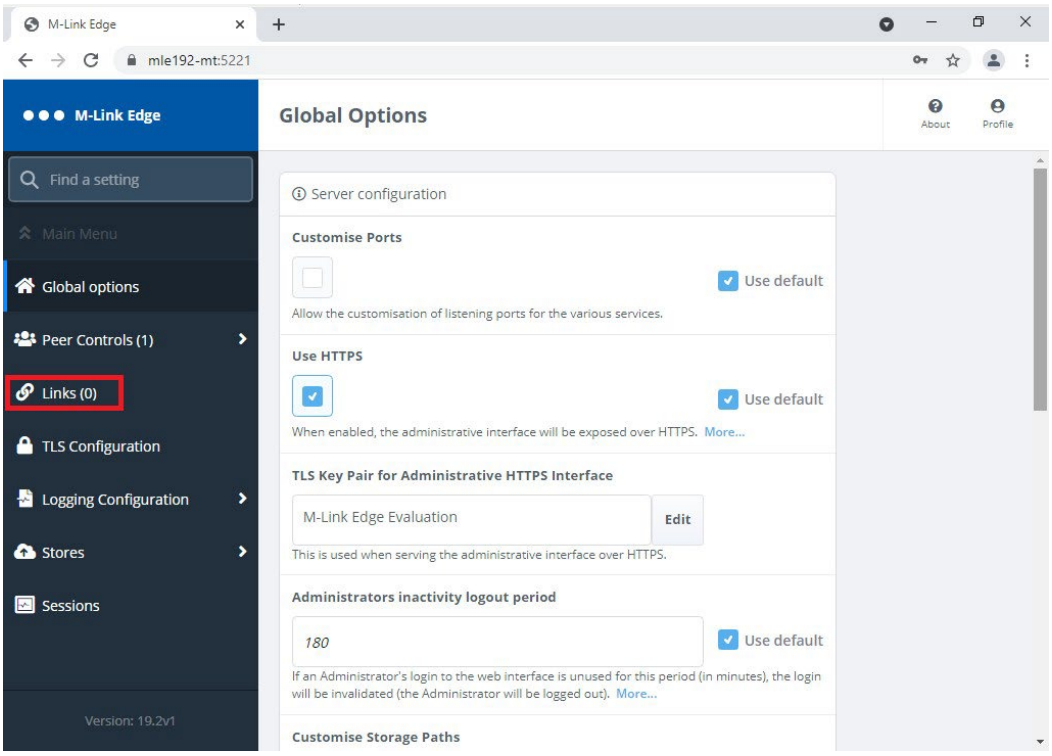

Figure 49: Configuring the GCXP Link Step 1.

Click "Links", not the number in brackets indicates the number of links currently configured.

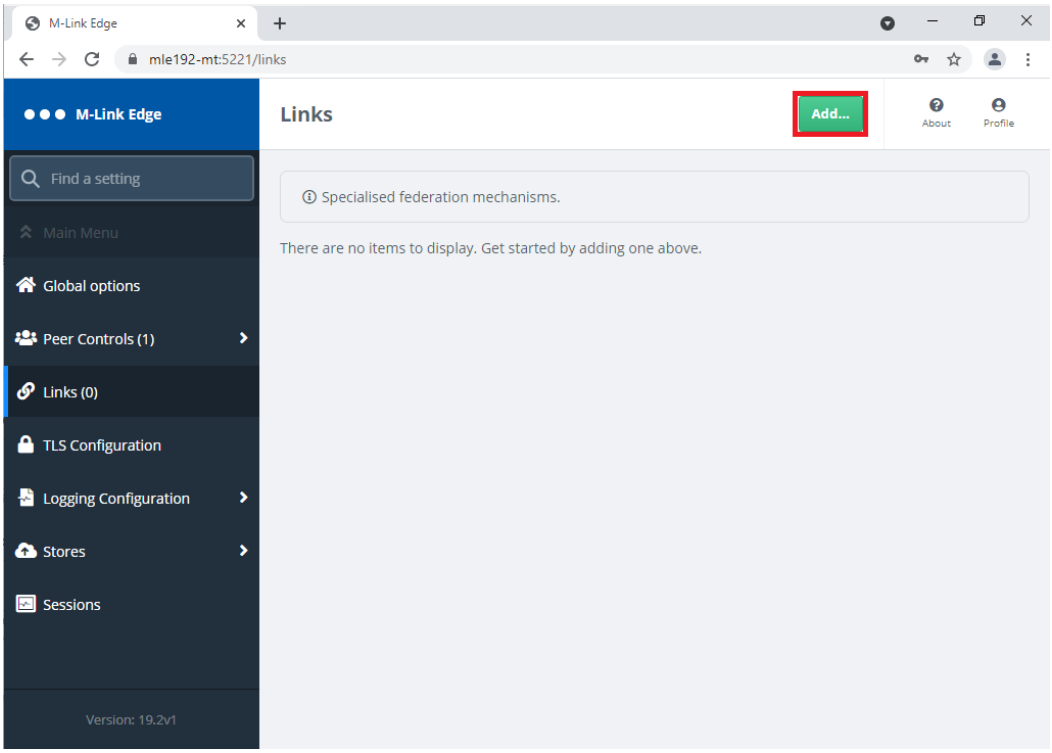

Figure 50: Configuring the GCXP Link Step 2.

Click "Add…".

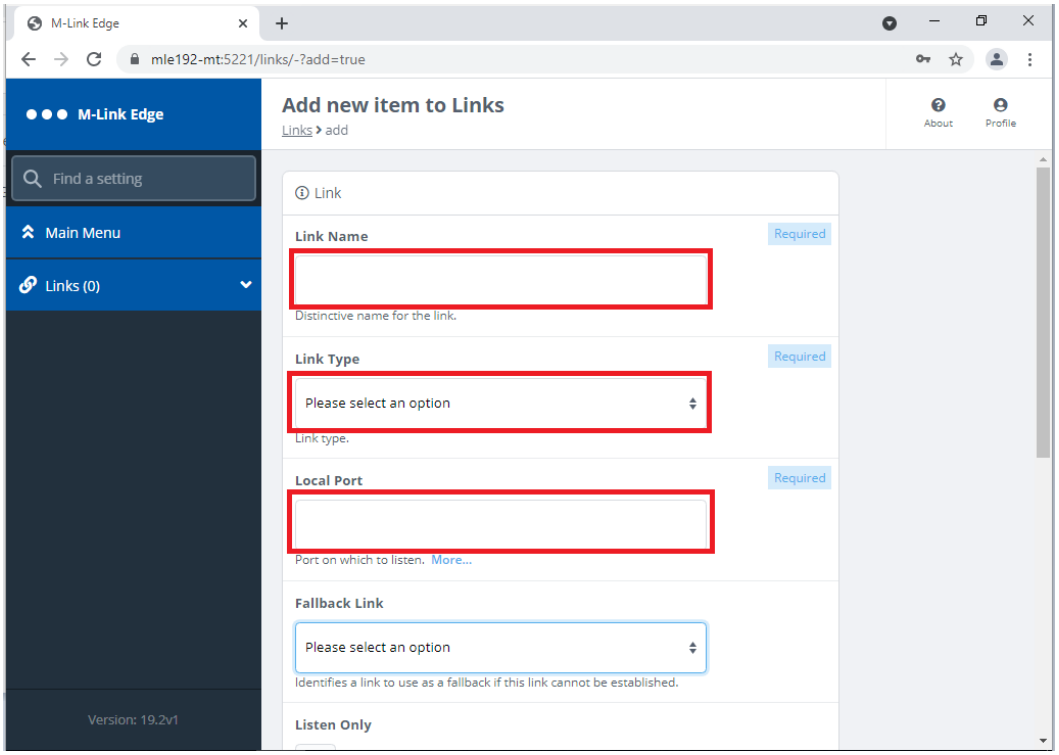

Figure 51: Configuring the GCXP Link Step 3.

Enter a "Friendly Name" for the "Link Name", select "GCXP" from the Drop Down for the "Link Type" and enter the Port that M-Link EDGE will listen on.

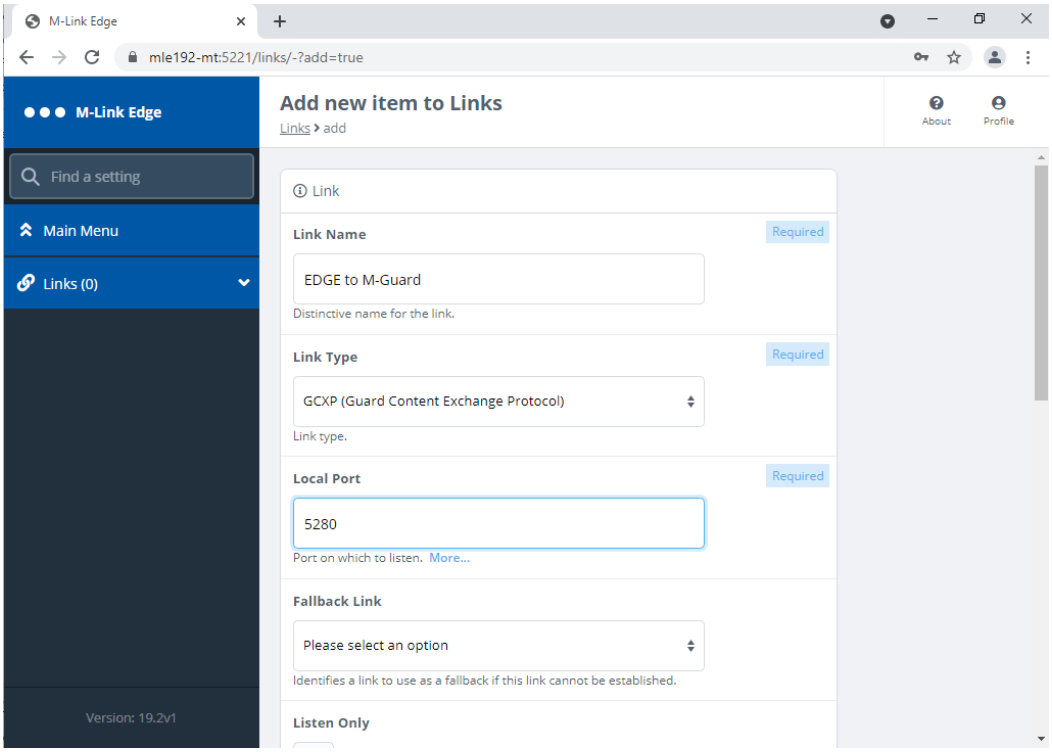

Figure 52: Configuring the GCXP Link Step 4.

Now scroll down.

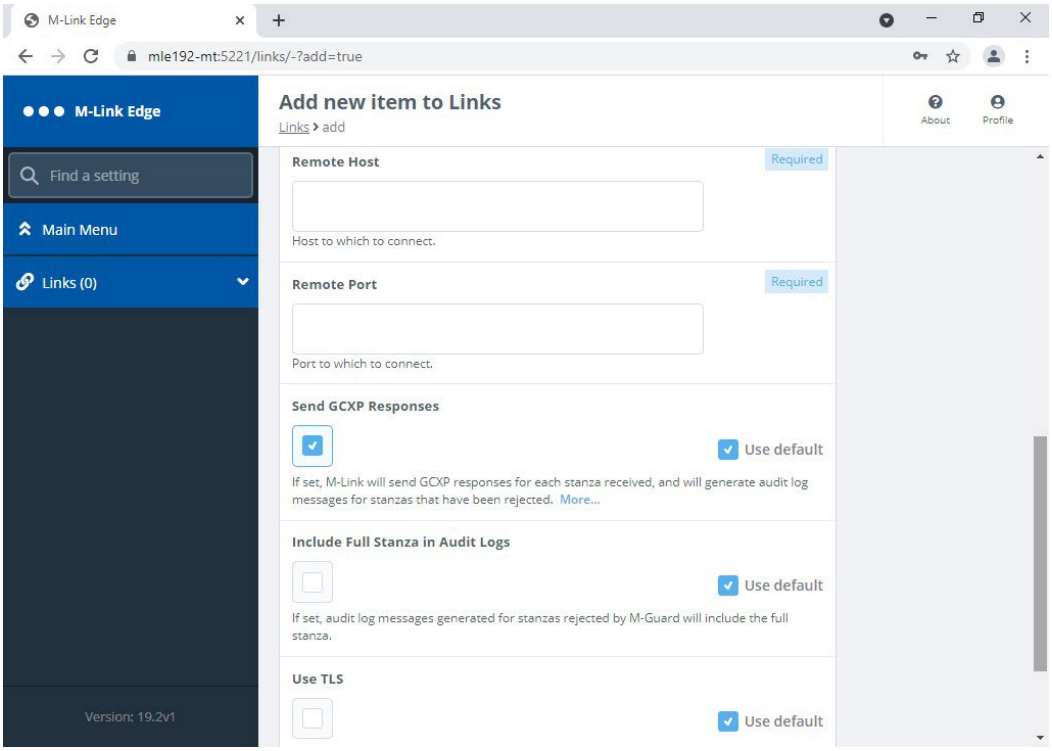

Figure 53: Configuring the GCXP Link Step 5.

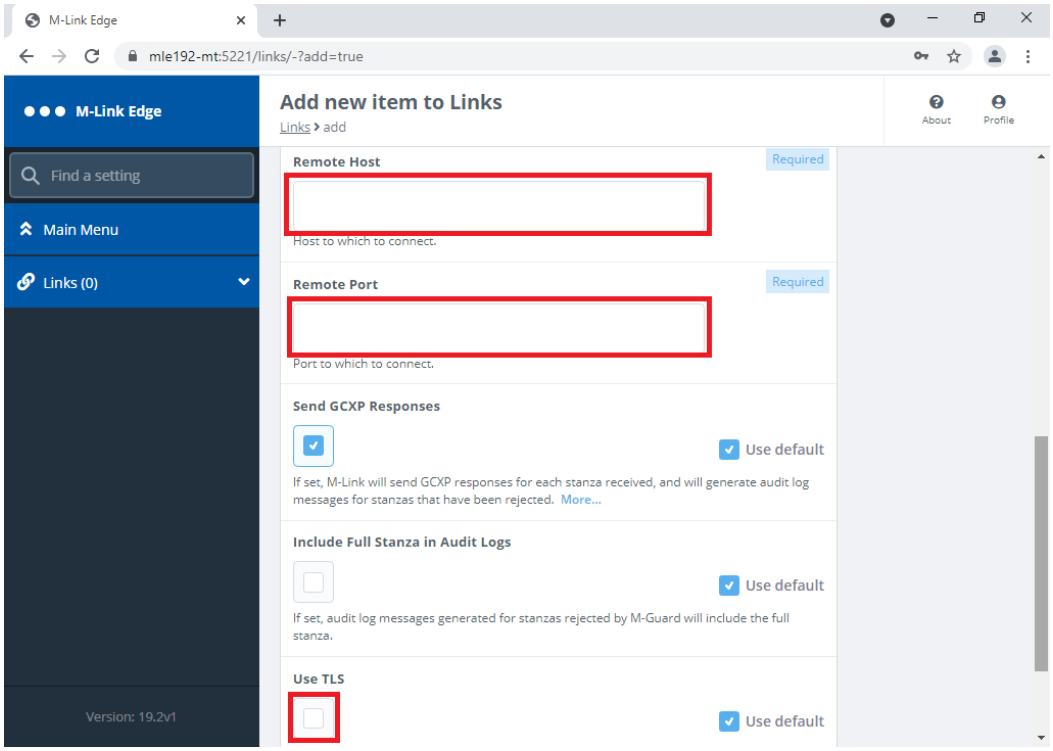

Figure 53: Configuring the GCXP Link Step 5.

