

M-Guard Evaluation Guide

Installing and configuring R1.5.4 M-Guard Appliance and R1.5.5 M-Guard Console of Isode's M-Guard XML Guard on Windows Hyper-V (Appliance) and Windows Desktop Operating System (Console).

Contents

Introduction.....	3
Objectives	3
Using Isode Support.....	4
Preparing the Environment.....	5
Network Overview	5
Obtain the Isode Software and Java	5
Configure the Hyper-V Networks.....	7
Importing the M-Guard Appliance	12
Configuring and Starting the M-Guard Appliance.....	17
Configuring and the Guard with M-Guard Console.....	22
Prepare to Add an M-Guard Instance.....	38
Configuring a new M-Guard Instance	41
Setup up the GCXP Producer and Consumer Certificates	50
Configure GCXP Producer and Consumer	56
Send messages between GCXP Producer and Consumer	62
What Next?	69
Whitepapers	69
Copyright	70

Introduction

This guide is intended to give the reader basic information on how to install and configure Isode's M-Guard Product. M-Guard is an XML Guard and comprises two components M-Guard Appliance (the Guard itself) and M-Guard Console (the GUI Configuration tool). The M-Guard Appliance can support multiple Guard instances.

The M-Guard Appliance can be installed as a Hyper-V virtual machine, an Oracle Virtual Box Virtual Machine or on our recommended hardware appliance the Netgate 6100. Once the Appliance is installed and M-Guard Console is connected then the configuration process is the same for all options. This guide will install on Windows Hyper-V. There will be a separate guide for how to install on Virtual Box. For installation on a Netgate 6100 please contact Isode Support using the email address isode.support@isode.com.

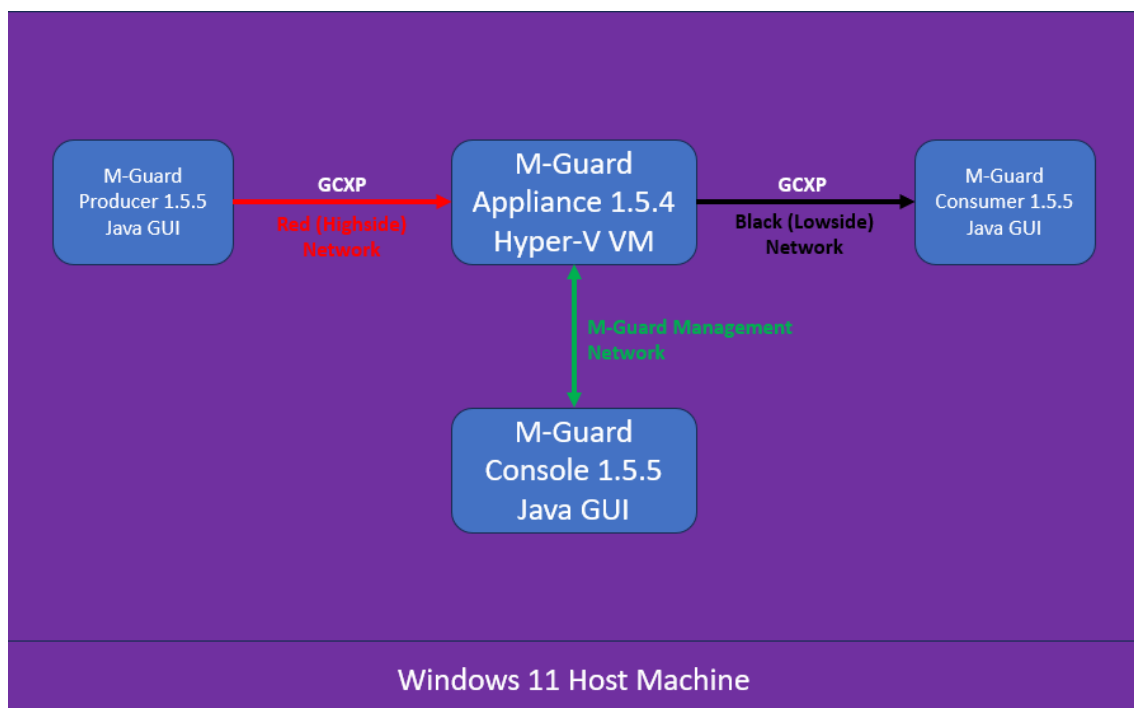
More information on M-Guard can be found at www.isode.com/product/xml-guard/

Objectives

In this guide you will be shown how to install the M-Guard Appliance on Windows Hyper-v and configure it using M-Guard Console. You will finish by creating a single XML Guard Instance that you will test using Isode's M-Guard GCXP Consumer and M-Guard GCXP Producer tools. The host operating system in the instance is Windows 11. You will need three separate networks; a Red Network, a Black Network and a M-Guard Management Network. In this evaluation all these Networks will be Hyper-V "Internal Networks".

The diagram below gives an overview of this setup.

System Overview



By the end of this guide, you will have:

1. Installed the M-Guard Appliance Hyper-V Virtual Machine
2. Installed the M-Guard Console software.
3. Connected M-Guard Console to the M-Guard Appliance.
4. Configured a single XML Guard instance on the M-Guard Appliance using M-Guard Console.
5. Created some basic rules.
6. Tested the above rules using the M-Guard GCXP Producer and Consumer tools.

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.

Preparing the Environment

Network Overview

As noted, you will need to create three separate Hyper-V Internal Networks. For the purposes of this evaluation, we will use this Network Architecture.

Hyper-V Internal Network	Red Network	M-Guard Management	Black Network
Host Machine IP	192.168.56.1	10.178.0.1	192.168.106.1
M-Guard IP	192.168.56.2	10.178.0.2	192.168.106.2
Netmask	255.255.255.0	255.255.255.0	255.255.255.0

Obtain the Isode Software and Java

You will need to obtain the following from Isode Support.

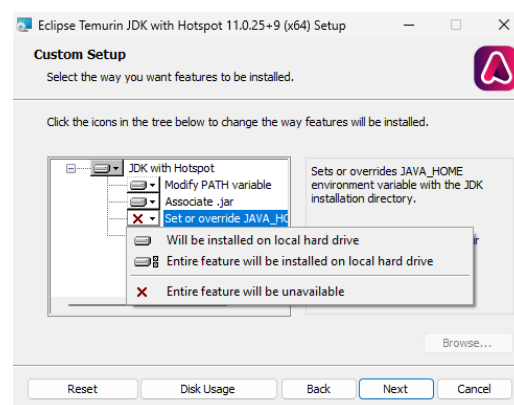
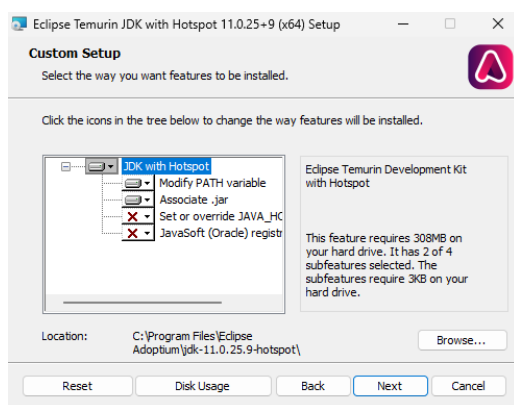
- | | |
|------------------------------------|--|
| M-Guard Appliance | M-Guard-1.5.4-hyper-full.zip |
| M-Guard Console | M-Guard-Console-1.5.5.jar |
| M-Guard Console Signature | M-Guard-Console-1.5.5.jar.sig |
| M-Guard Console Profiles | M-Guard-Console-1.5.5-Profiles.jar |
| M-Guard Console Profiles Signature | M-Guard-Console-1.5.5-Profiles.jar.sig |

M-Guard Console requires OpenJDK 11 to be installed, this can be obtained from the Adoptium Temurin website:

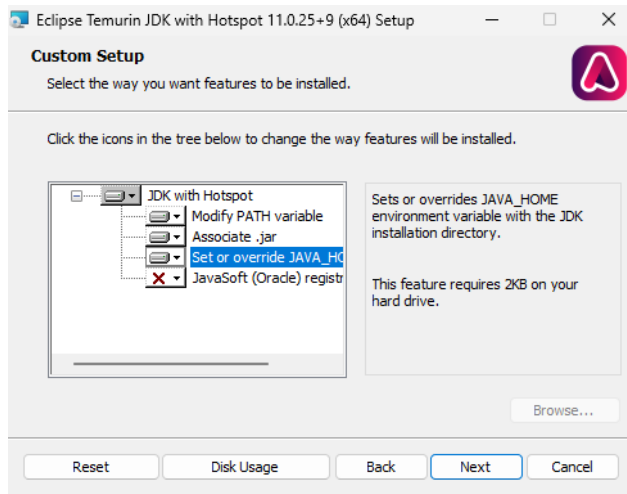
<https://adoptium.net/en-GB/temurin/releases/?os=windows&arch=x64&package=jdk&version=11>

Note that when installing Java you should set the JAVA_HOME Variable on Windows this is done during the .msi installation.

Set JAVA_HOME



Set JAVA_HOME



You may well need to reboot your Windows 11 Machine for this to take effect. You can test it by running the command `java -version` in a Windows Command Prompt.

Test JAVA_HOME

```
Command Prompt
Microsoft Windows [Version 10.0.26100.2605]
(c) Microsoft Corporation. All rights reserved.

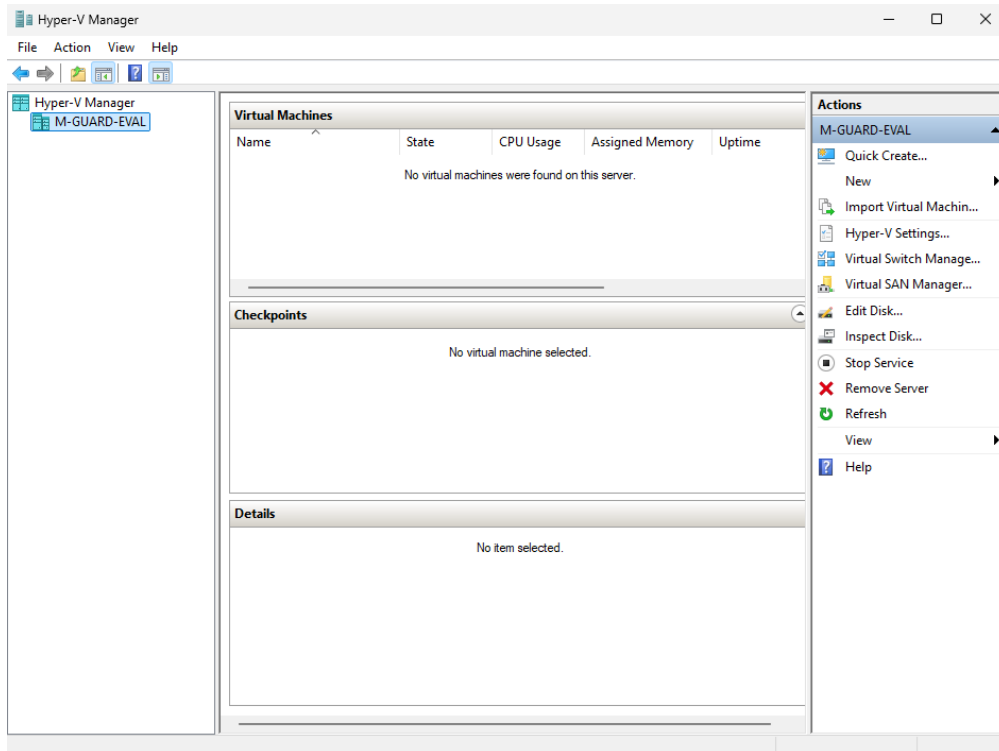
C:\Users\markt>java -version
openjdk version "11.0.25" 2024-10-15
OpenJDK Runtime Environment Temurin-11.0.25+9 (build 11.0.25+9)
OpenJDK 64-Bit Server VM Temurin-11.0.25+9 (build 11.0.25+9, mixed mode)

C:\Users\markt>
```

Configure the Hyper-V Networks

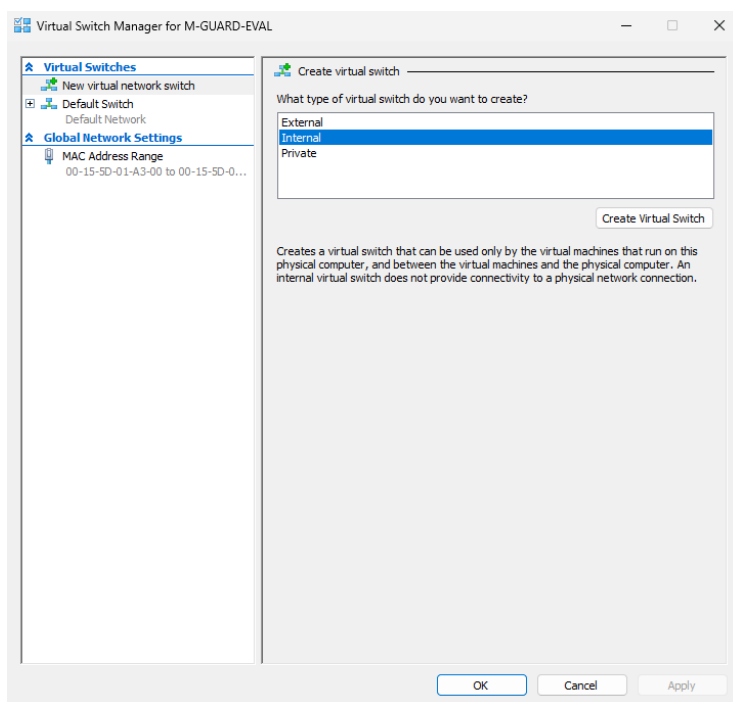
From the Hyper-V Manager.