Enter the "Remote Host" and "Remote Port" of the M-Guard Server you will be using and check the "Use TLS" box.

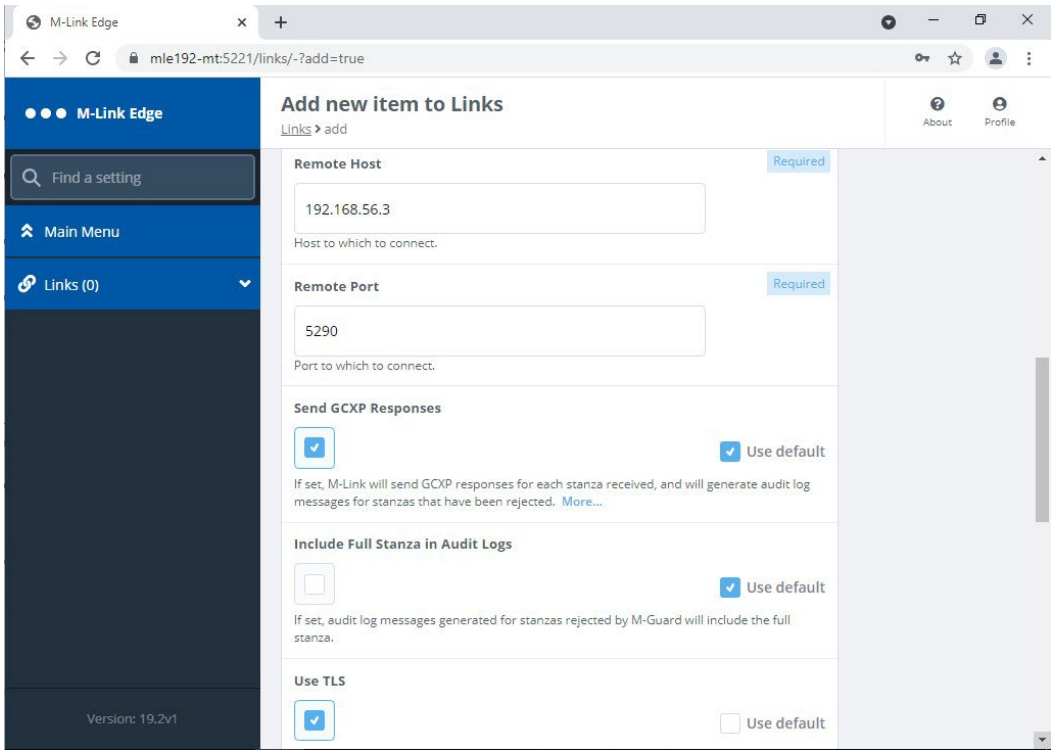

Figure 54: Configuring the GCXP Link Step 6.

Scroll down to configure the TLS.

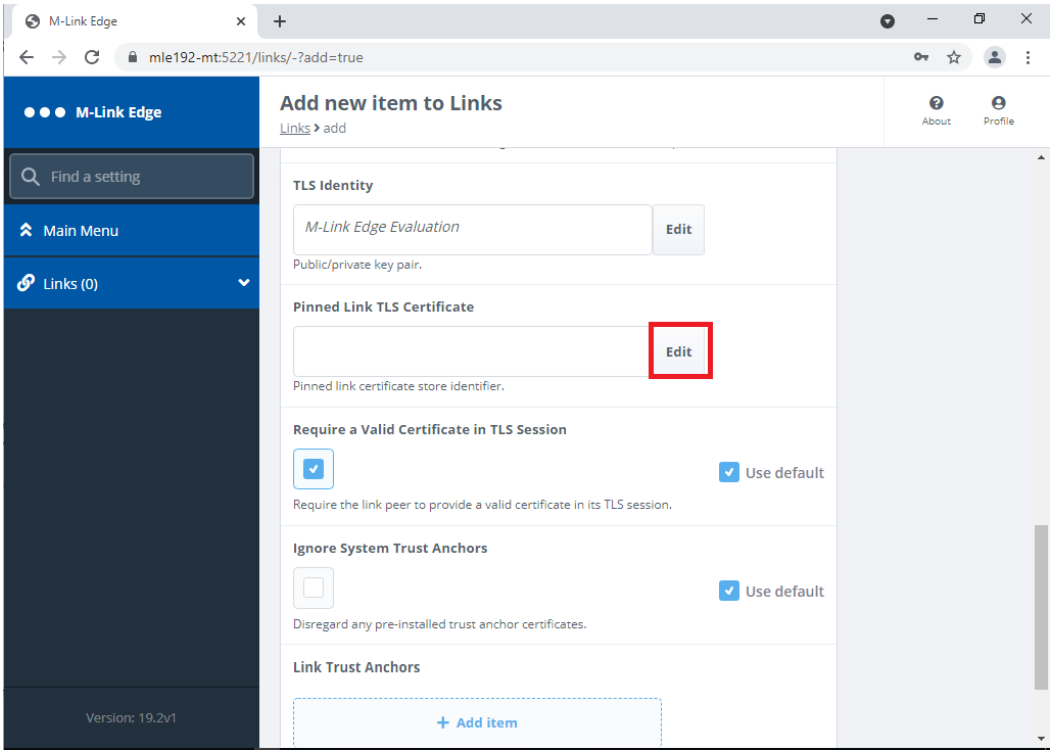

Figure 55: Configuring the GCXP Link Step 7.

As the Certificate we are using is a Certificate Chain including the Trust Anchor there is no need to add any Trust Anchors here. Click "Edit" on the "Pinned Link TLS Certificate.

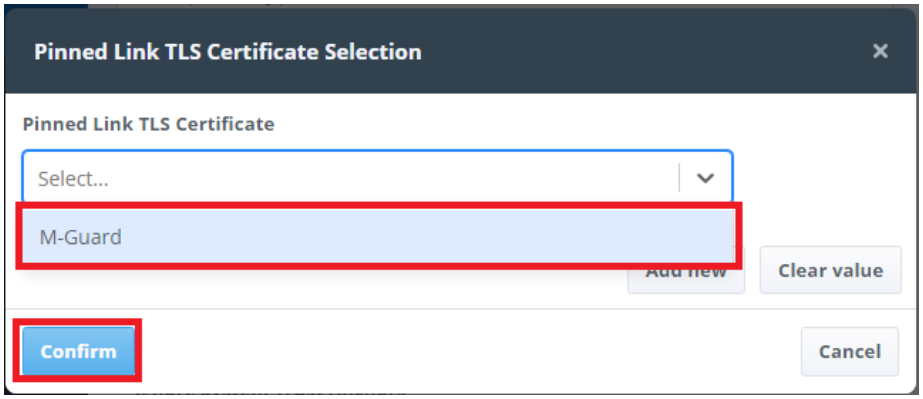

Figure 56: Configuring the GCXP Link Step 8.

Select the M-Guard Certificate you have loaded previously and Click, "Confirm".

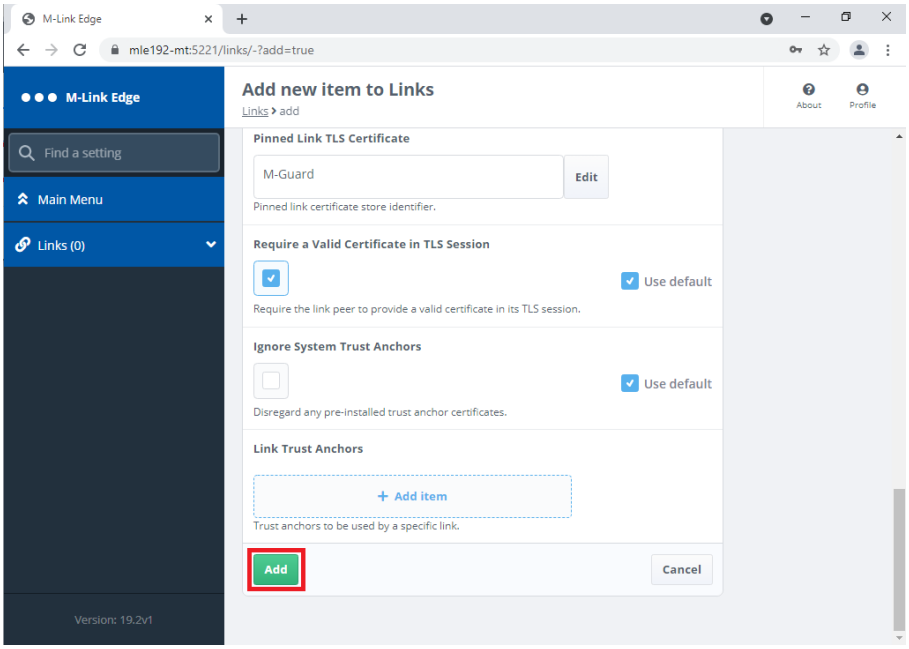

Figure 57: Configuring the GCXP Link Step 9.

Click “Add”.

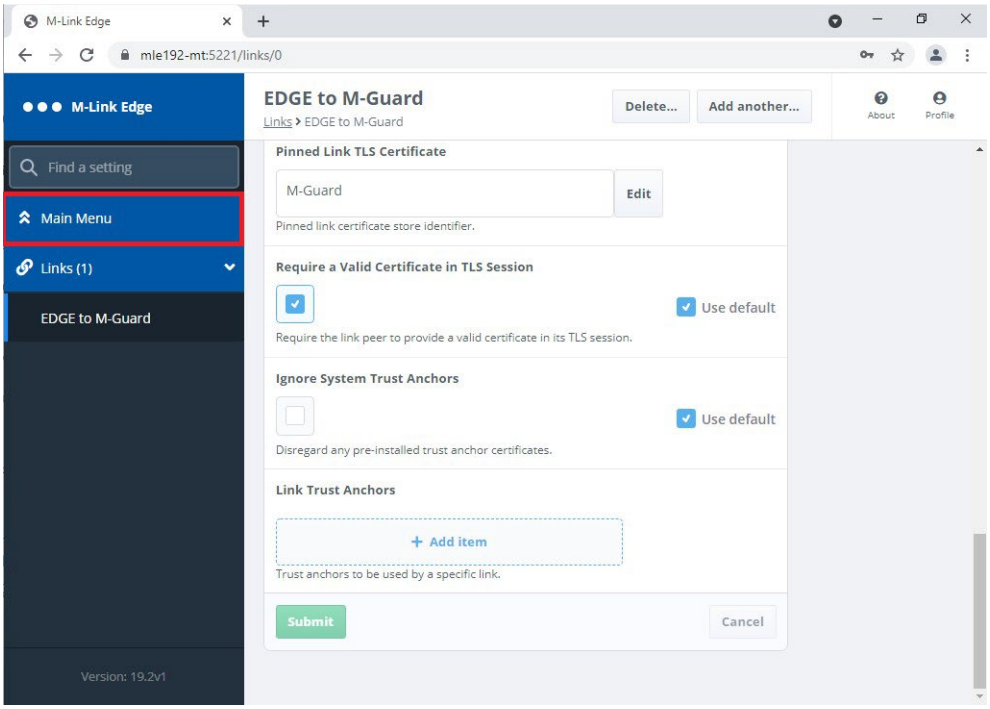

Figure 58: Configuring the GCXP Link Step 10.

We have now completed the GCXP Link configuration and are ready to create a “Peer Control” that will use it. Click “Main Menu”.

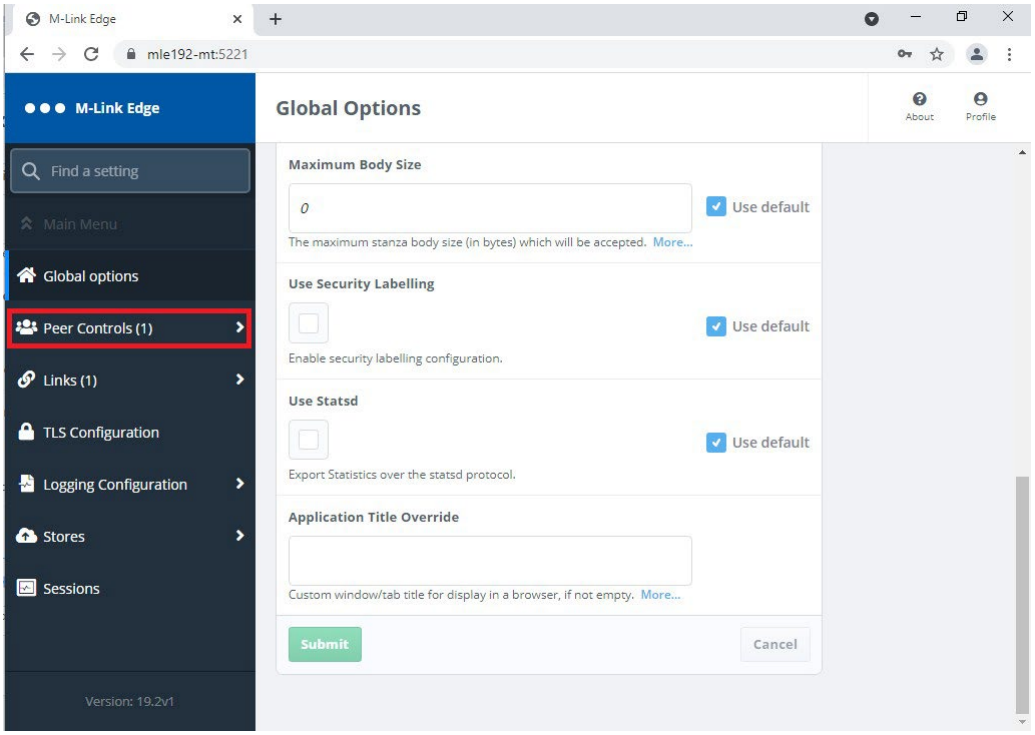

Figure 59: Configuring the Peer Control Step 1.

Select "Peer Controls" note that the number in brackets is the number of Peer Controls currently configured.

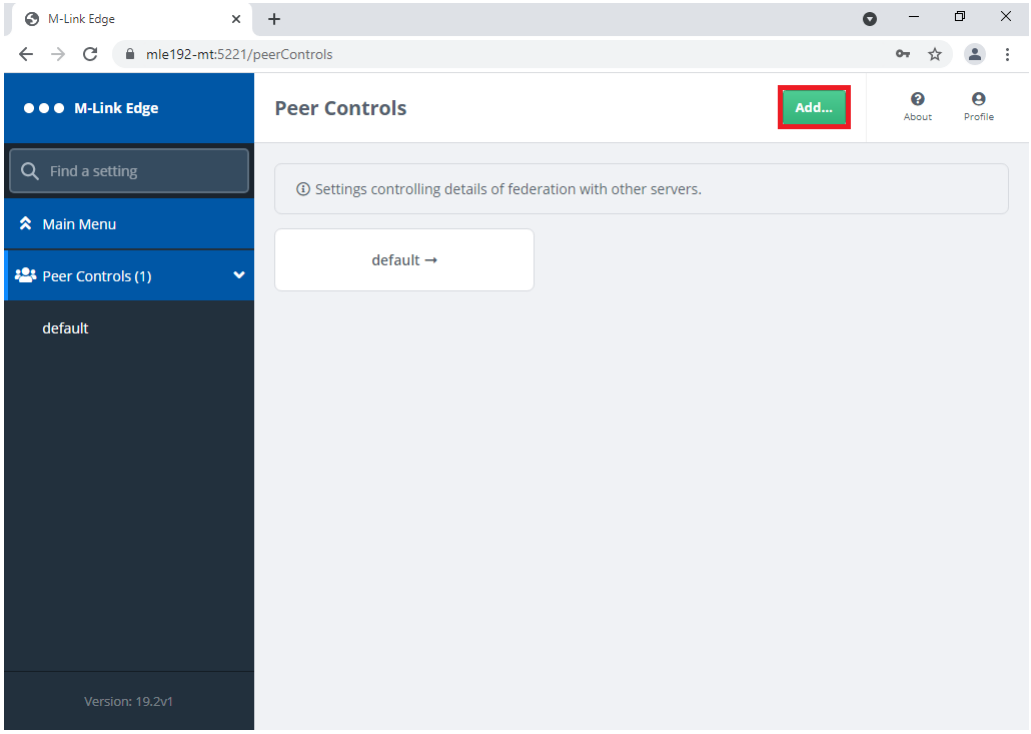

Figure 60: Configuring the Peer Control Step 2.

Click "Add…".

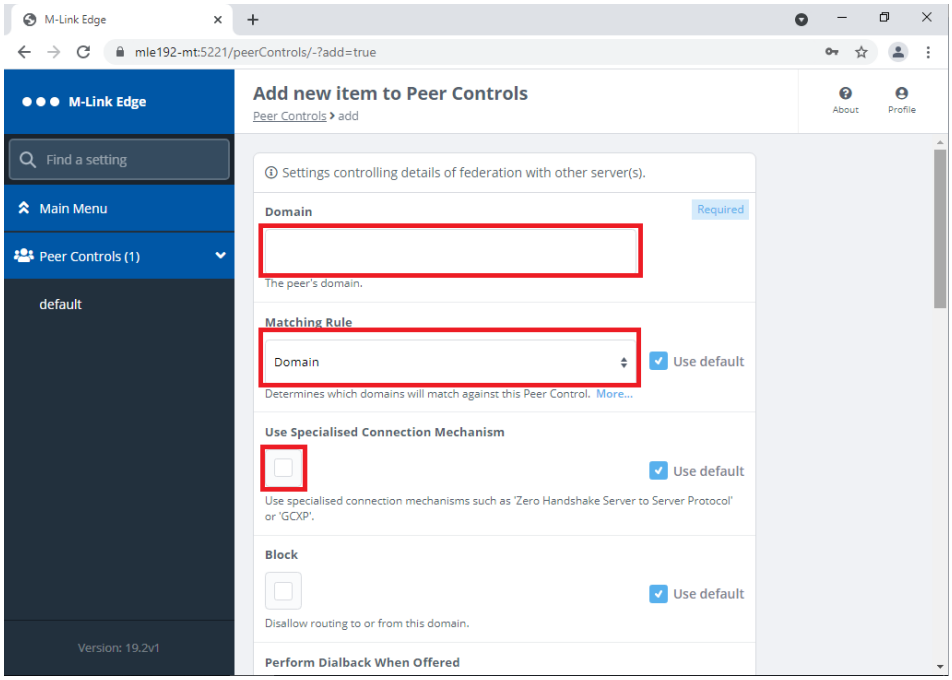

Figure 61: Configuring the Peer Control Step 3.

Complete the "Domain", "Matching Rule" and Check the "Use Specialised Connection Mechanism" Checkbox.

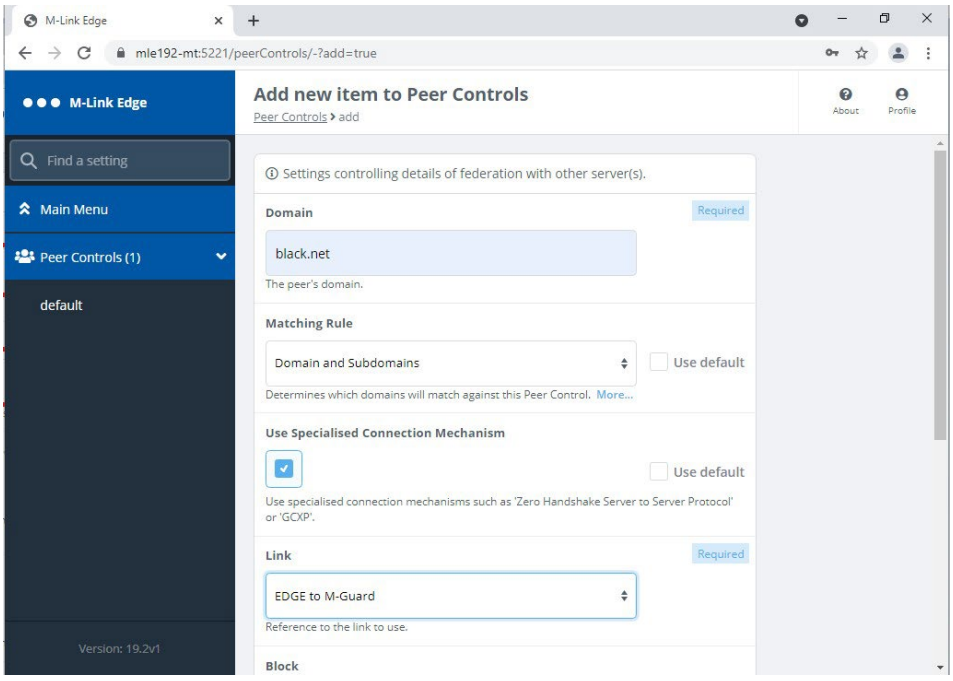

Figure 62: Configuring the Peer Control Step 4.

The "Domain" should be the XMPP Domain of the Server you are connecting to.
The "Matching Rule" should be "Domain and Subdomain" if you want to include both the 1 to 1 Domain and Multi User Chat (MUC) Domain. You should then select the "Link" you have just created from the drop down and then scroll down.

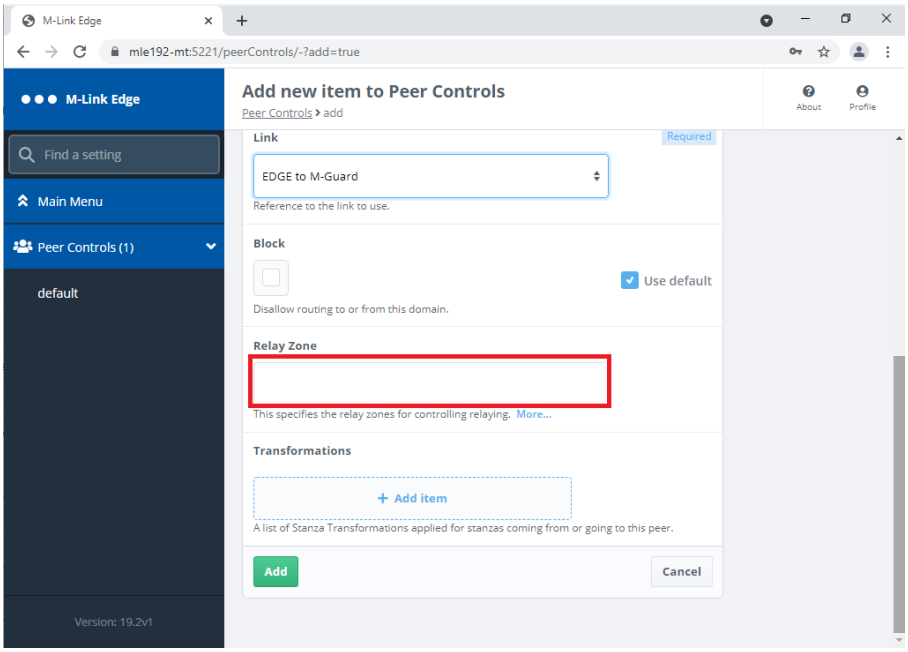

Figure 63: Configuring the Peer Control Step 5.

The M-Link EDGE Server as it has no domain of it's own it typically relays between different XMPP Domains. In order to do this each link needs a unique "Relay Zone" defined. This is a free text name, so should be something to remind you of where you are relaying between.

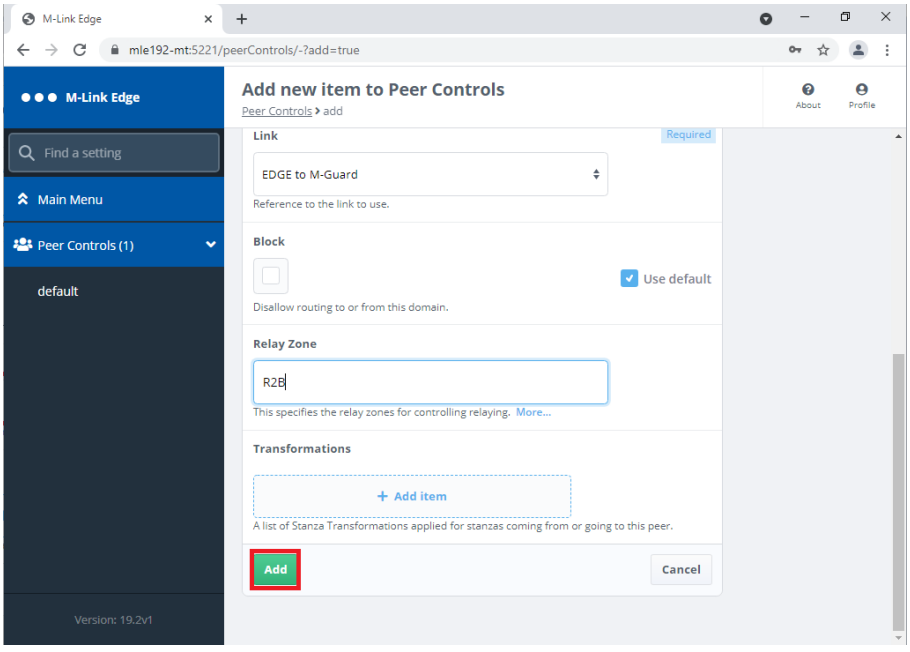

Figure 64: Configuring the Peer Control Step 6.

Enter your "Relay Zone" name and Click "Add".

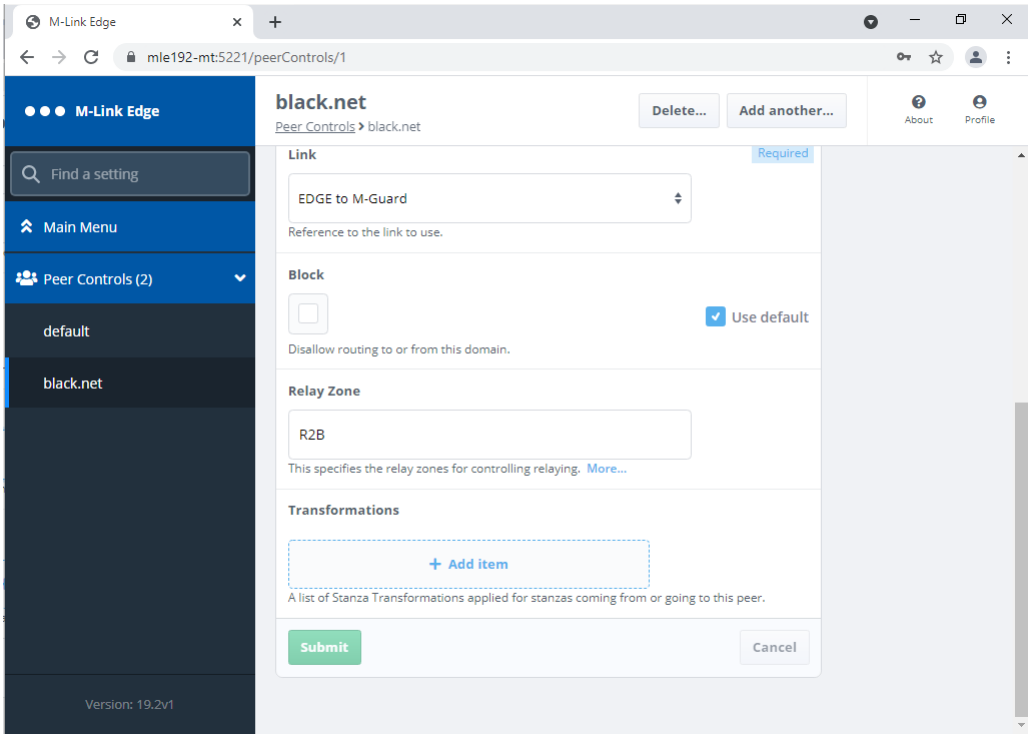

Figure 65: Configuring the Peer Control Step 7.

You have now completed the configuration of the GCXP Link and associated Peer Control. We will now proceed to create an XEP-0361 Zero Handshake Server to Server Protocol Link (X2X) and associated Peer Control.

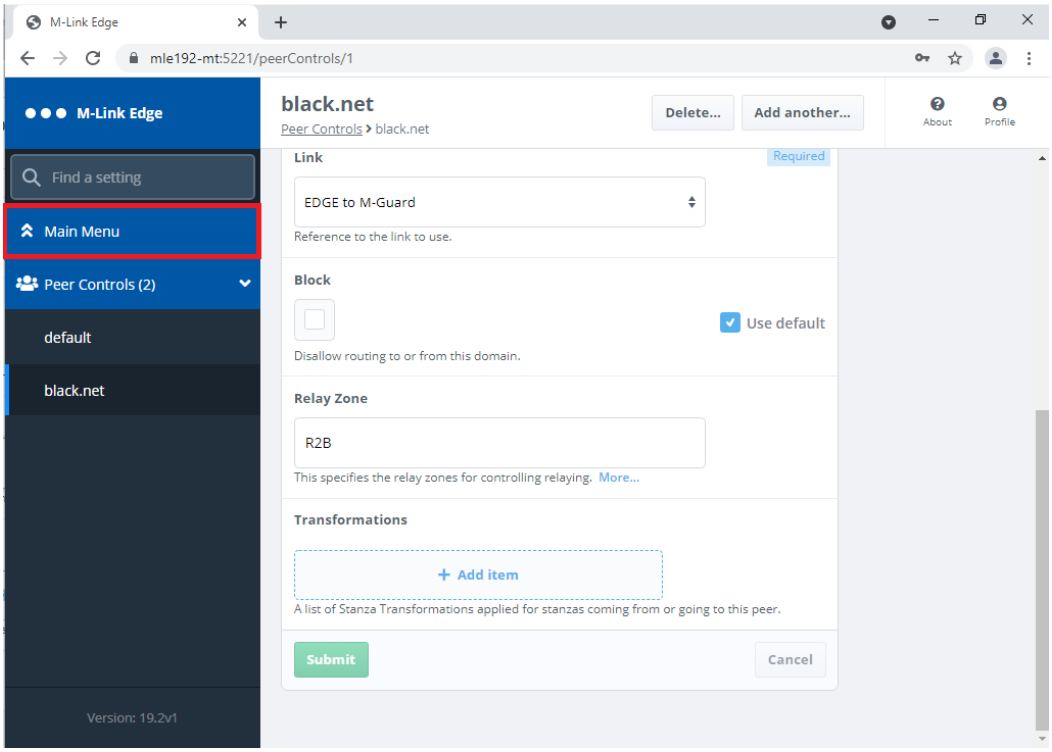

Figure 66: Configuring the Peer Control Complete.