Hyper-V Manager



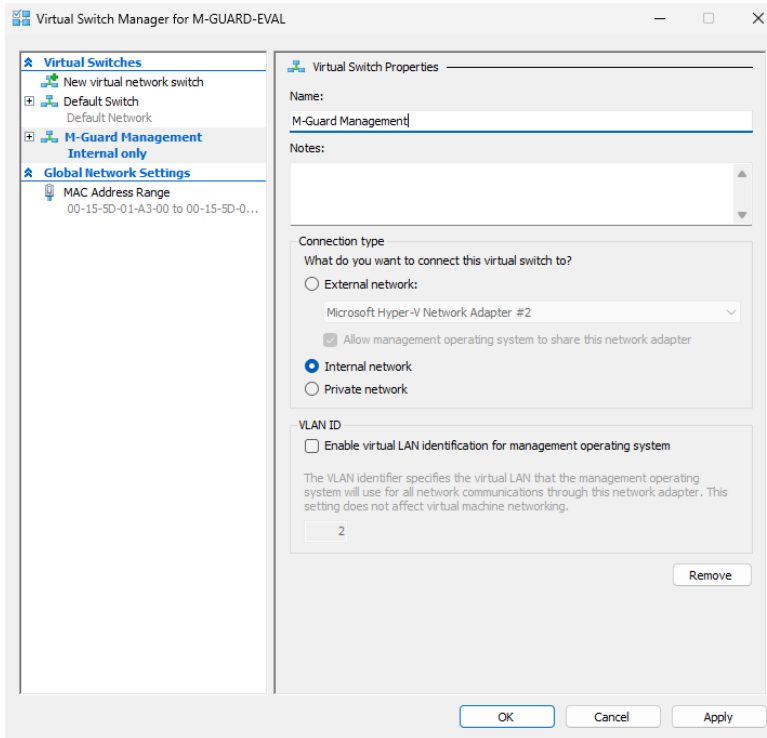
Select “Virtual Switch Manager”

Virtual Switch Manager



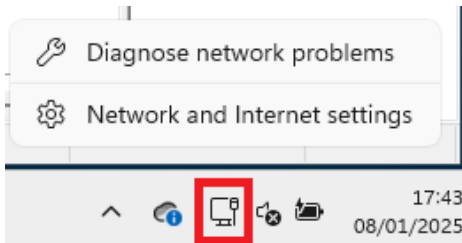
Select “Internal” and Click “Create Virtual Switch”.

Virtual Switch Manager



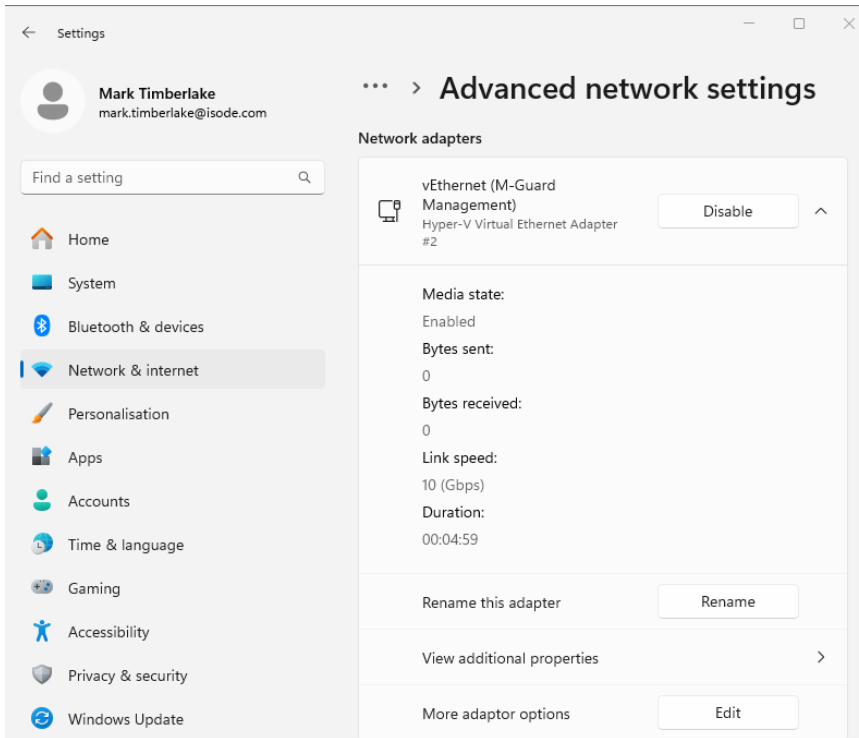
Give it a Name of “M-Guard Management” and Click “Apply” and then Click “OK”.
 Now we need to configure this Network on the host machine.
 Right Click on the Network Icon in the Taskbar.

Host Network



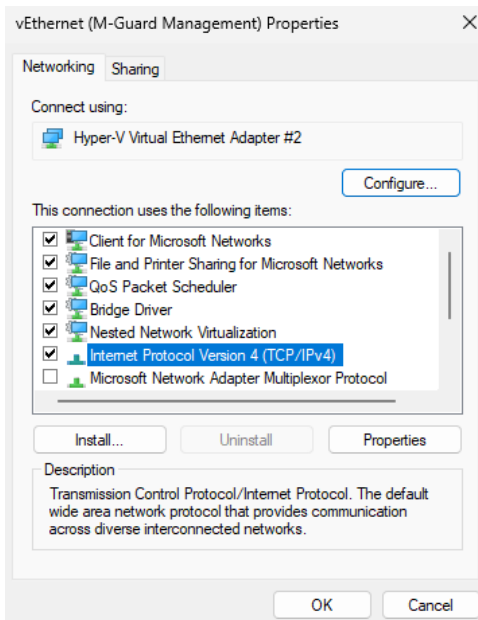
Select “Network and Internet settings”.

Configure Network



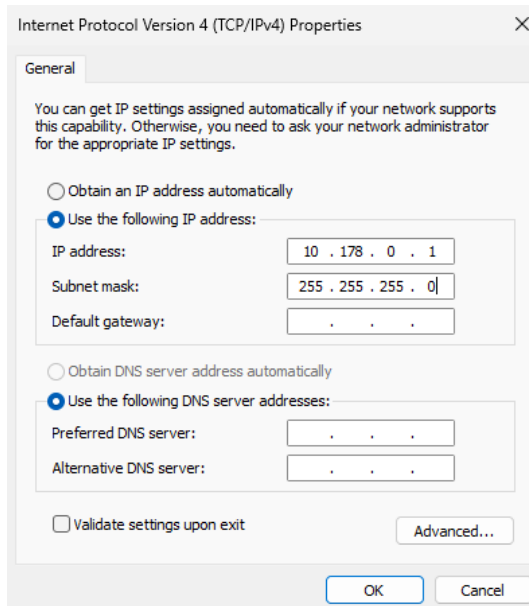
In the “Advanced network settings” for the “M-Guard Management” Adapter Click “Edit”.

Configure Network



Select the “Internet Protocol Version 4 (TCP/IPV4)” and click “Properties”.

Configure Network

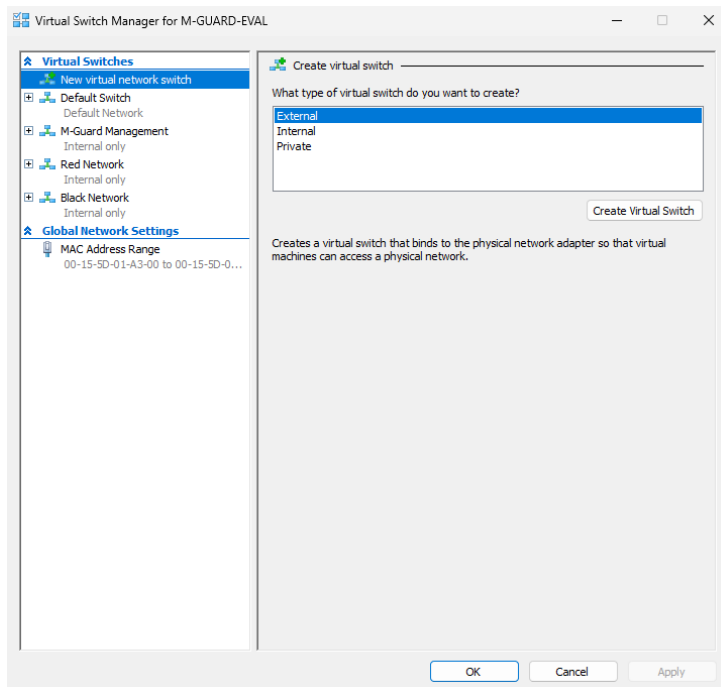


Set the IP Address and Network Mask as per the Network plan earlier and Click “OK”.

Repeat this process for the Red Network and Black Network.

Hyper-V Virtual Switch Manager should now look like this.

Hyper-V Virtual Switch Manager



You can check the IP Addresses using a Windows command prompt and the command ipconfig.