Click “Main Menu”.

Configuring a XEP-0361 Zero Handshake Server to Server Protocol Link

A XEP-0361 Zero Handshake Server to Server Protocol Link is typically used for connecting over a Low Bandwidth TCPIP Connection e.g. SATCOM or some 3rd Party XMPP Guards.

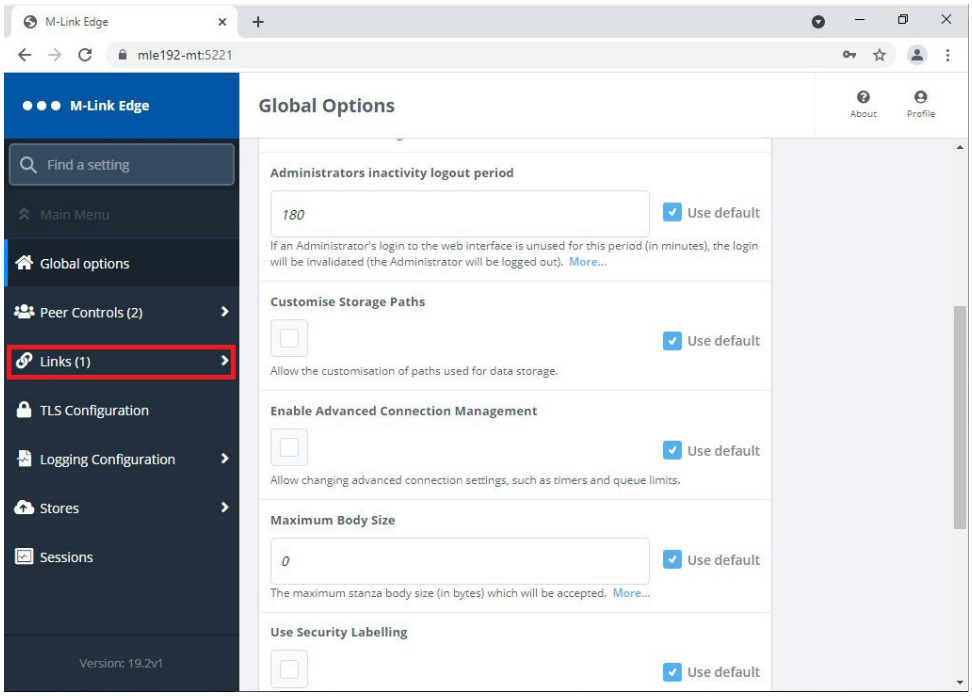

Figure 67: Configuring the XEP-0361 Zero Handshake Server to Server Protocol Link Step 1.

Click "Links".

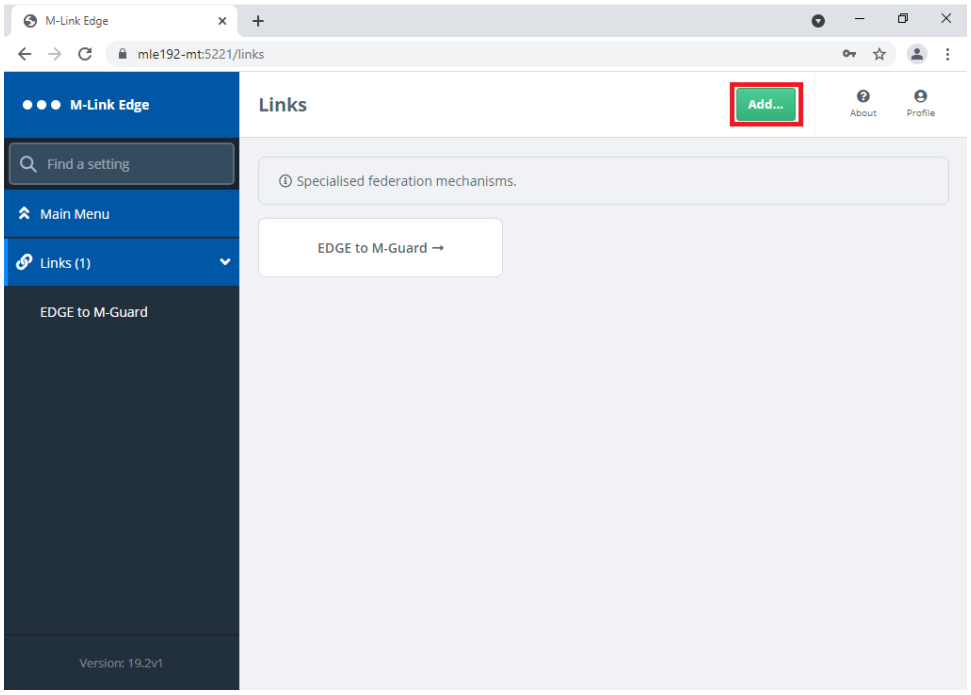

Figure 68: Configuring the XEP-0361 Zero Handshake Server to Server Protocol Link Step 2.

Click "Add…".

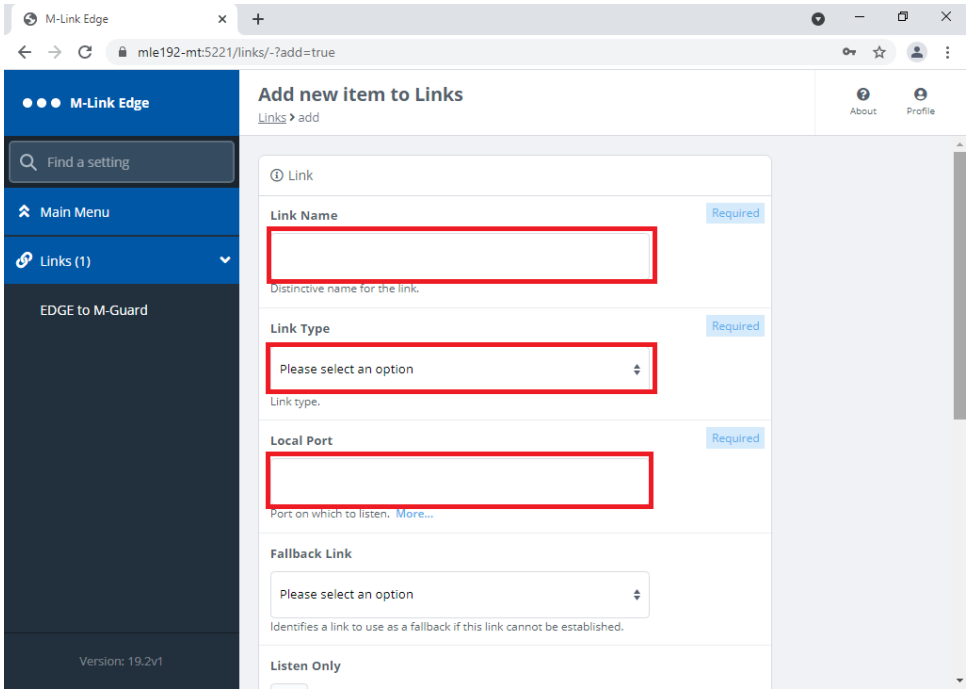

Figure 69: Configuring the XEP-0361 Zero Handshake Server to Server Protocol Link Step 3.

The "Link Name" is a "Friendly Name" that you should use to identify the Link, the "Link Type" will be "XEP-0361 Zero Handshake Server to Server Protocol Link" selected from the drop down. The Port will be agreed between the two servers.

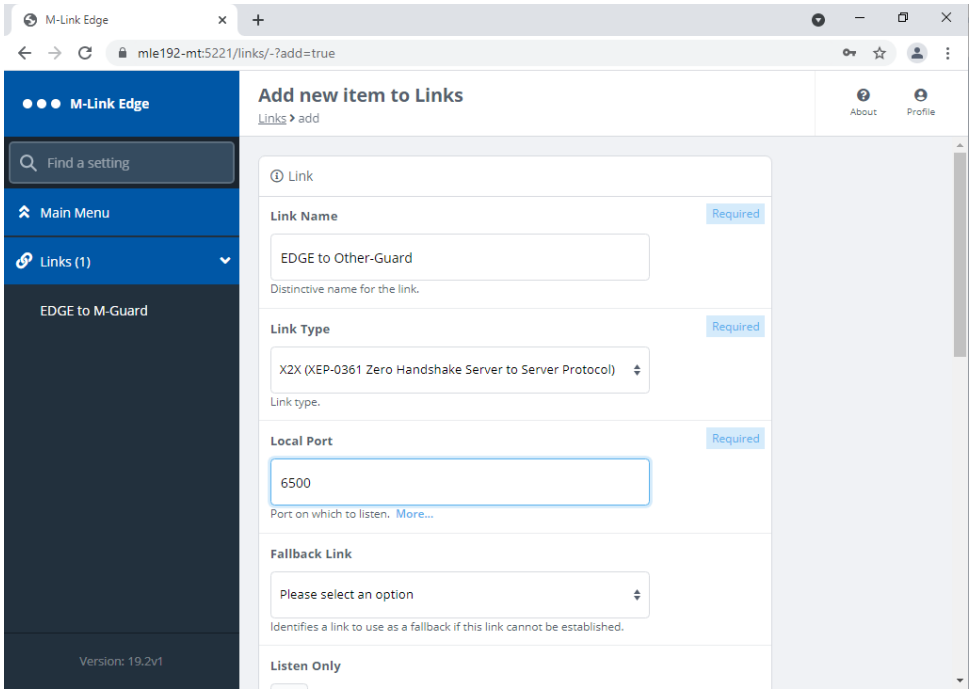

Figure 70: Configuring the XEP-0361 Zero Handshake Server to Server Protocol Link Step 4.

Scroll Down.

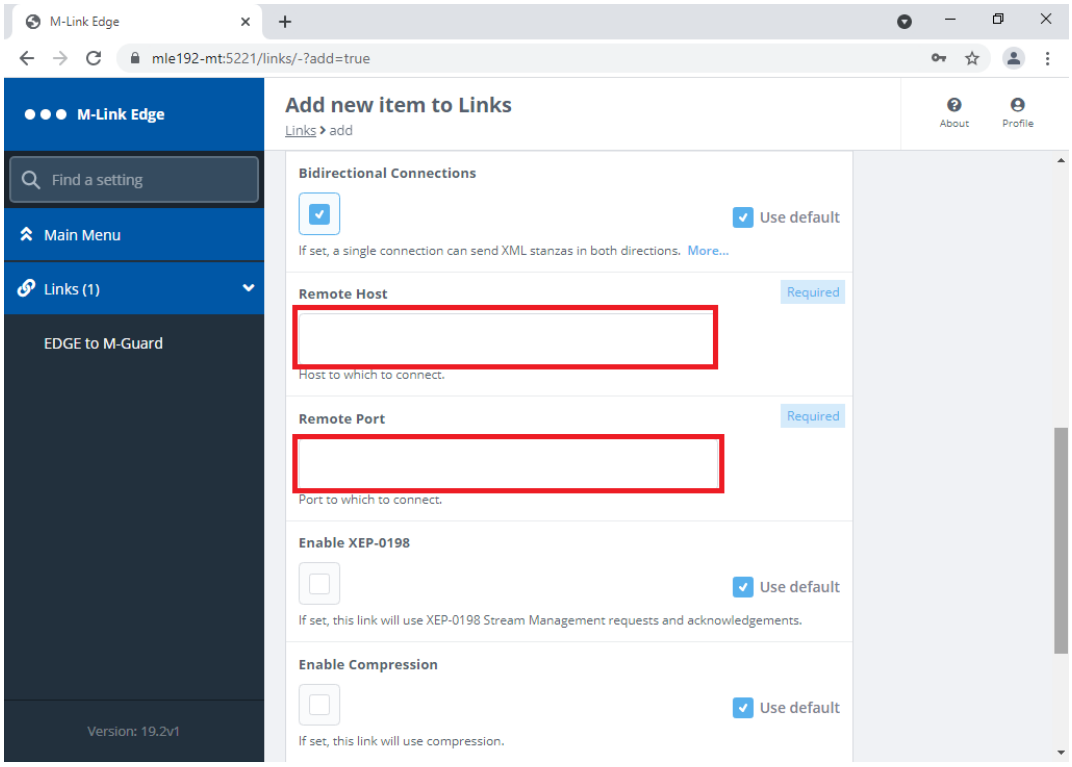

Figure 71: Configuring the XEP-0361 Zero Handshake Server to Server Protocol Link Step 5.

Enter the "Remote Host" IP or Hostname and "Remote Port".

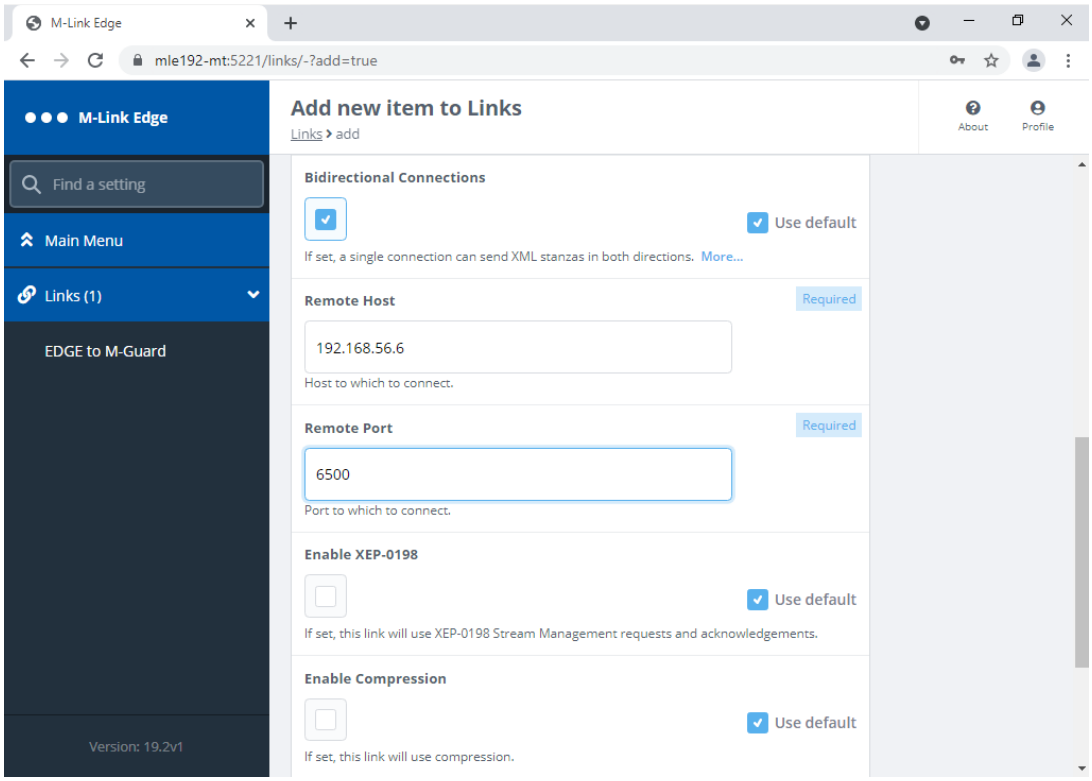

Figure 72: Configuring the XEP-0361 Zero Handshake Server to Server Protocol Link Step 6.