Check Network Addresses

```
Command Prompt
C:\Users\markt>ipconfig

Windows IP Configuration

Ethernet adapter vEthernet (M-Guard Management):

    Connection-specific DNS Suffix . . . :
    Link-local IPv6 Address . . . . . : fe80::1ce5:e619:cbd0:384%33
    IPv4 Address. . . . . : 10.178.0.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter vEthernet (Red Network):

    Connection-specific DNS Suffix . . . :
    Link-local IPv6 Address . . . . . : fe80::d2f:b004:f62c:a8d1%39
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter vEthernet (Black Network):

    Connection-specific DNS Suffix . . . :
    Link-local IPv6 Address . . . . . : fe80::fc2:d452:ac3d:79c%45
    IPv4 Address. . . . . : 192.168.106.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```

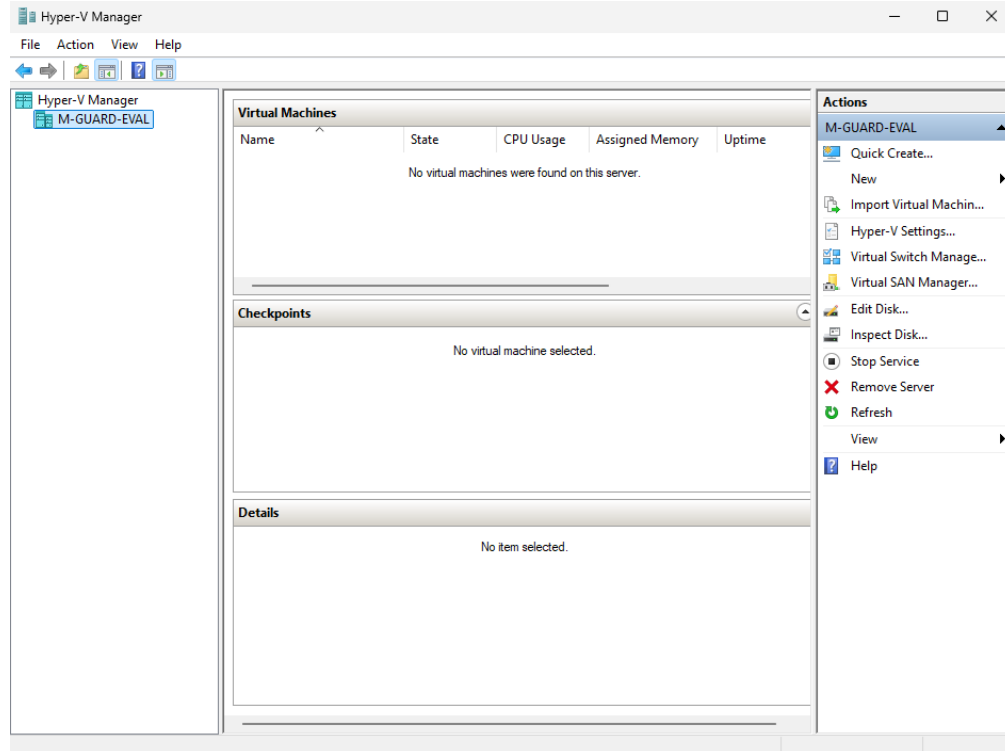
You are now ready to import the M-Guard Appliance Virtual Machine.

Importing the M-Guard Appliance

You will have been provided by Isode Support with a .zip file that contains the M-Guard Appliance. You will need to extract this zip file prior to the following steps and note the location.

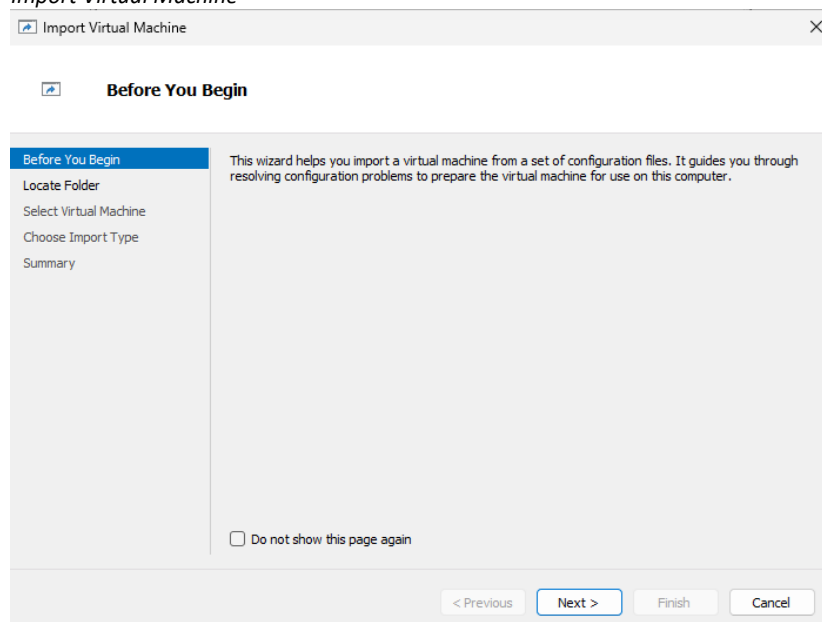
From Hyper-V Manager.

Hyper-V Manager



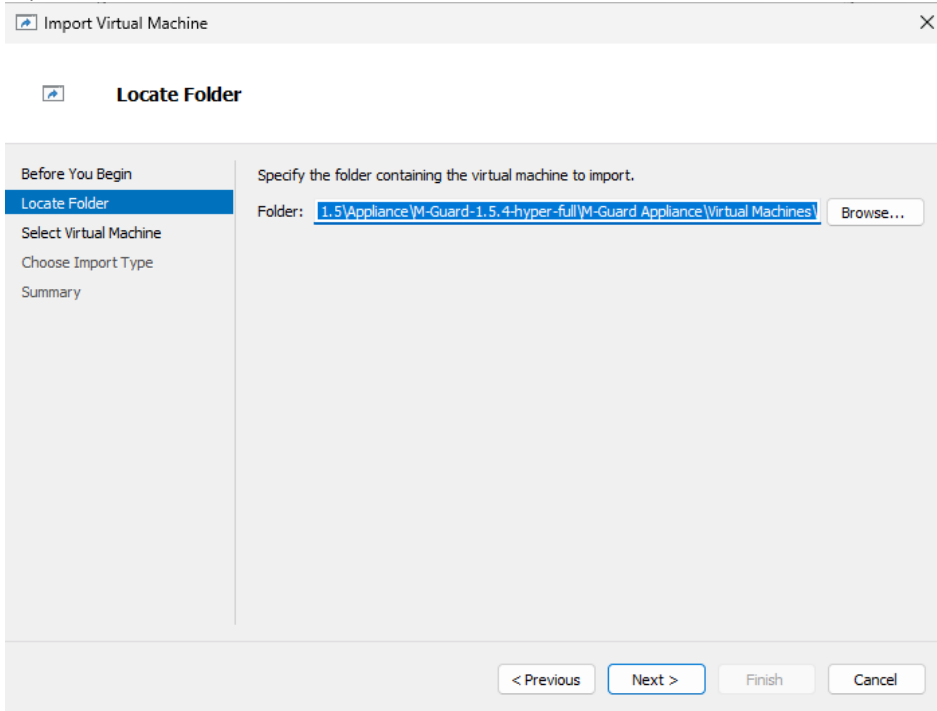
Select Import Virtual Machine.

Import Virtual Machine



Click "Next>"

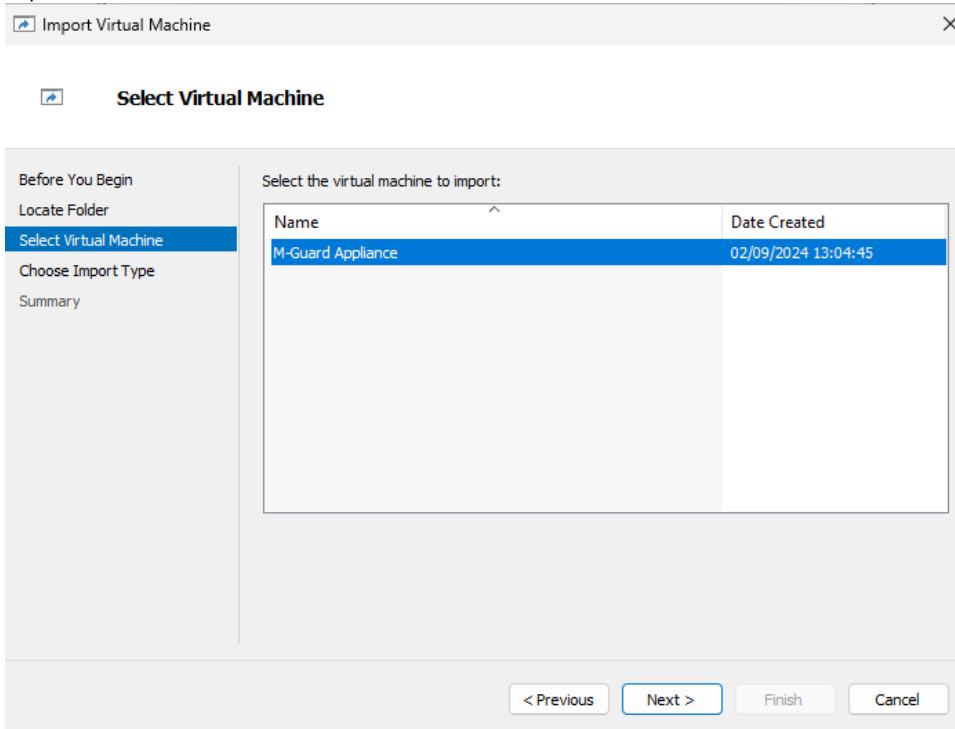
Import Virtual Machine



Browse to the \M-Guard-1.5.4-hyper-full\M-Guard Appliance\Virtual Machines\ folder of the .zip extract.

Click “Next>”

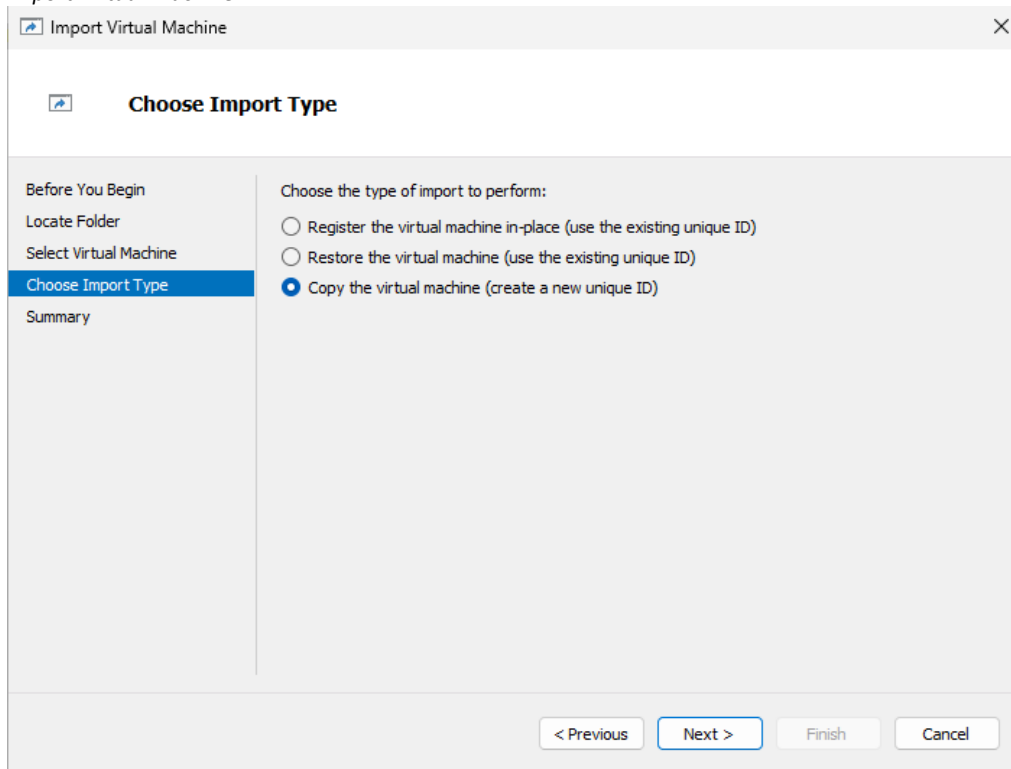
Import Virtual Machine



Select “M-Guard Appliance”.

Click “Next>”