Scroll down.

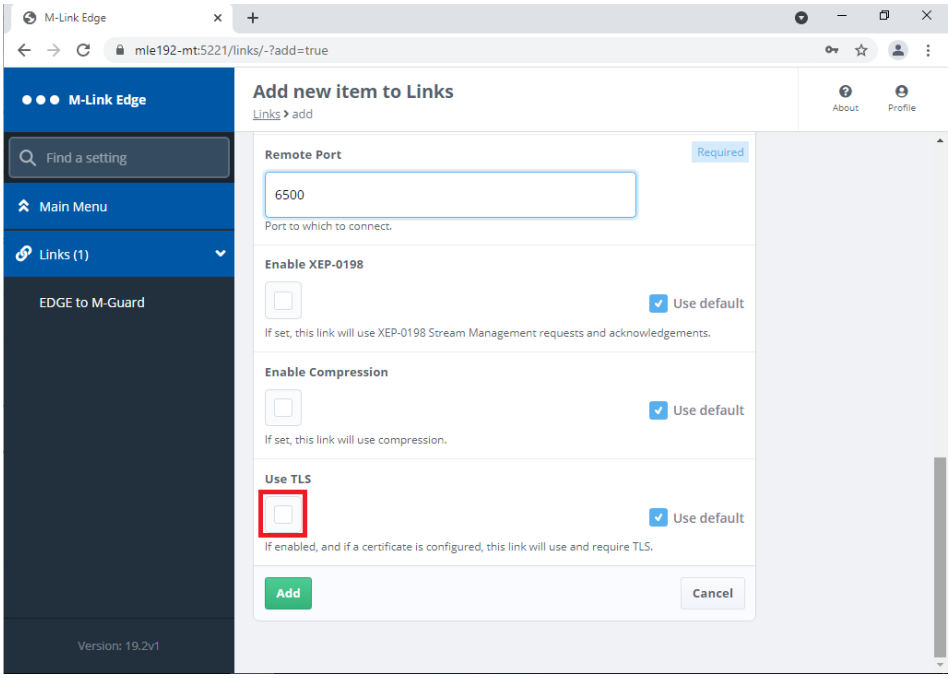

Figure 73: Configuring the XEP-0361 Zero Handshake Server to Server Protocol Link Step 7.

If you are using TLS Check the "Use TLS" Checkbox otherwise Click "Add" and skip to the end of the Link Configuration Screens. We will continue with "Use TLS" Checked.

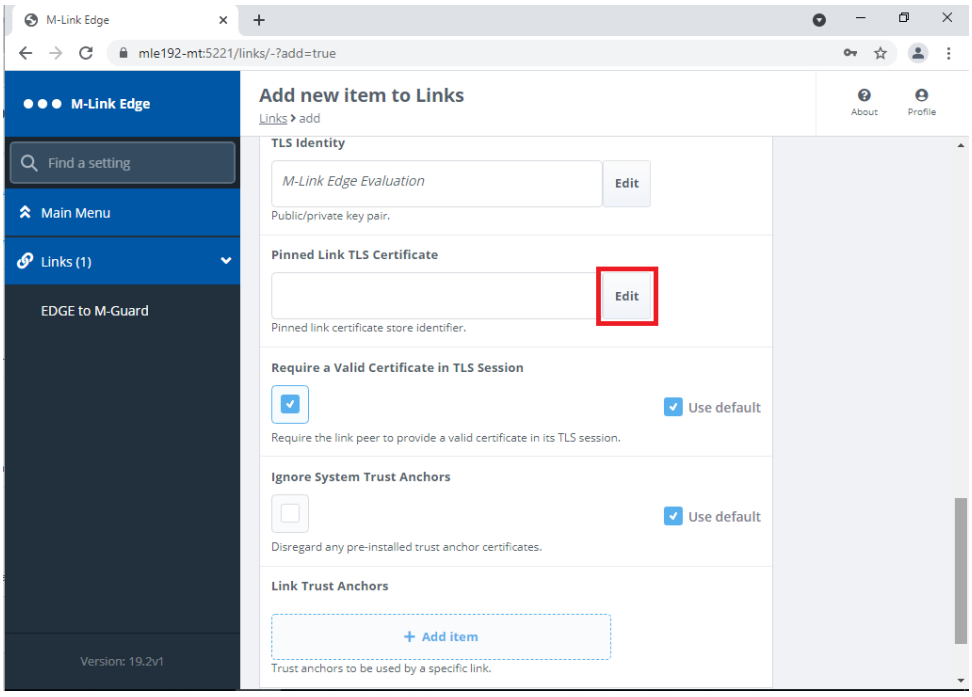

Figure 74: Configuring the XEP-0361 Zero Handshake Server to Server Protocol Link Step 8.

Unless you want to use a different TLS Identity for different Links and have configured other TLS Identities then leave the TLS Identity as it is. Click "Edit" on the "Pinned TLS Certificate.

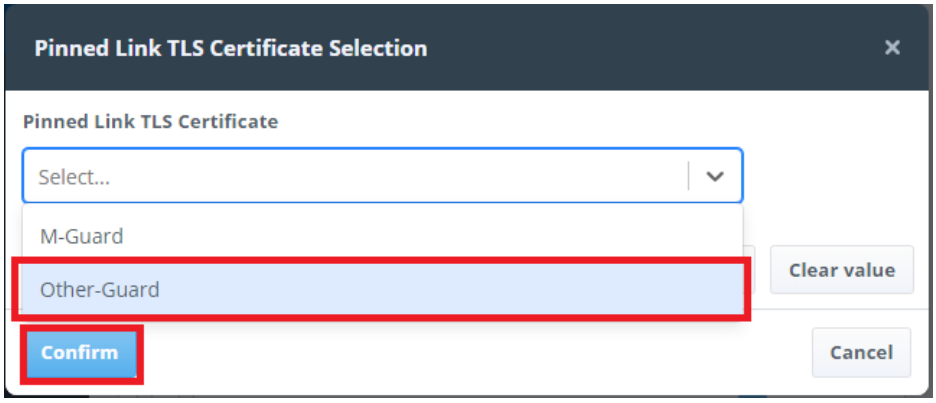

Figure 75: Configuring the XEP-0361 Zero Handshake Server to Server Protocol Link Step 9.

Select the TLS Certificate you have previously loaded for your remote server and Click "Confirm".

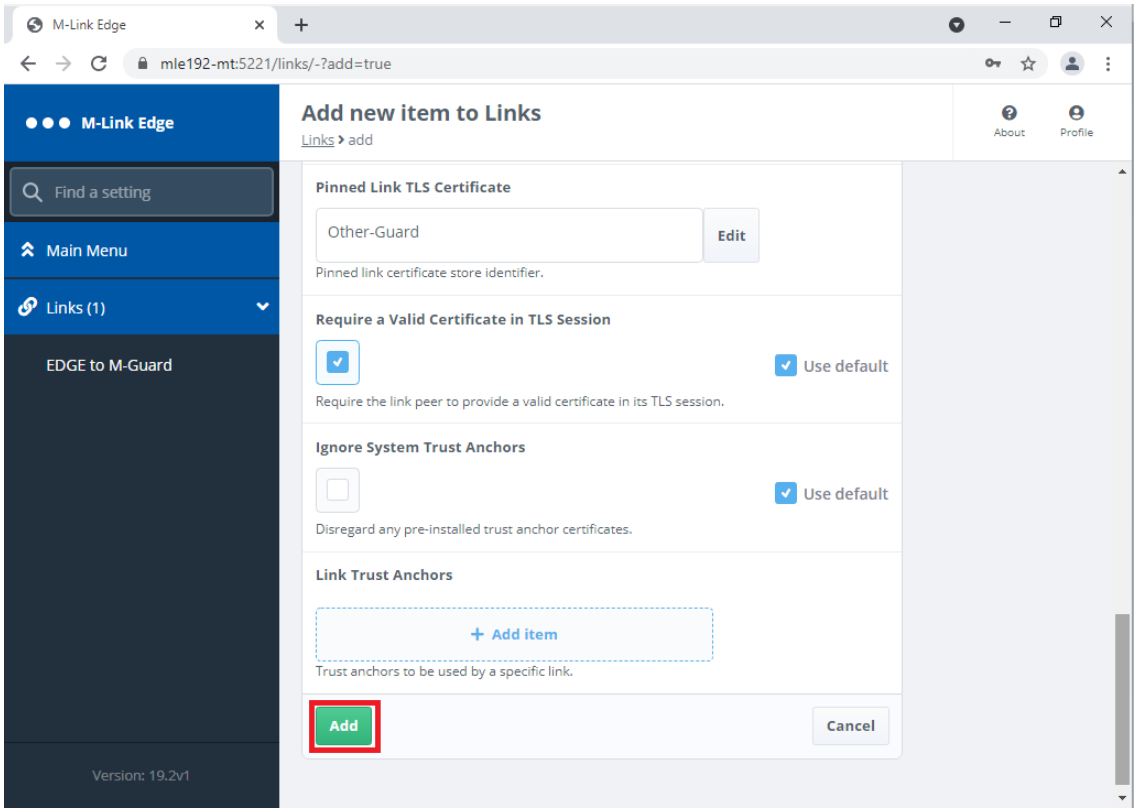

Figure 76: Configuring the XEP-0361 Zero Handshake Server to Server Protocol Link Step 10.

No "Link Trust Anchors" are required as the Trust Anchor is included in the Certificate Chain previously imported.

Click "Add".

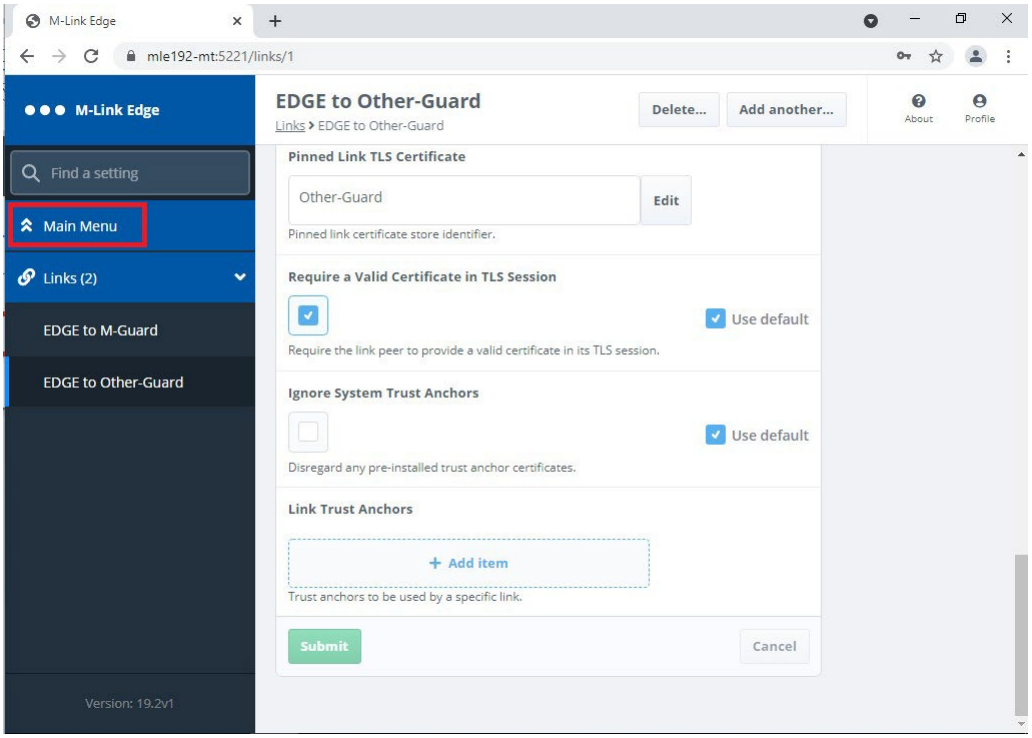

Figure 77: Configuring the XEP-0361 Zero Handshake Server to Server Protocol Link Complete.

The configuration of the XEP-0361 Zero Handshake Server to Server Protocol Link is now complete and we can proceed to add it to a Peer Control Configuration. Click "Main Menu".

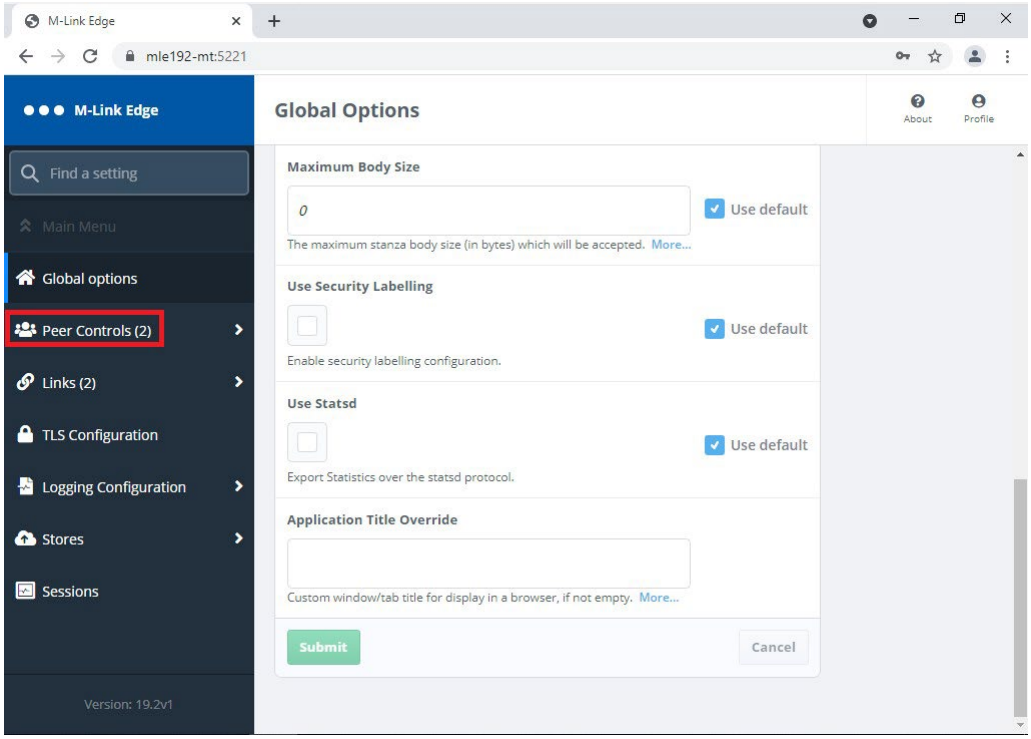

Figure 78: Configuring the Peer Control with an X2X Link Step 1.

Click "Peer Controls".