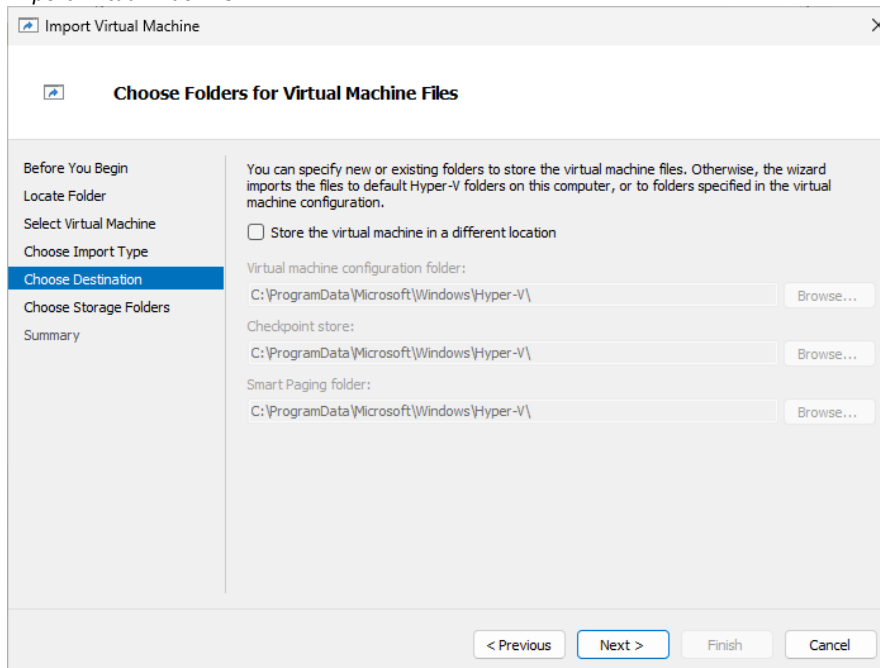
Import Virtual Machine



Select “Copy the virtual machine (create a new unique ID)”

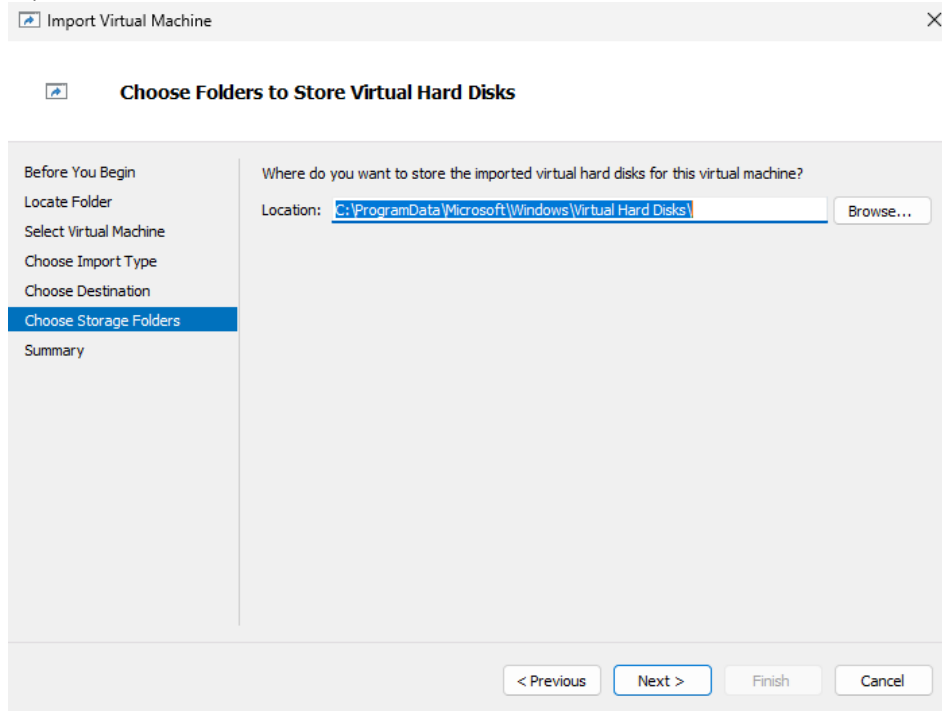
Click “Next>”

Import Virtual Machine



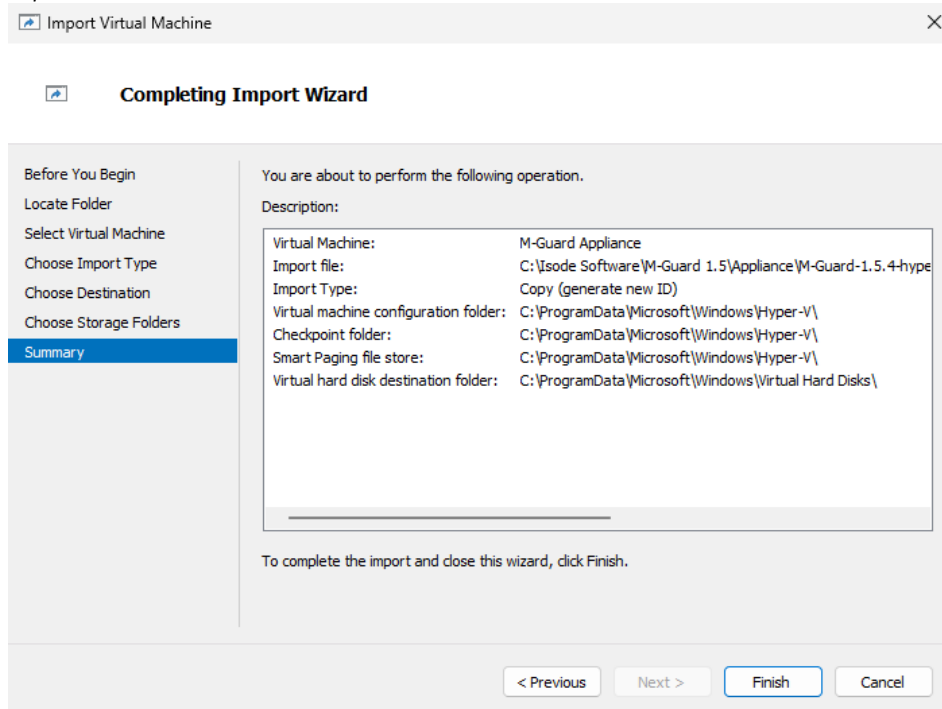
Click “Next>”

Import Virtual Machine



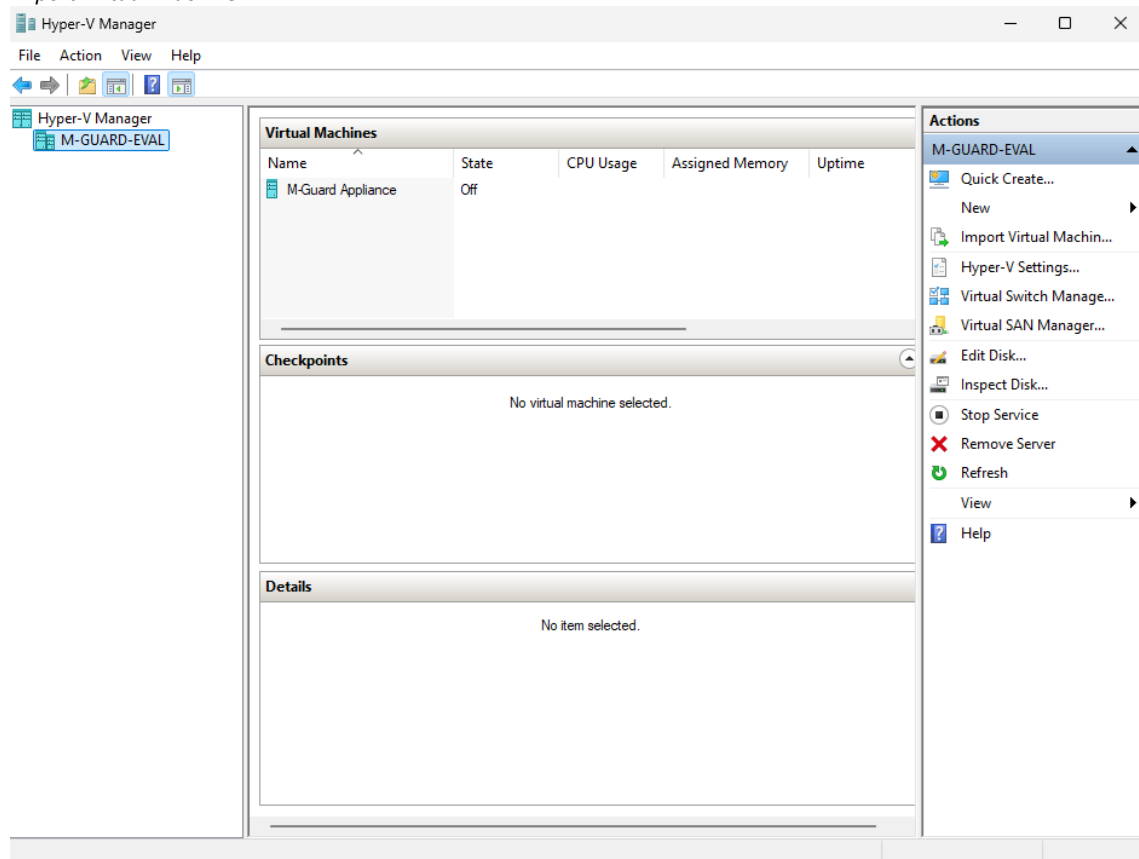
Click “Next>”

Import Virtual Machine



Click “Finish”

Import Virtual Machine



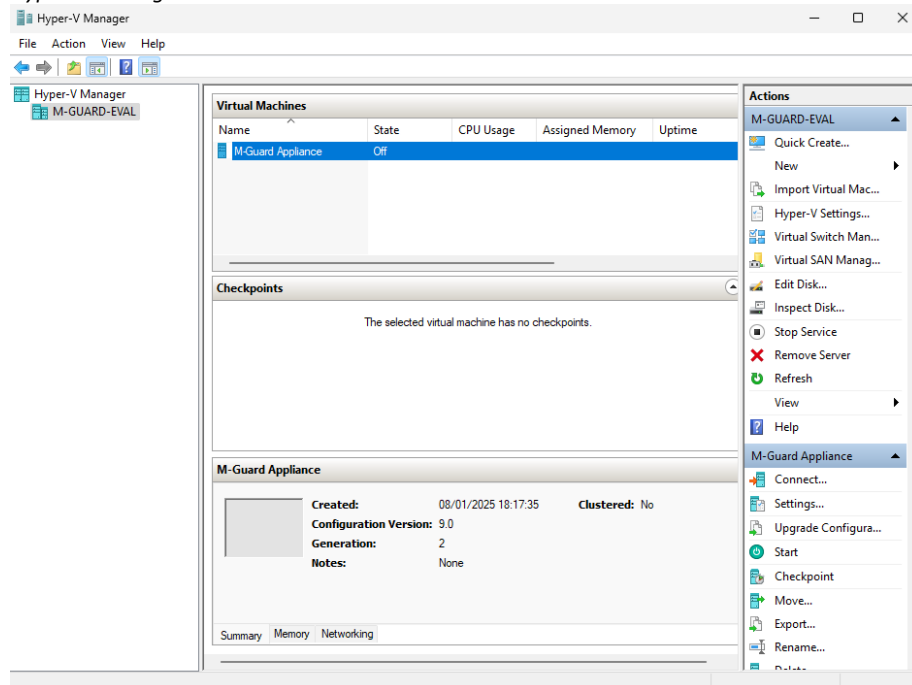
You have now successfully imported the M-Guard Appliance.

You now need to configure the M-Guard Appliance, Start it and Connect to it with M-Guard Console.

Configuring and Starting the M-Guard Appliance

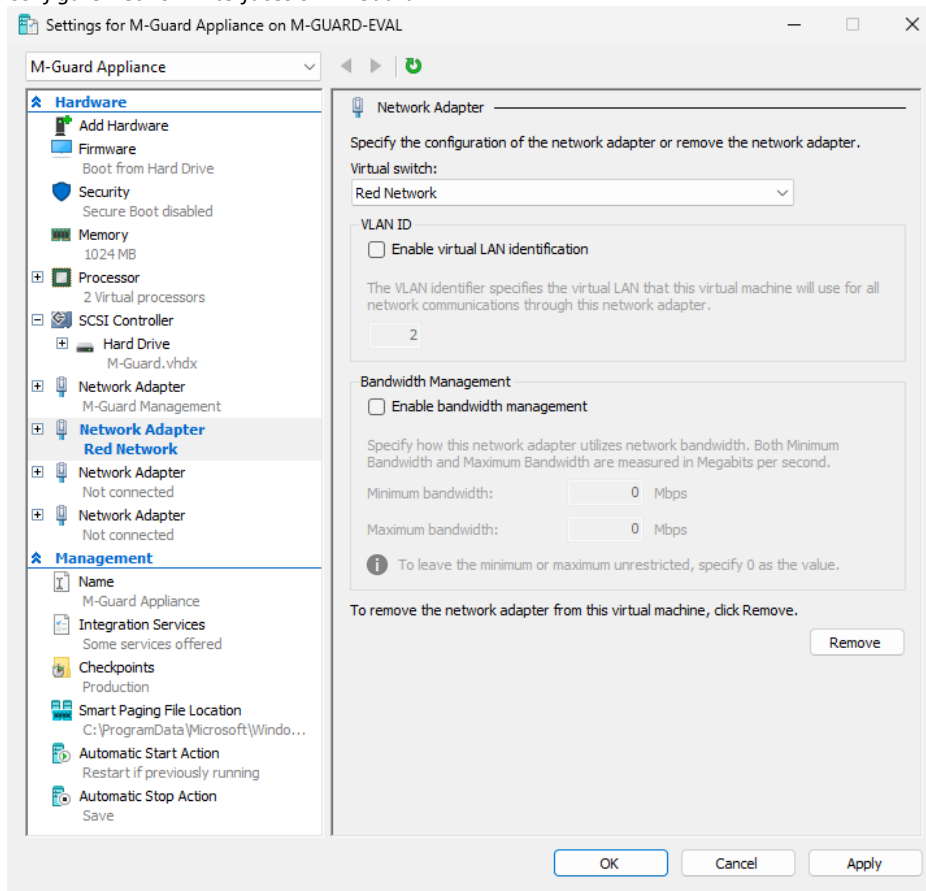
From the Hyper-V Manager we need to configure the Network Interfaces on M-Guard.

Hyper-V Manager



Select the M-Guard Appliance and Click Settings.

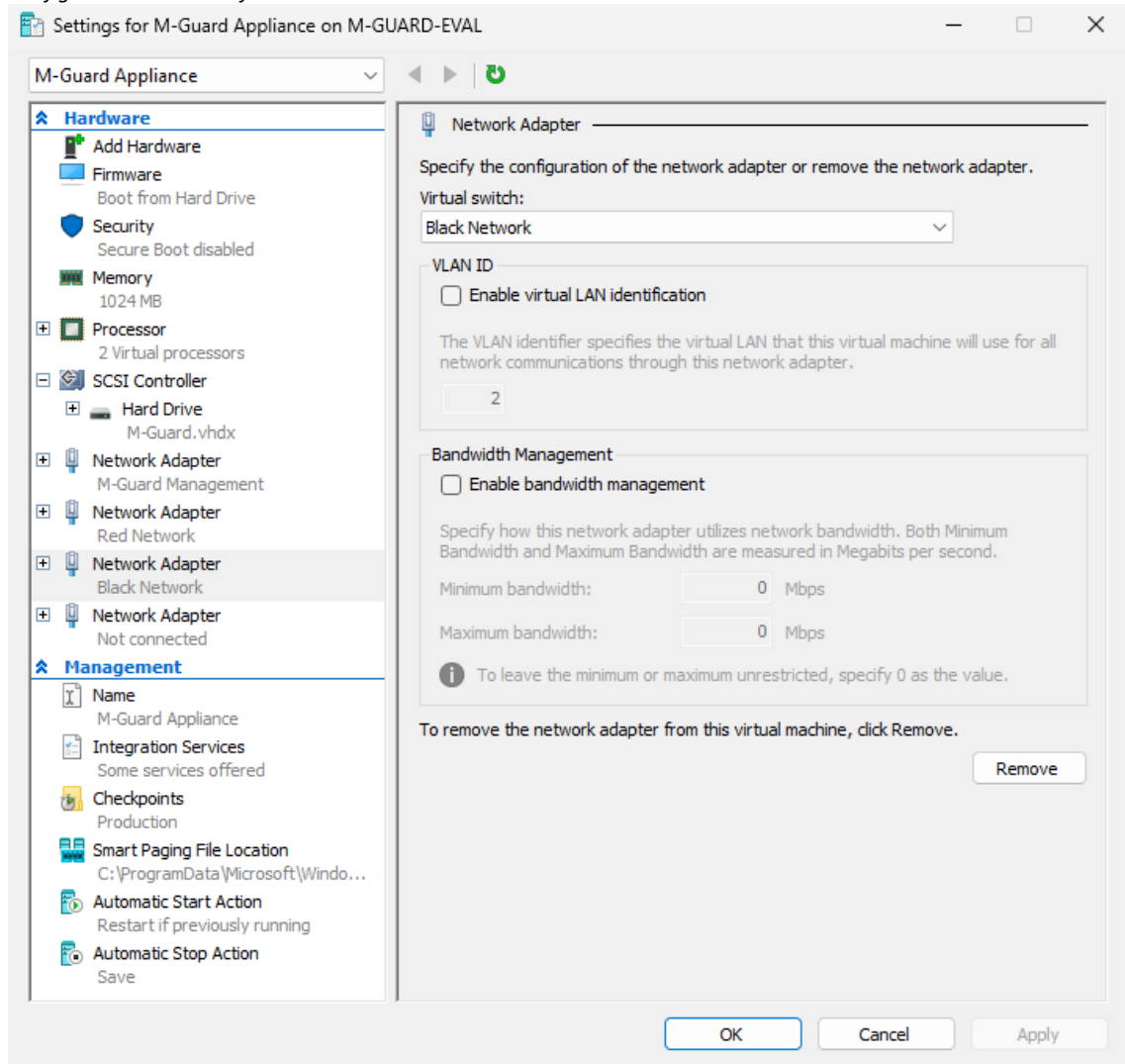
Configure Network Interfaces on M-Guard



The 1st Network Adapter is already configured for M-Guard Management. Change the 2nd Network to Red Network. Click “Apply” and “OK”. Do the same for the 3rd Network Adapter except choose the Black Network. You do not need to do anything with the 4th Network Adapter.

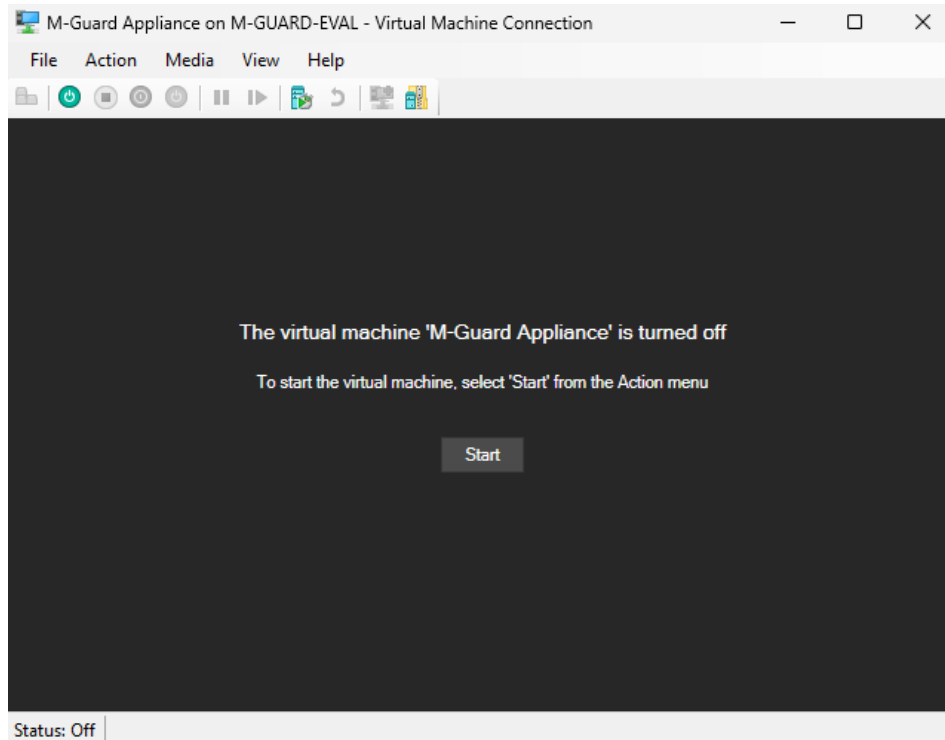
You should have something like the following.

Configure Network Interfaces on M-Guard



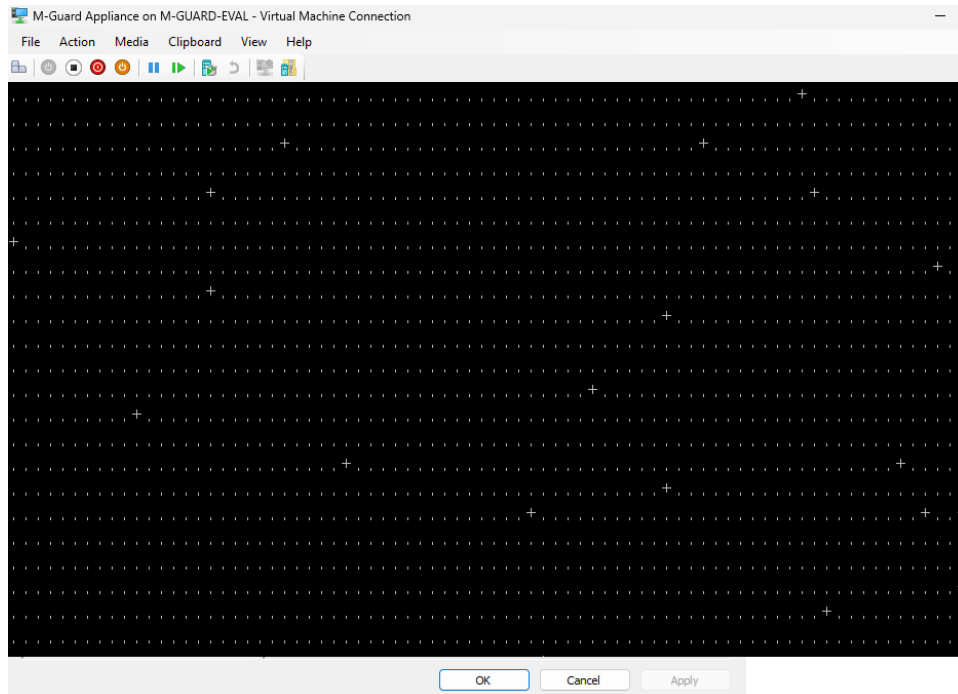
Click "OK". Then from the Hyper-V Manager connect to the M-Guard Appliance.

Connect to M-Guard



Click “Start”. There will be a lot of display like the below but ignore this it is normal.

M-Guard 1st Start



When this has finished you will see the screen below.

```
M-Guard Boot complete
Thu Jan  9 11:38:00 UTC 2025
2025-01-09T11:38:00.838211+00:00 - init[1] kernel security level changed from 0 to 1

SSH host fingerprints:
SHA256:Shj9a4SCLvvCyVp01EL0Ue483y1ZfjkyY6th1ns9ZU8 (ECDSA)
MD5:2c:b4:1d:c2:8c:31:2c:f6:dc:53:fa:52:96:3a:99:ec (ECDSA)
SHA256:uY0JVS5asCcJ/TDHIq/6k1v0+p+1rBS9oRc5ydkNFRE (ED25519)
MD5:33:a1:00:fe:61:b9:d4:14:59:f5:8b:ba:30:00:62:19 (ED25519)
SHA256:ukzHtVtHIXKG+fSVNJ4EHqnTHt7d673euWXBnuxXKJ8 (RSA)
MD5:1b:80:98:e5:60:c2:5f:e6:6f:27:63:c5:99:ed:c6:87 (RSA)
IPv4 link-local address: 169.254.60.116/16 (hn0)
IPv6 link-local address: fe80::215:5dff:fe01:a303%hn0/64
Admin (root) password set to: nTPlf23bJAEum

M-Guard Appliance/m-guard (Amnesiac) (ttyv0)

login: █
```

You will need to note the root Password, the IPv6 link-local address and the last fingerprint key displayed.

You are now ready to connect to the M-Guard Appliance with M-Console.

I suggest creating a folder C:\M-Guard and placing the M-Guard-Console-1.5.5.jar file in there.

Open a command prompt, navigate to the C:\M-Guard folder and run the command.