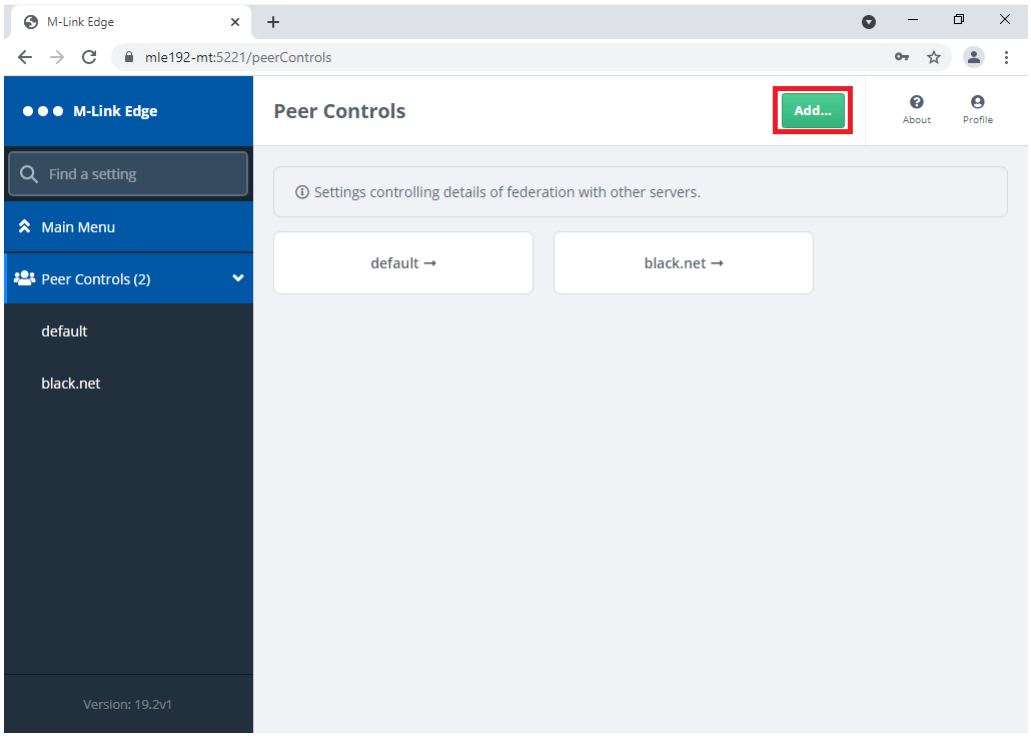

Figure 79: Configuring the Peer Control with an X2X Link Step 2.

Click "Add…"

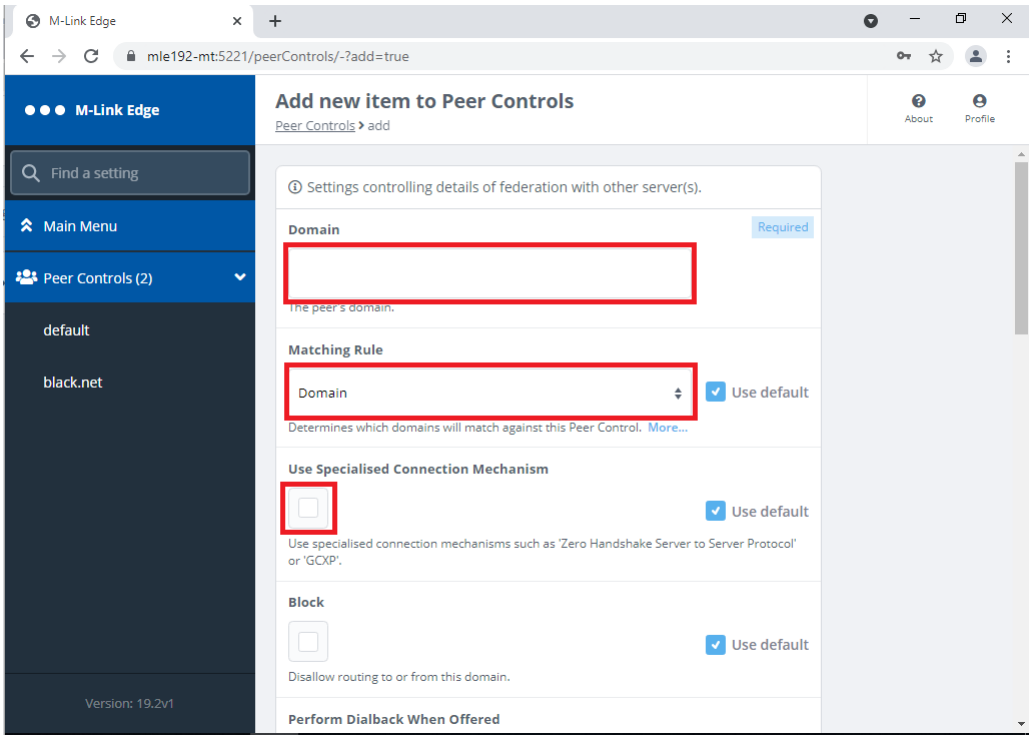

Figure 80: Configuring the Peer Control with an X2X Link Step 3.

Complete the "Domain", "Matching Rule" and Check the "Use Specialised Connection Mechanism" Checkbox.

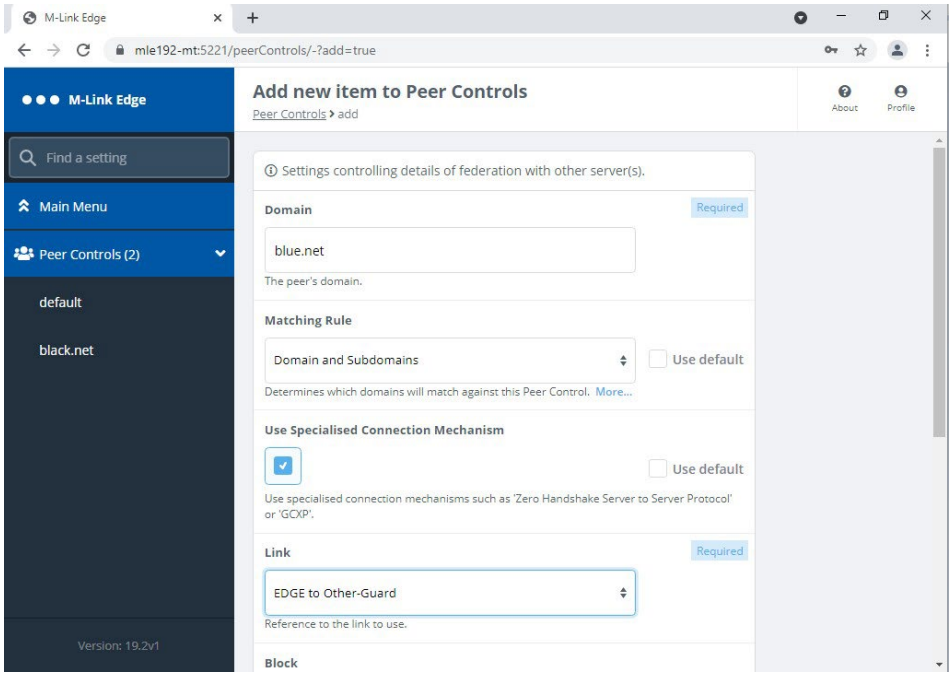

Figure 81: Configuring the Peer Control with an X2X Link Step 4.

The "Domain" should be the XMPP Domain of the Server you are connecting to.
The "Matching Rule" should be "Domain and Subdomain" if you want to include both the 1 to 1 Domain and Multi User Chat (MUC) Domain. You should then select the "Link" you have just created from the drop down and then scroll down.

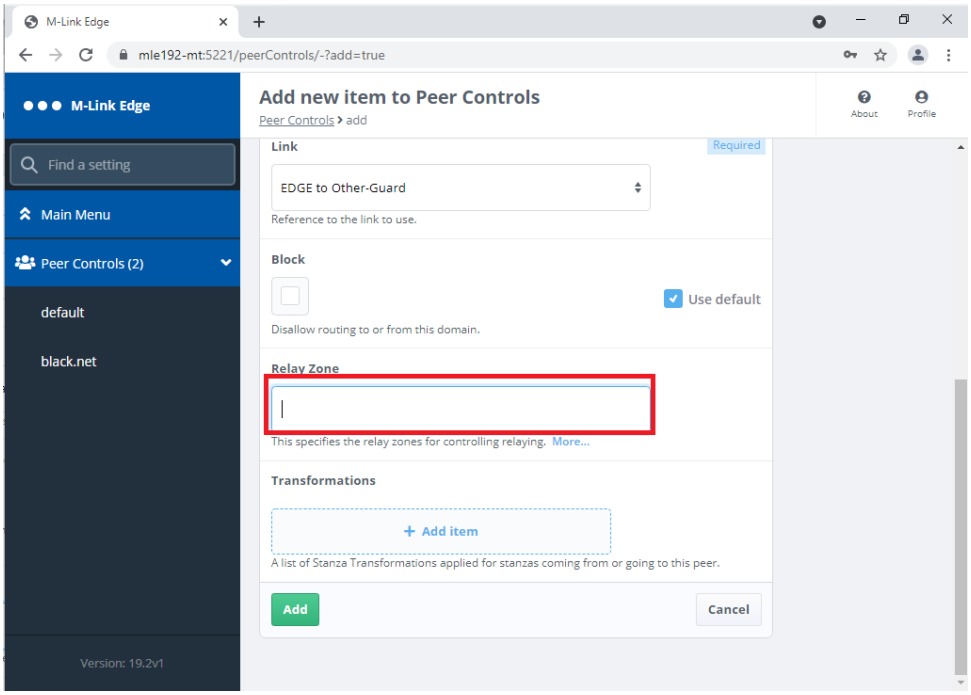

Figure 82: Configuring the Peer Control with an X2X Link Step 5.

The M-Link EDGE Server as it has no domain of it's own it typically relays between different XMPP Domains. In order to do this each link needs a unique "Relay Zone" defined. This is a free text name, so should be something to remind you of where you are relaying between.

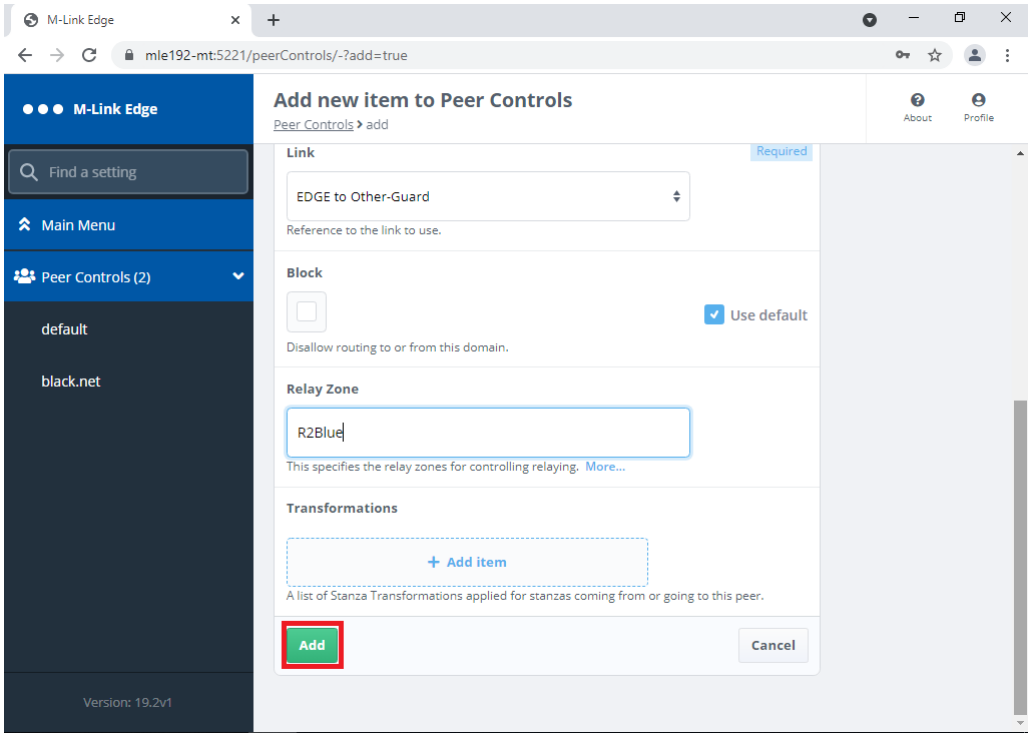

Figure 83: Configuring the Peer Control with an X2X Link Step 6.

Enter your "Relay Zone" name and Click "Add".

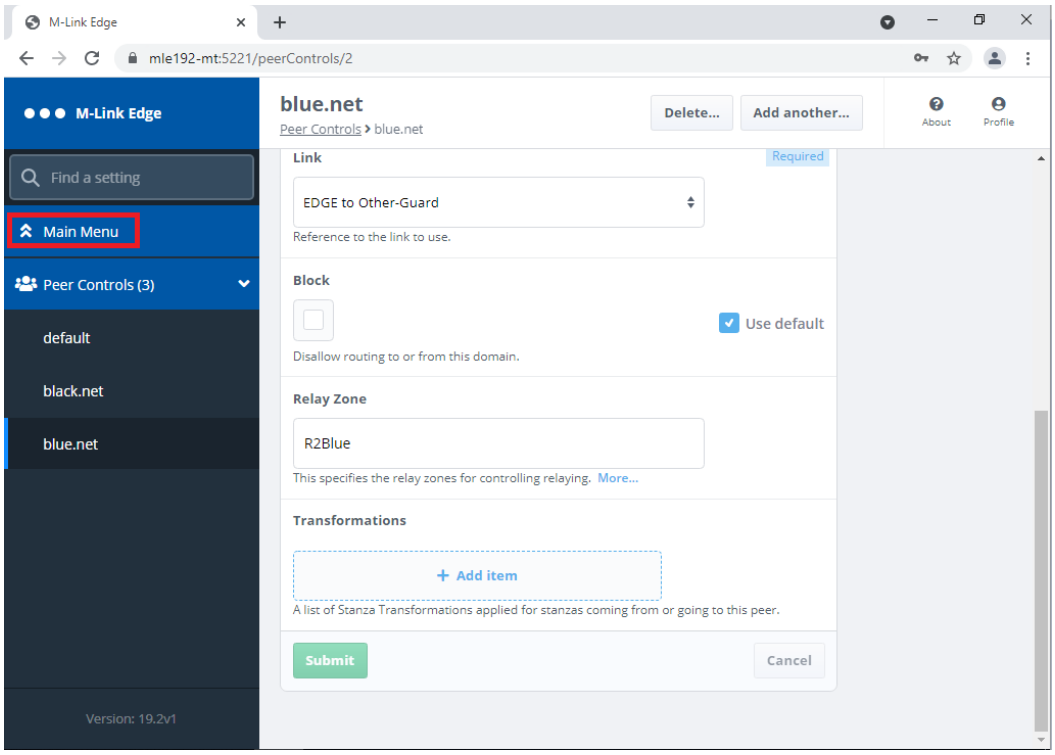

Figure 84: Configuring the Peer Control with an X2X Link Complete.

You have now completed configuring the XEP-0361 Zero Handshake Server to Server Protocol Link (X2) Link and associated Peer Control. Click "Main Menu" and we will configure an XMPP Server to Server Peer Control.

Configuring a XMPP Server to Server Peer Control

A XMPP Server to Server Peer Control is typically used to connect the M-Link EDGE Server to an XMPP User Server e.g. M-Link R17.0.

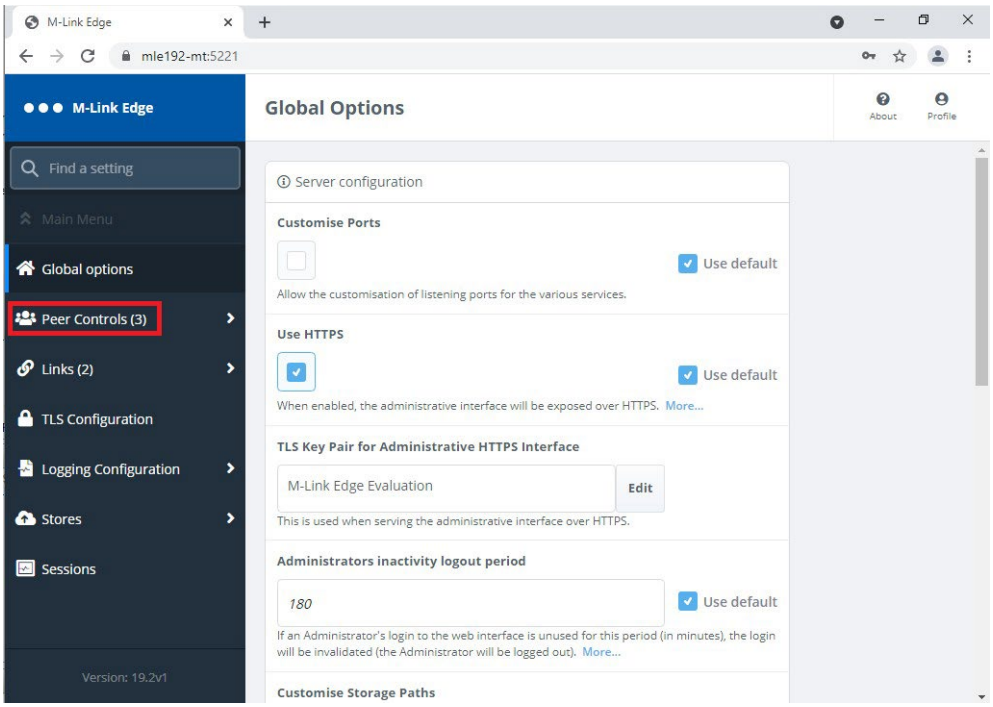

Figure 85: Configuring the XMPP Server to Server Peer Control Step 1.

Click "Peer Controls"

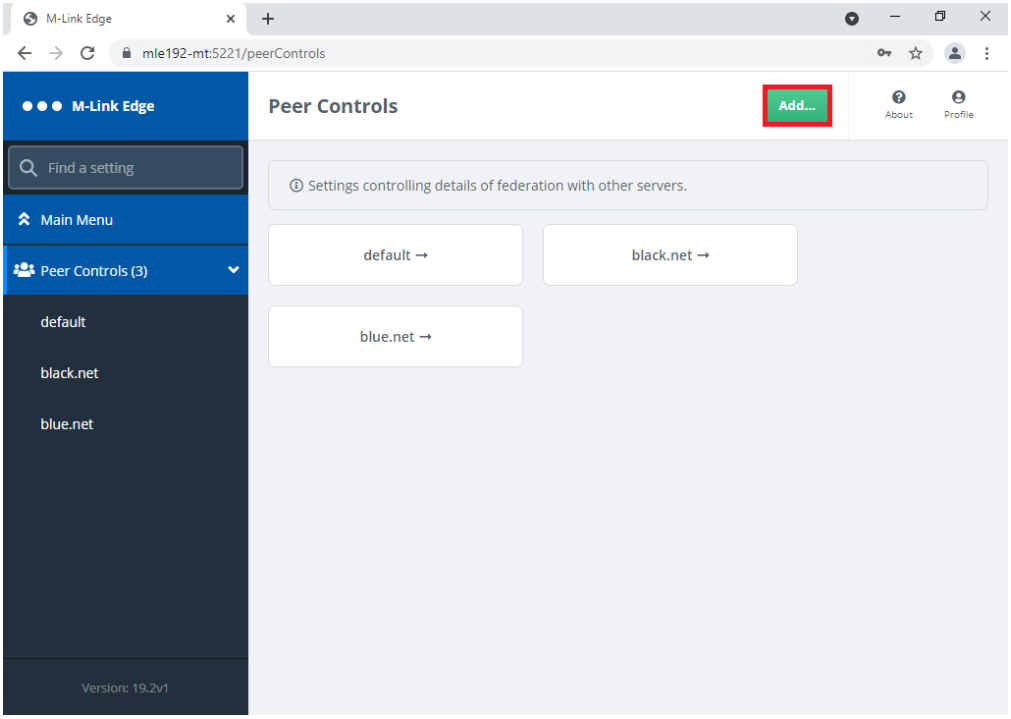

Figure 86: Configuring the XMPP Server to Server Peer Control Step 2.

Click "Add…"

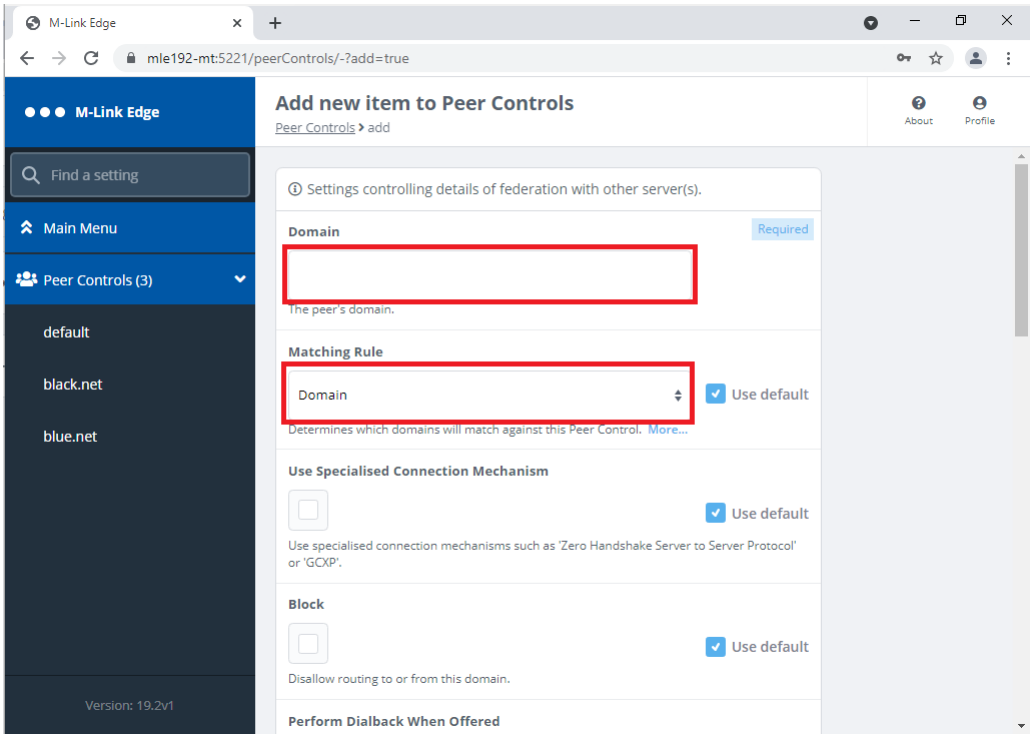

Figure 87: Configuring the XMPP Server to Server Peer Control Step 3.

Complete the "Domain" and "Matching Rule".

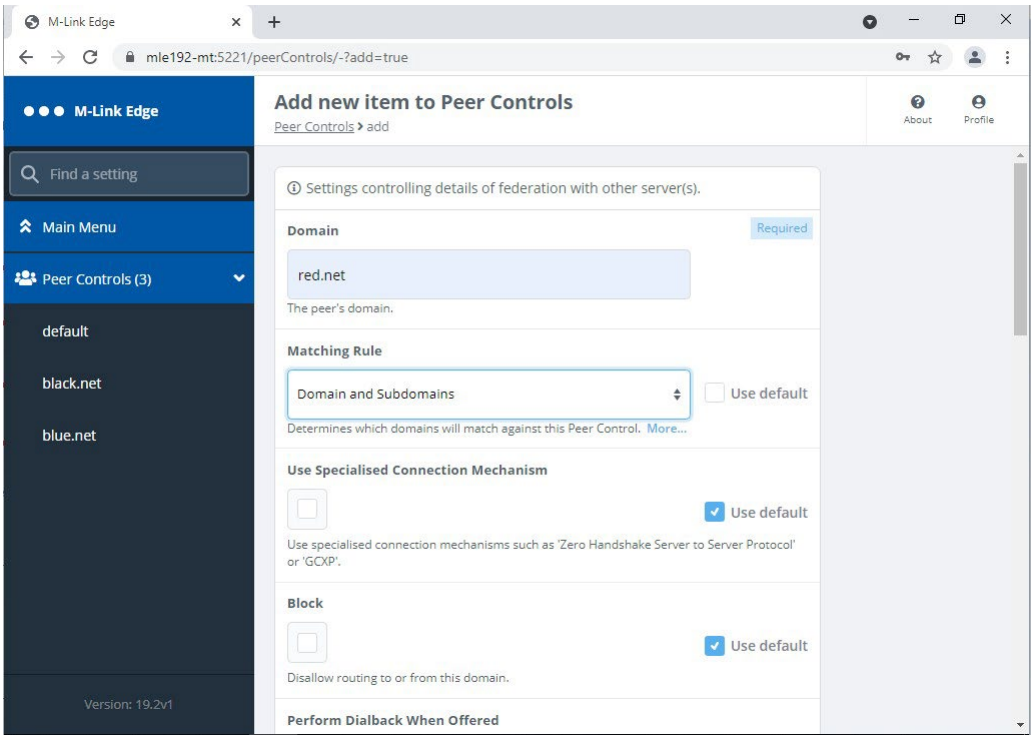

Figure 88: Configuring the XMPP Server to Server Peer Control Step 4.

The "Domain" should be the XMPP Domain of the Server you are connecting to.
The "Matching Rule" should be "Domain and Subdomain" if you want to include both the 1 to 1 Domain and Multi User Chat (MUC) Domain. Scroll down.

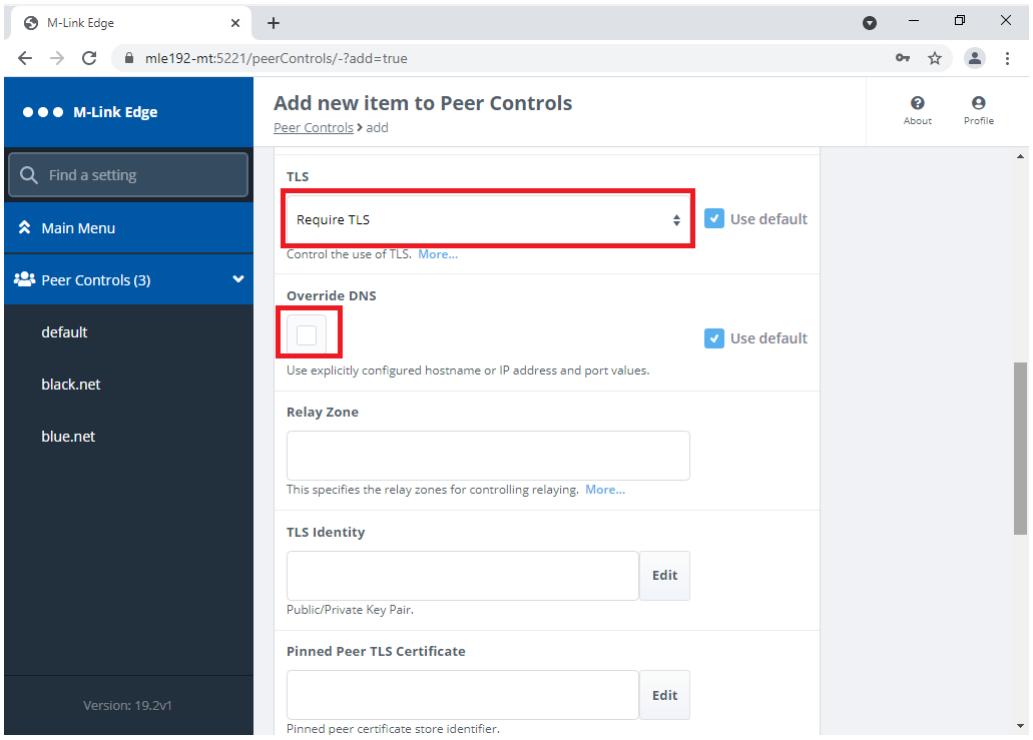

Figure 89: Configuring the XMPP Server to Server Peer Control Step 5.

There are various TLS Options from "Do not use TLS" to "Require Authenticated TLS", choose the option that best suits you. In this guide we will use the default "Require TLS". If the Remote XMPP Server does not have any DNS XMPP SRV Records then you can manually configure this using the "Override DNS" Checkbox and we will do this in this example.

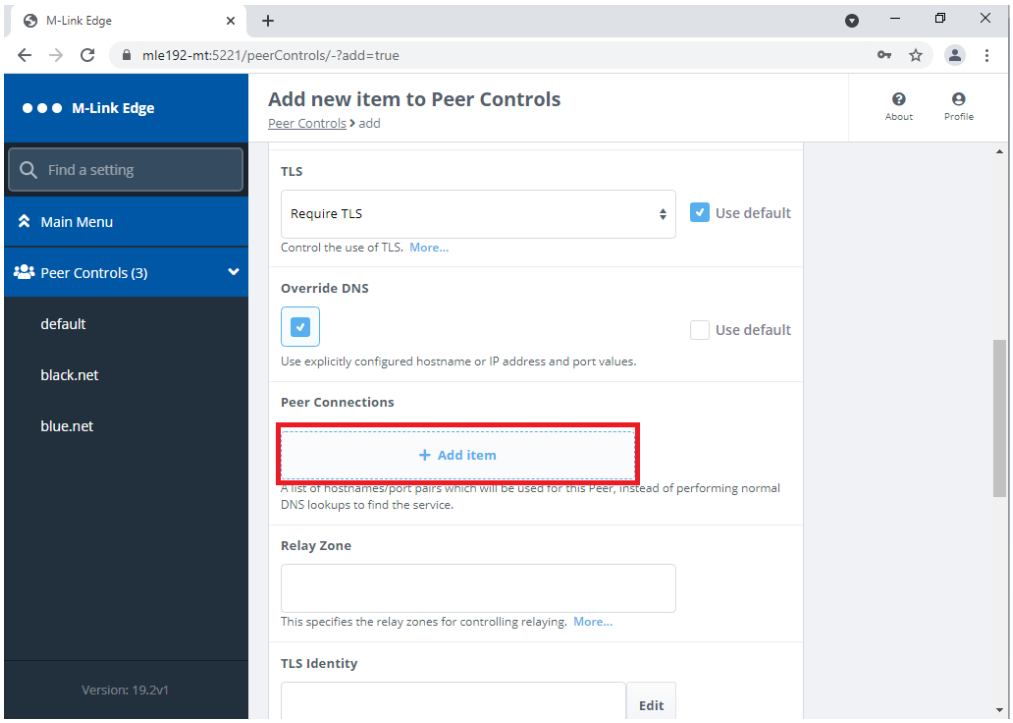

Figure 90: Configuring the XMPP Server to Server Peer Control Step 6.