```
C:\M-Guard> java - jar M-Guard-Console-1.5.5.jar
```

Configuring and the Guard with M-Guard Console

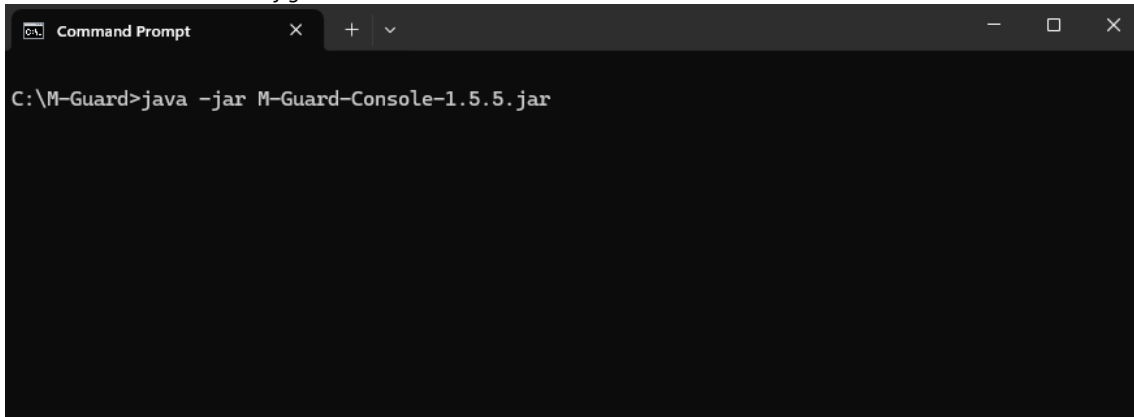
I suggest creating a folder C:\M-Guard and placing the M-Guard-Console-1.5.5.jar file in there.

I also suggest you create an empty subfolder of C:\M-Guard\M-Guard Eval

Open a command prompt, navigate to the C:\M-Guard folder and run the command.

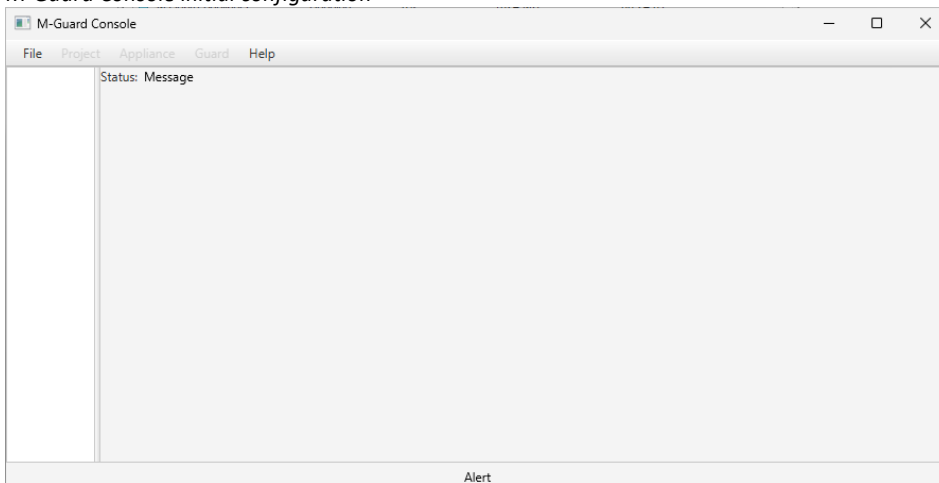
```
C:\M-Guard> java -jar M-Guard-Console-1.5.5.jar
```

M-Guard Console initial configuration



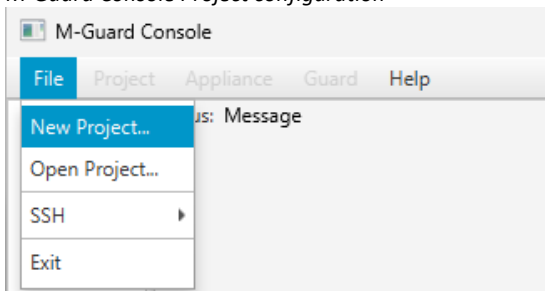
You will then be presented with this screen.

M-Guard Console initial configuration

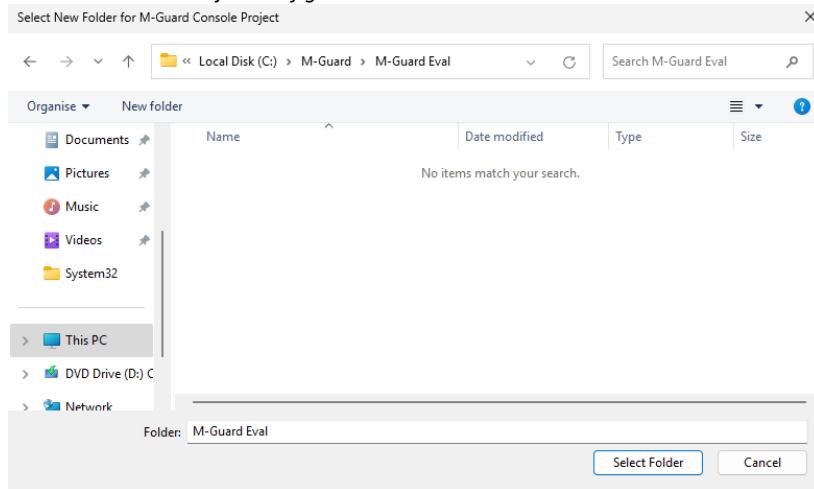


Select File--> New Project

M-Guard Console Project configuration

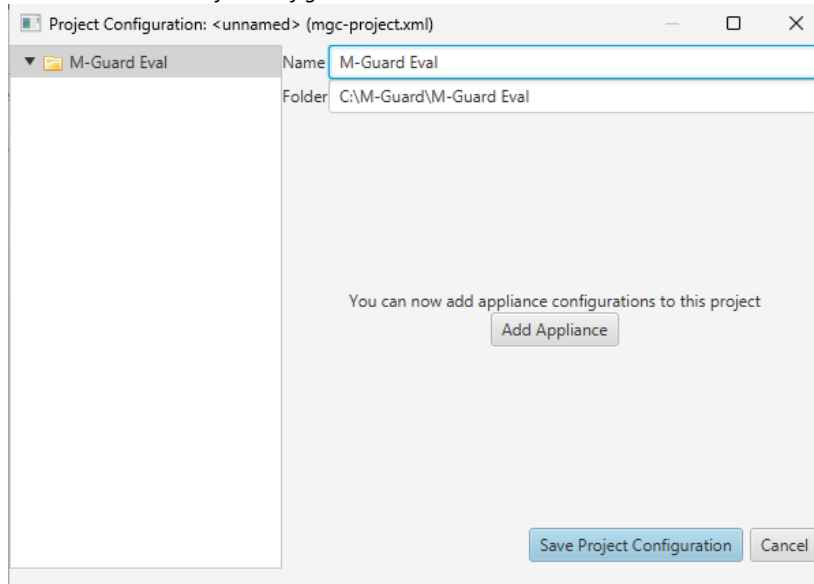


M-Guard Console Project configuration



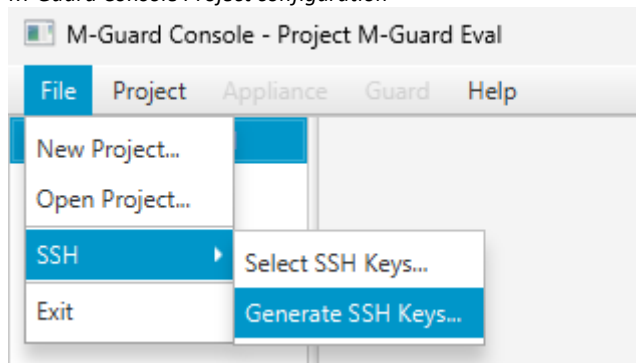
Select Folder C:\M-Guard\M-Guard Eval

M-Guard Console Project configuration



Enter Name --> M-Guard Eval, then Click “Save Project Configuration”.

M-Guard Console Project configuration



Select File-->SSH-->Generate SSH Keys. You will be presented with the following screen.

M-Guard Console Project configuration

This will generate a new SSH key pair for use by M-Guard Console and save them in the specified folder

Directory

Key Length Key Type

Comment

Passphrase

Confirm Passphrase

M-Guard Console Project configuration

This will generate a new SSH key pair for use by M-Guard Console and save them in the specified folder

Directory

Key Length Key Type

Comment

Passphrase

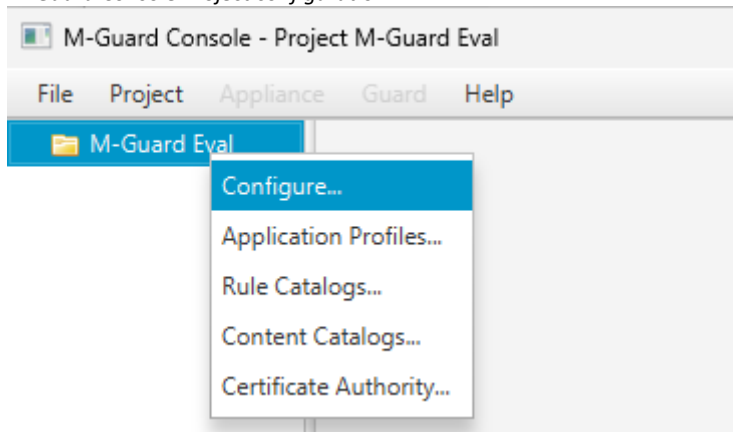
Confirm Passphrase

Select Folder C:\M-Guard\M-Guard Eval

Enter email and Passphrase (does not need to be your email) note the passphrase is not related to your email password.

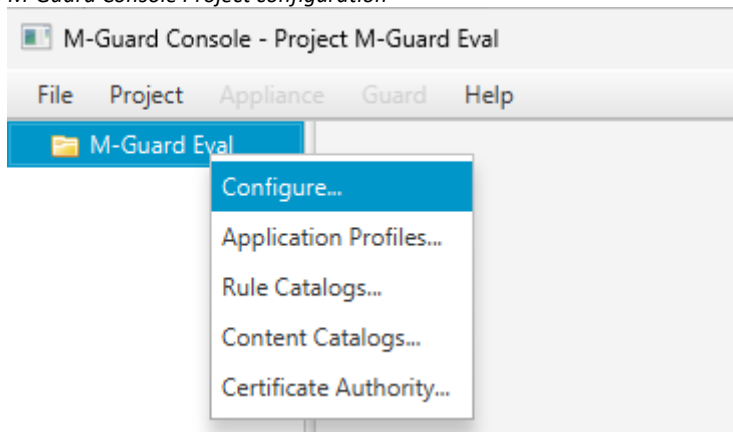
Click “Generate”.

M-Guard Console Project configuration

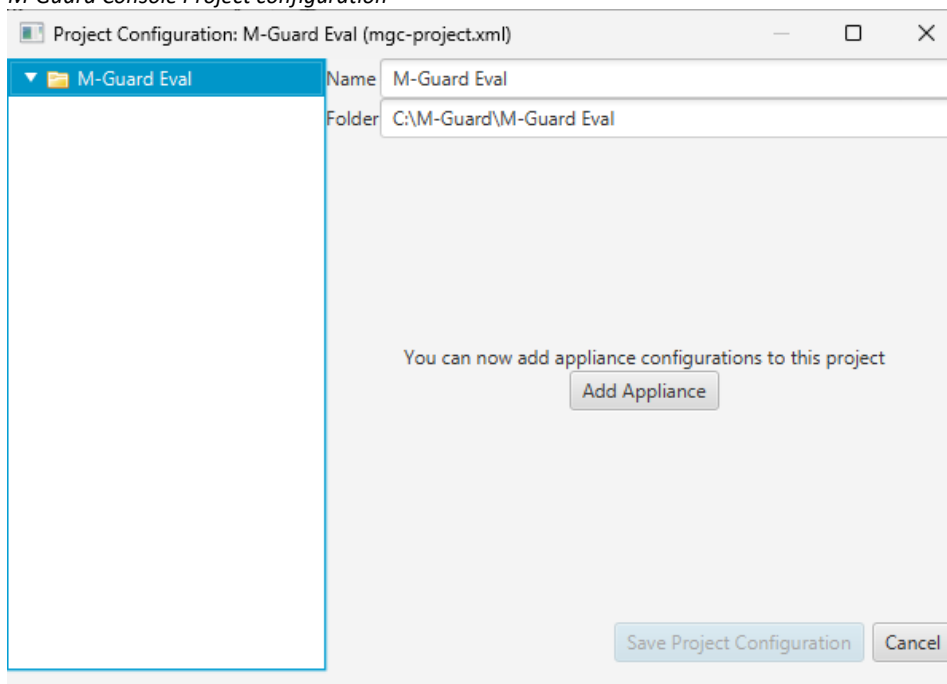


Right Click on Project M-Guard Eval and select Configure.

M-Guard Console Project configuration

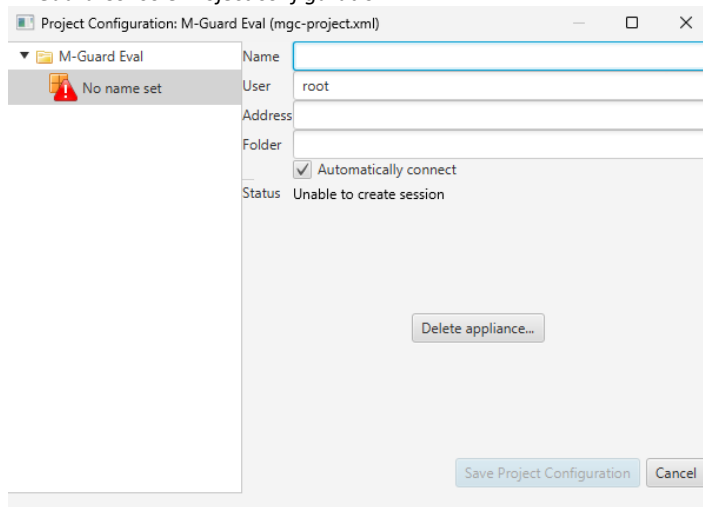


M-Guard Console Project configuration



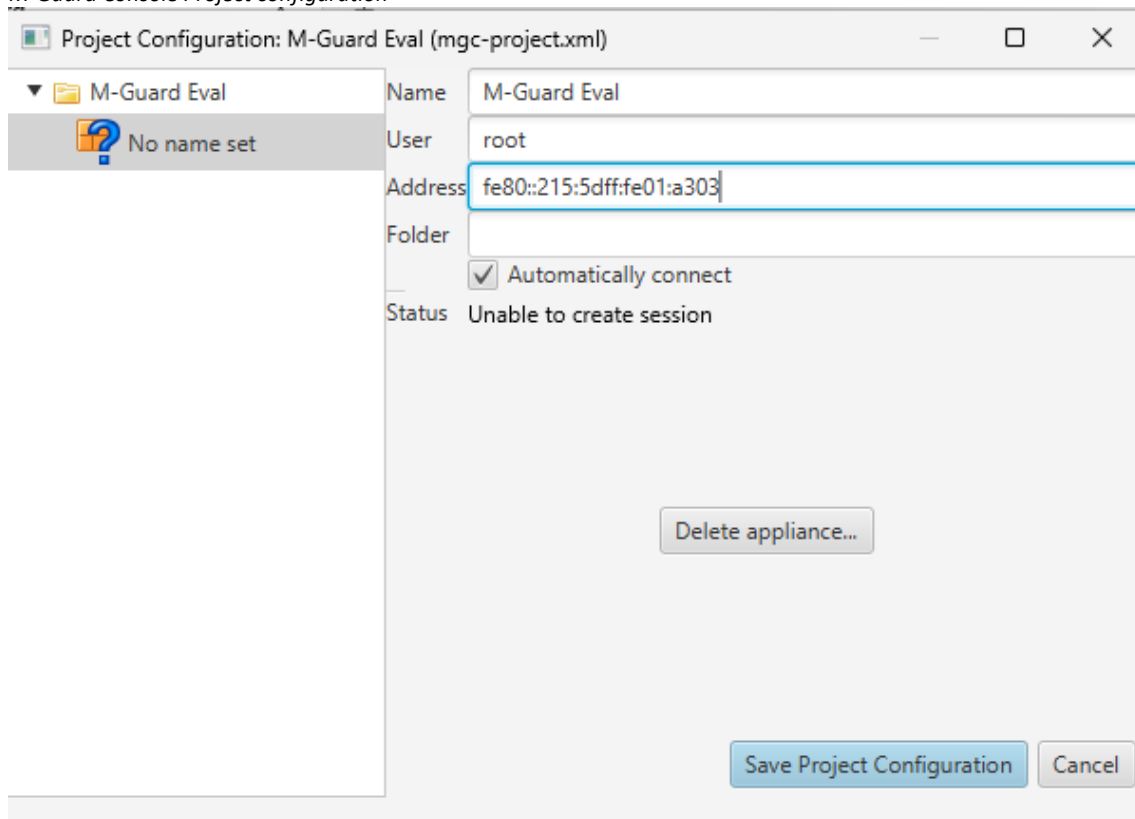
Click "Add Appliance".

M-Guard Console Project configuration



Enter Name, IPv6 Address where the IPv6 Address is the one you noted down earlier.

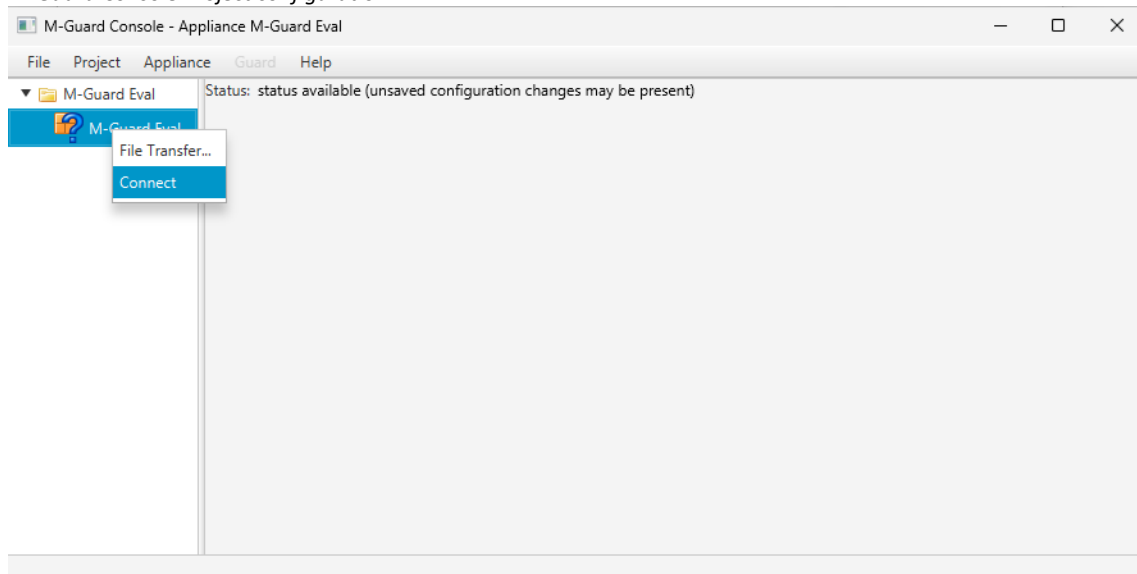
M-Guard Console Project configuration



Click “Save Project Configuration”.

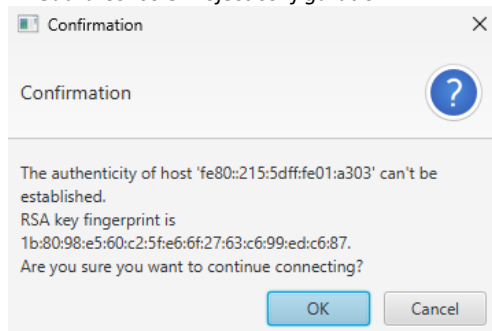
Right Click on the Appliance and Click Connect.

M-Guard Console Project configuration



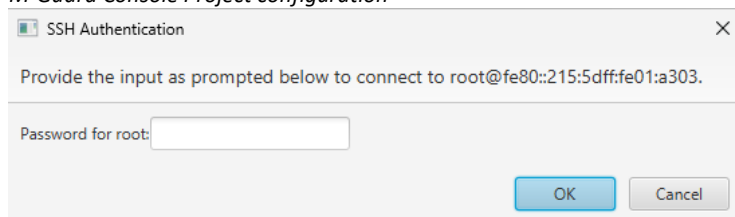
You will see the following dialogue box.

M-Guard Console Project configuration



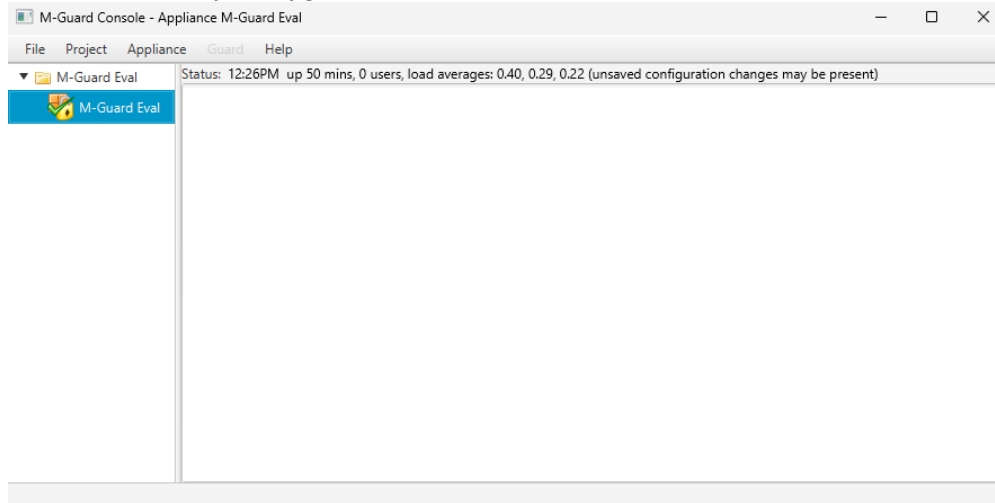
Verify that the Key displayed matches the one you noted earlier and Click “OK”

M-Guard Console Project configuration



Enter the root password noted earlier. Click “OK”.

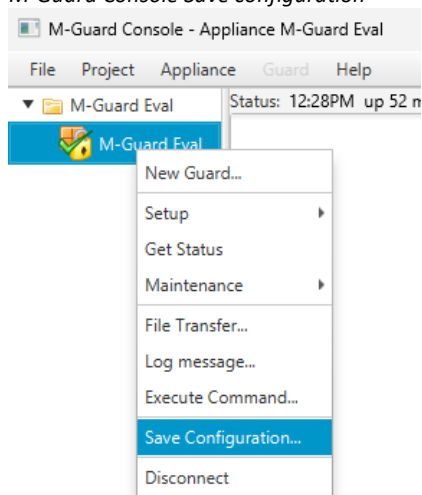
M-Guard Console Project configuration



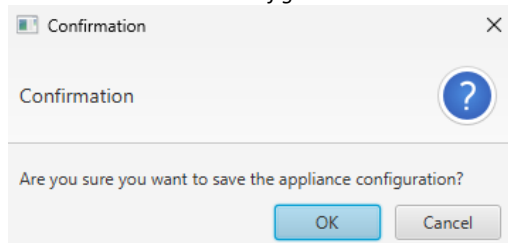
You have now connected to the Appliance and need to start configuring it.

During the Configuration Process it is good practice to regularly "Save the Configuration". Right Click on the Appliance and Click "Save Configuration"

M-Guard Console Save configuration

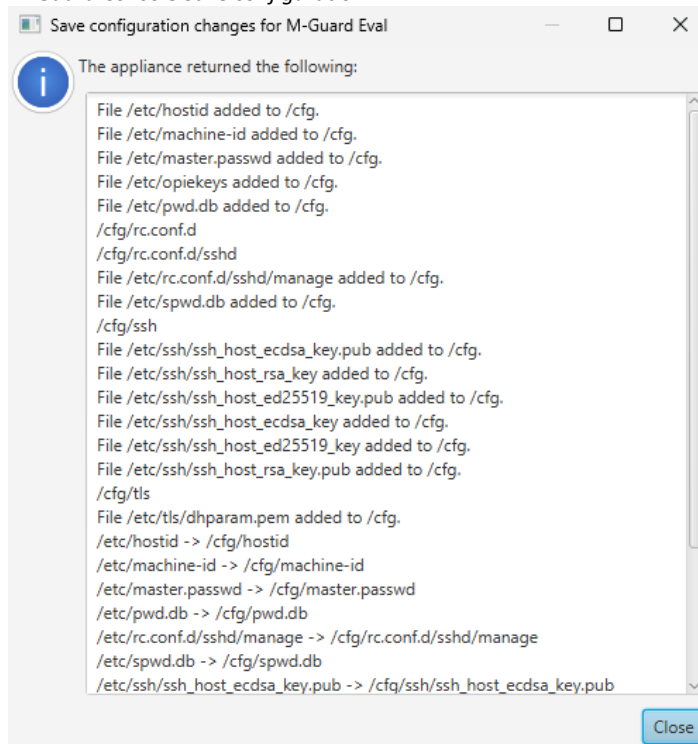


M-Guard Console Save configuration



Click OK

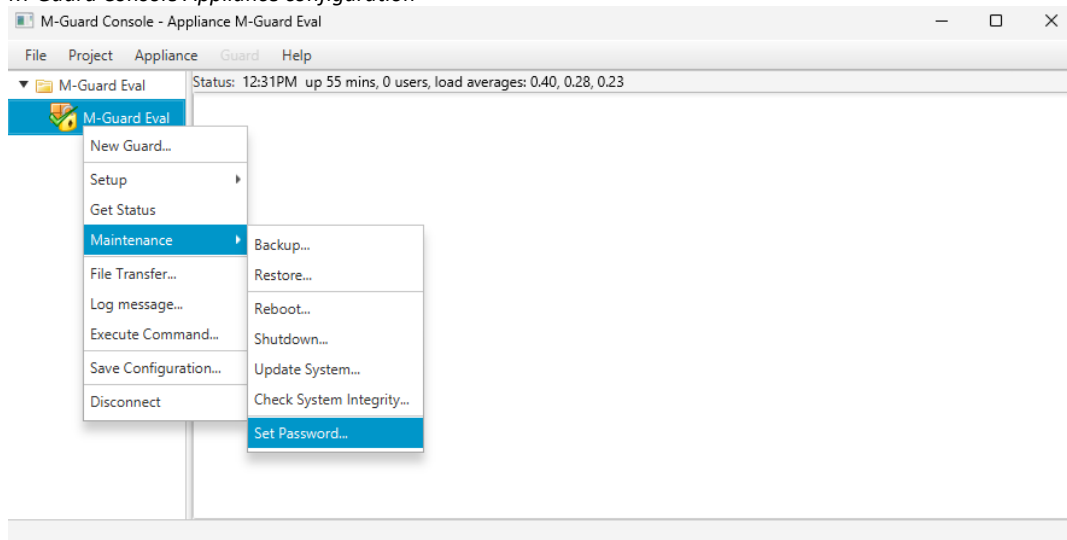
M-Guard Console Save configuration



Click Close.

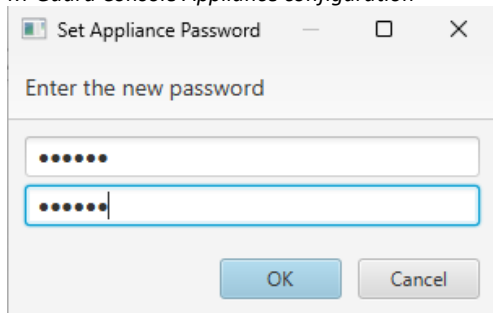
Right Click on the Appliance Maintenance-->Set Password

M-Guard Console Appliance configuration



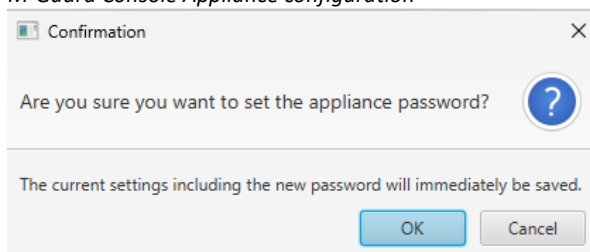
The following Dialogue will appear.

M-Guard Console Appliance configuration



Enter your New Password and Click “OK”.

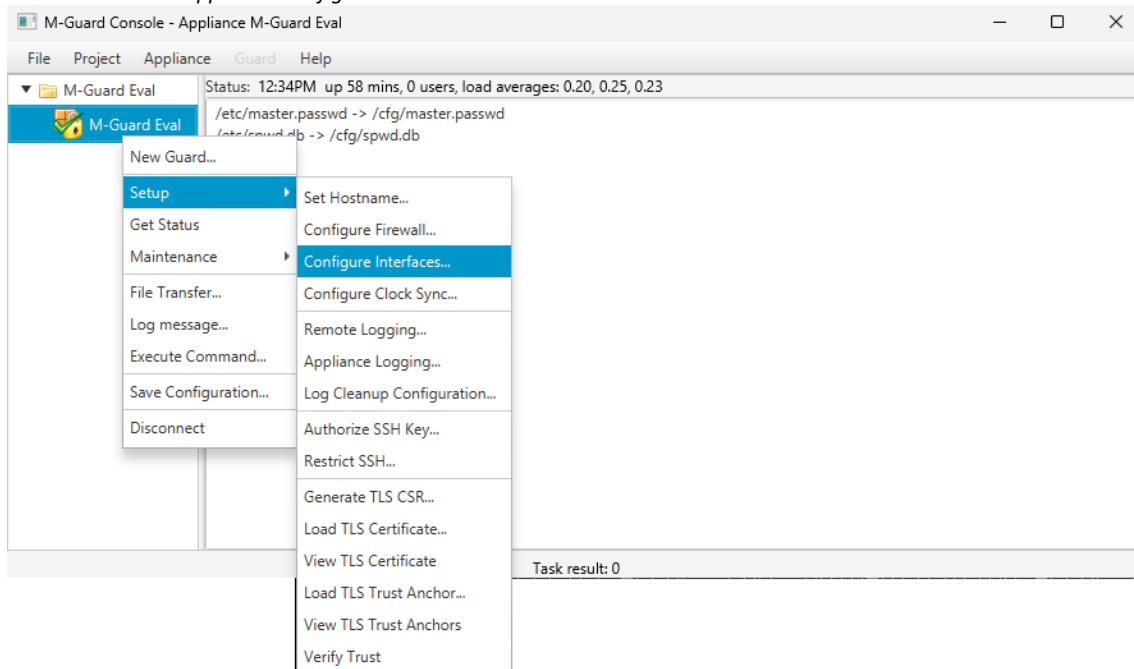
M-Guard Console Appliance configuration



Click “OK”.

Right Click on the Appliance Setup-->Configure Interfaces..

M-Guard Console Appliance configuration



M-Guard Console Appliance configuration