Click "+ Add item" on the Peer Connections.

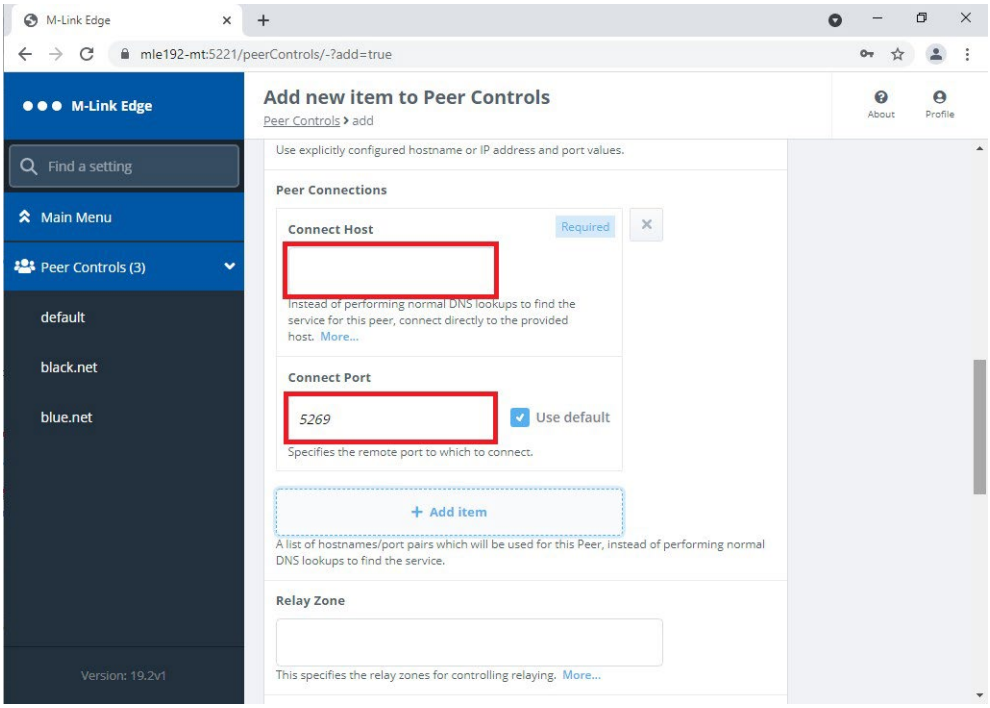

Figure 91: Configuring the XMPP Server to Server Peer Control Step 7.

Enter the IP Address of the Remote XMPP Server and Change the Port if it is not default.

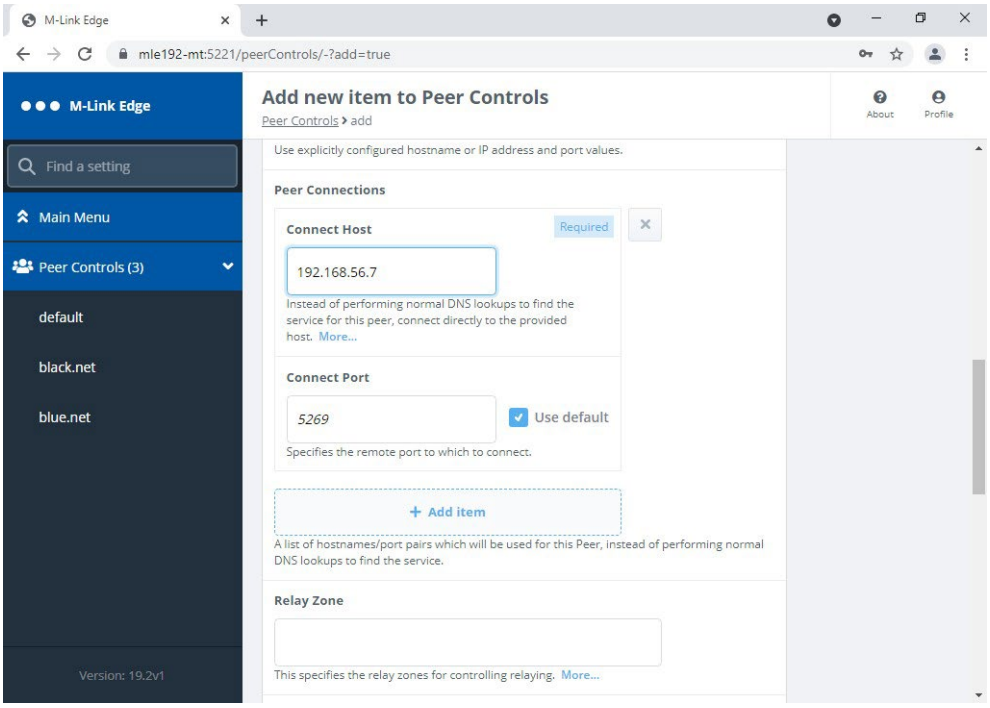

Figure 92: Configuring the XMPP Server to Server Peer Control Step 8.

If there are Multiple XMPP Servers supporting this domain e.g. in a M-Link User Server Cluster then repeat the previous two steps. Otherwise Scroll Down.

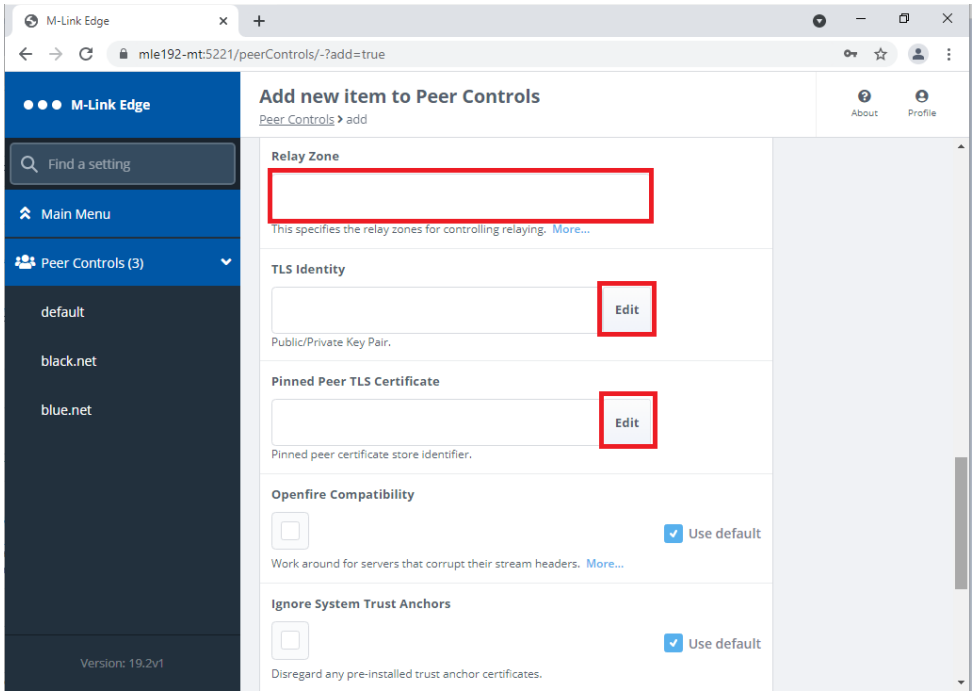

Figure 93: Configuring the XMPP Server to Server Peer Control Step 9.

The M-Link EDGE Server as it has no domain of it's own it typically relays between different XMPP Domains. In order to do this each link needs a unique "Relay Zone" defined. This is a free text name, so should be something to remind you of where you are relaying between. As we are using TLS we will need to configure the "TLS Identity" for the Link and also the "Pinned Peer TLS Certificate" using the "Edit" Buttons.

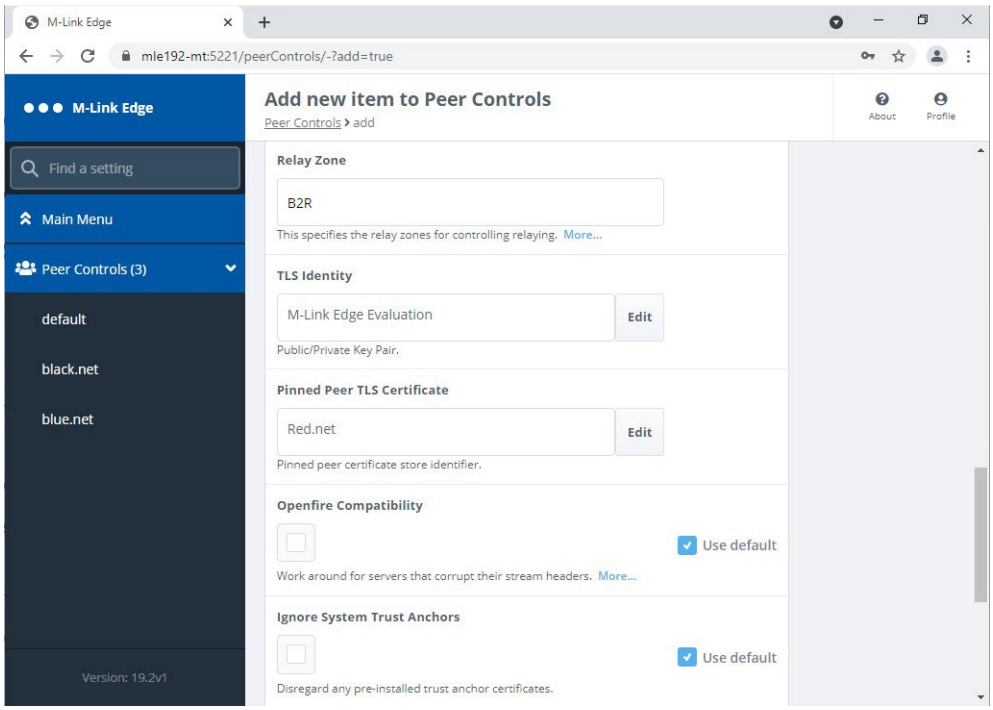

Figure 94: Configuring the XMPP Server to Server Peer Control Step 10.

The "TLS Identity and" "Pinned Peer TLS Certificate" will be selected from a dropdown of previously configured Identities/Certificates.

Scroll down.

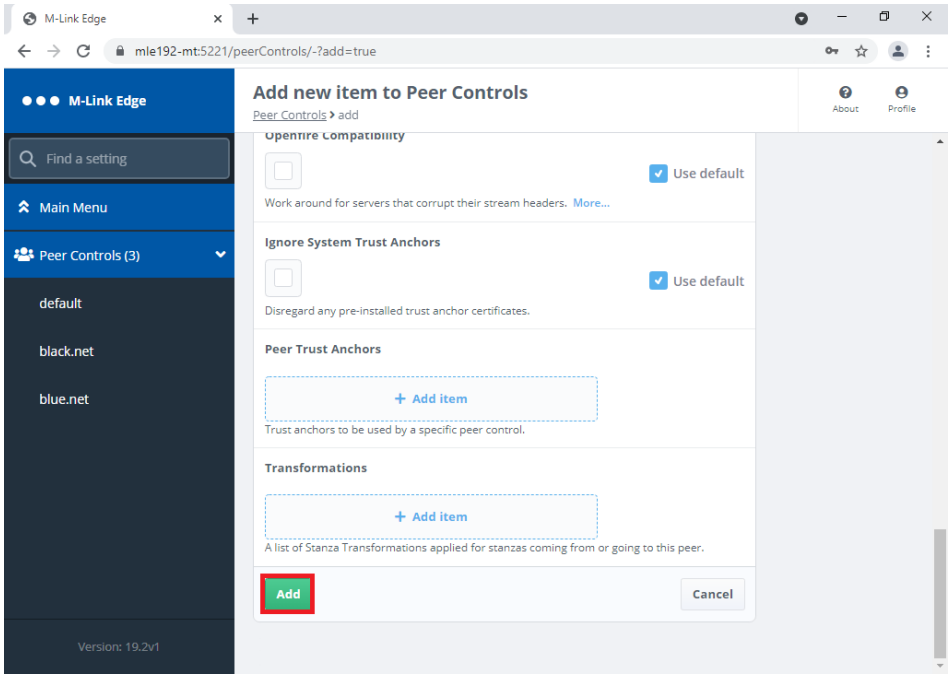

Figure 95: Configuring the XMPP Server to Server Peer Control Step 11.

There are no "Peer Trust Anchors" to configure as they are included in the Certificate Chain previously loaded.

Click "Add".

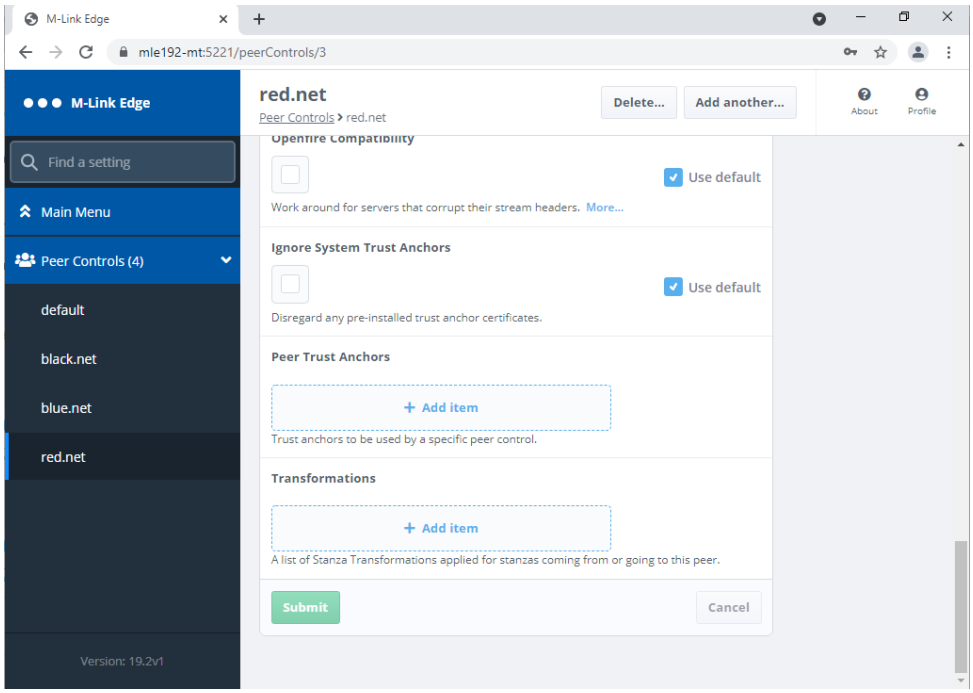

Figure 96: Configuring the XMPP Server to Server Peer Control Complete.

You have now completed configuring the XMPP Server to Server Peer Control.

You have also reached the end of this Guide. Further Advanced Configuration Options can be found in the M-Link R19.3 User Manual or by contacting support@isode.com .

Other Evaluations

This guide is one 5 relating to Isode's XMPP Messaging Products, the other guides are:

- Setting up an XMPP System for 1:1 and Multi-User Chat
- Connecting XMPP and IRC Chat Services
- XMPP for Constrained Network Environments

Information on all of these evaluations can be found at *www.isode.com/evaluate/evaluate-xmpp.html* . For messaging evaluations outside the scope of these guides, please contact us.

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