The screenshot shows the 'Interface Configuration' window for the 'hn0' interface. The 'IP Address' tab is selected, showing the IPv4 address set to 10.178.0.2 with a prefix length of 24. The IPv6 section is currently empty. A status message at the top indicates 'hn0 is currently enabled'. At the bottom, there are 'OK', 'Revert', and 'Cancel' buttons, along with a note that configuration on this tab has been modified.

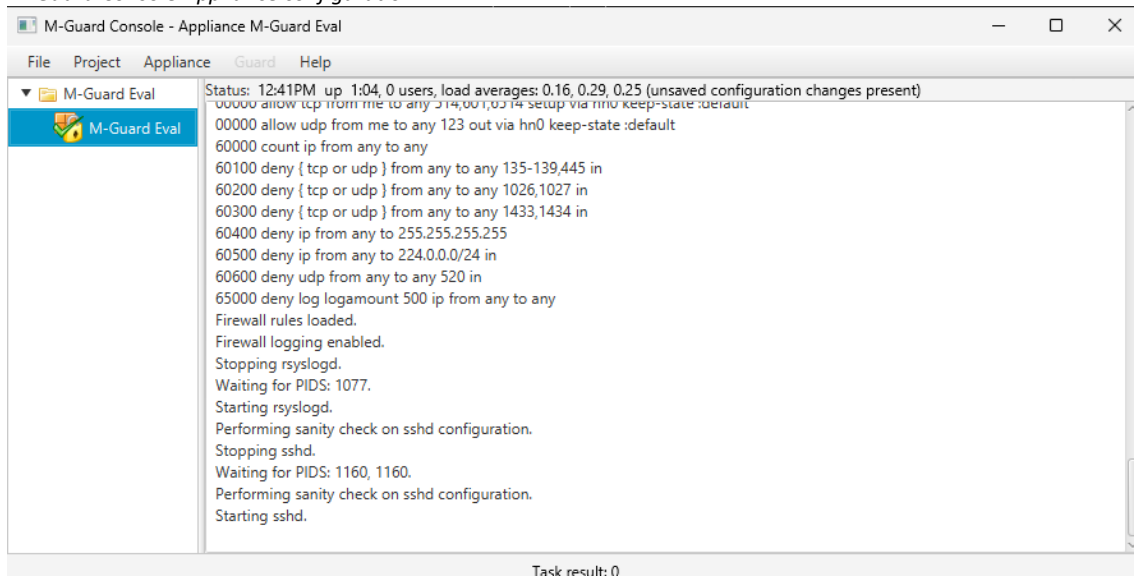
Start with “hn0”, the Management Interface and set the IPv4 Address to 10.178.0.2.
Then Settings Tab

M-Guard Console Appliance configuration

The screenshot shows the 'Interface Configuration' window for the 'hn0' interface, now on the 'Settings' tab. The 'Name' field is set to 'hn0'. There are three checkboxes: 'Allow management services' (checked), 'Allow GCXP' (unchecked), and 'Allow time services' (unchecked). At the bottom, there are 'OK', 'Revert', and 'Cancel' buttons, and a note that configuration on this tab has been modified.

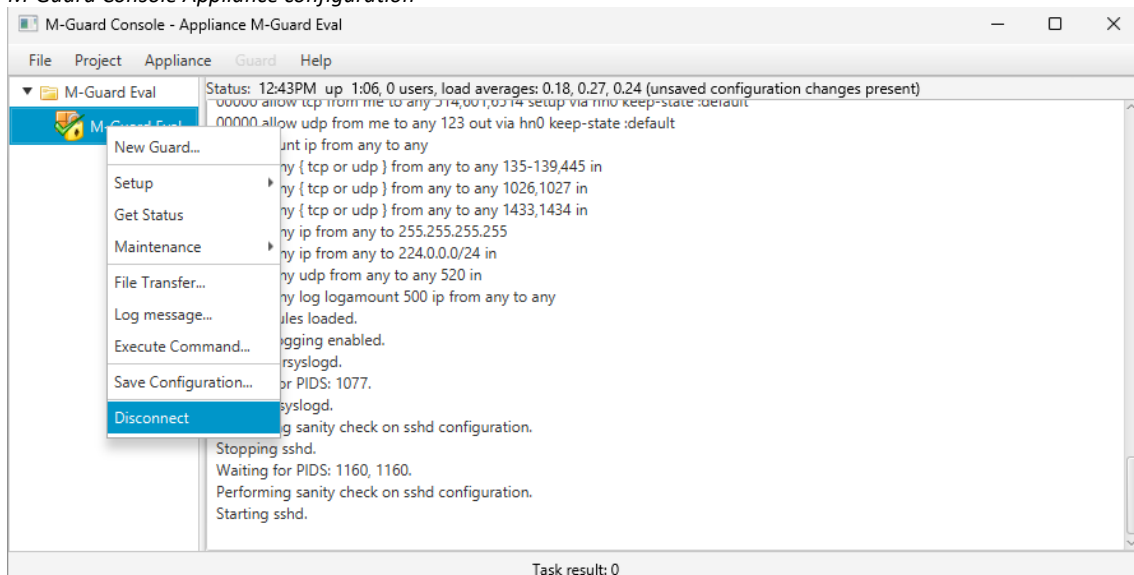
Check “Allow management services” . Click “OK”.

M-Guard Console Appliance configuration



Your Appliance should “Disconnect”, if it does not, Right Click on the Appliance.

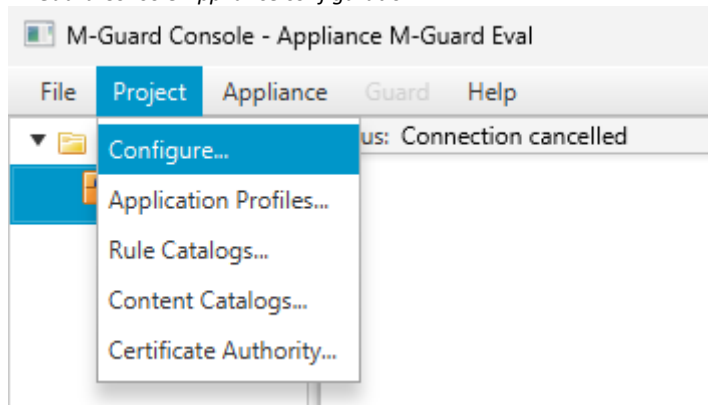
M-Guard Console Appliance configuration



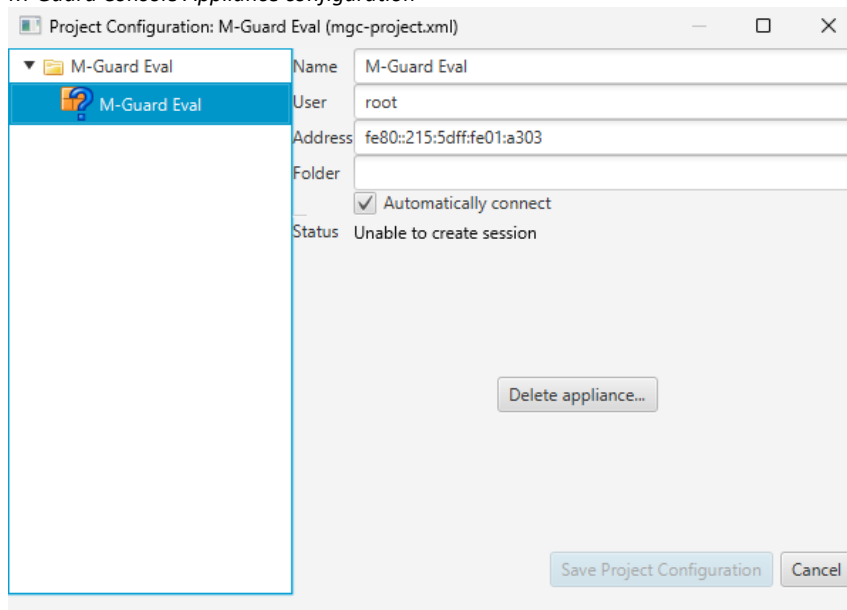
Select “Disconnect”.

Select Project --> Configure

M-Guard Console Appliance configuration

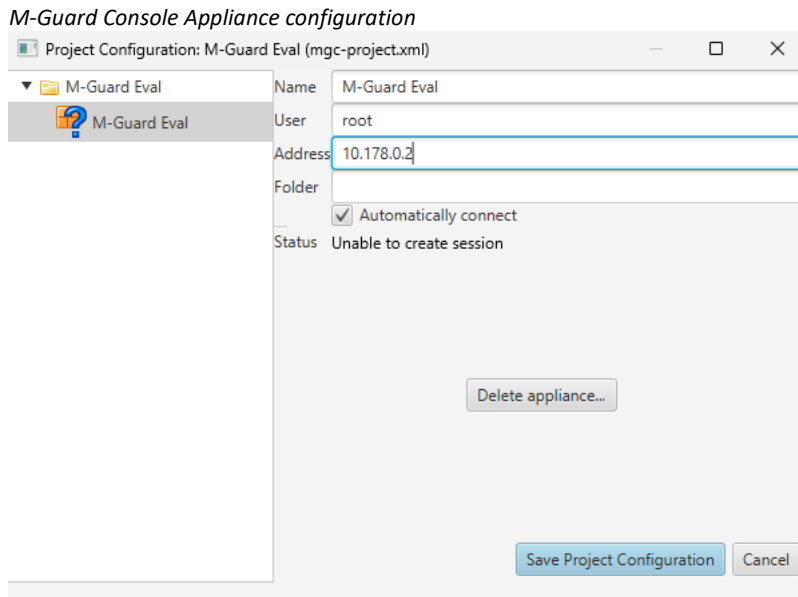


M-Guard Console Appliance configuration



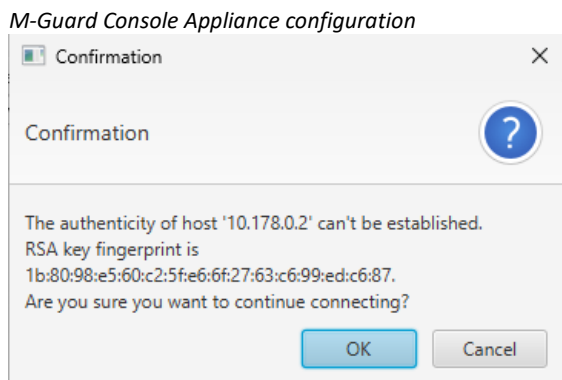
Select M-Guard Eval

Change the IPv6 Address to your just configured IPv4 Address



Click “Save Project Configuration”

Right Click on the Appliance and Click “Connect.”



Verify SSH Key, Click OK.

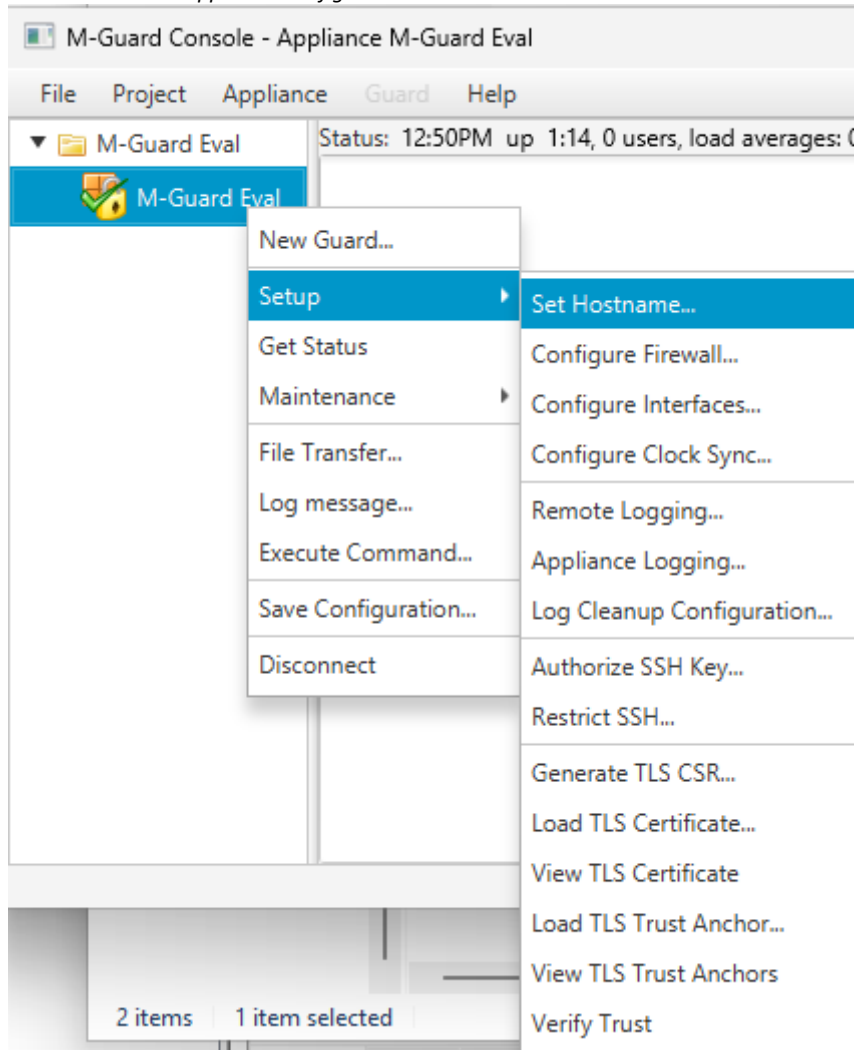
Enter New Password you set.

Run the “Save Configuration” process.

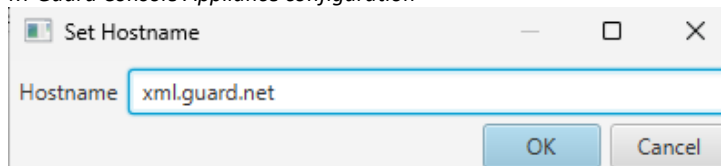
We now need to Set the ”Hostname” of the Appliance.

Right Click Setup-->Set hostname

M-Guard Console Appliance configuration

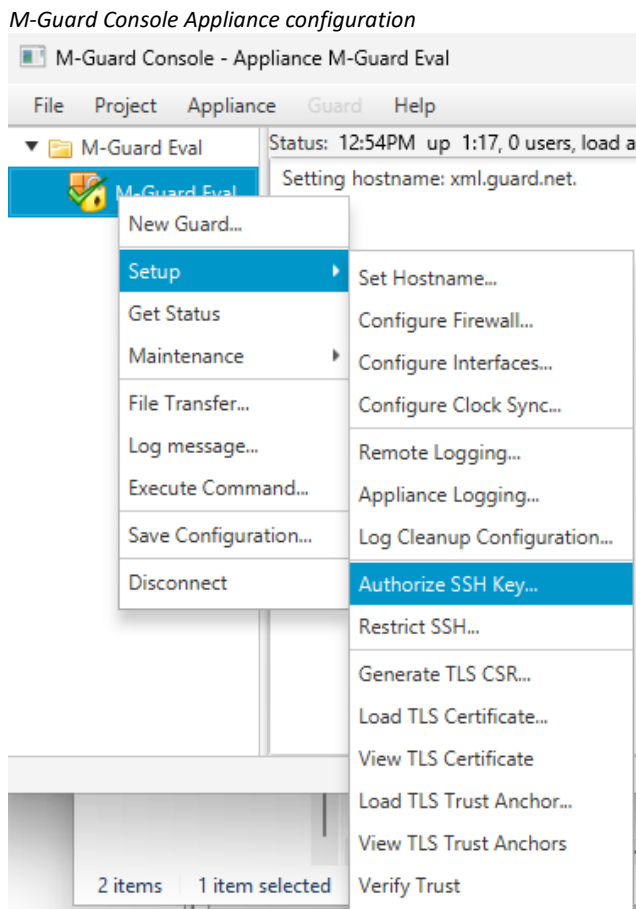


M-Guard Console Appliance configuration

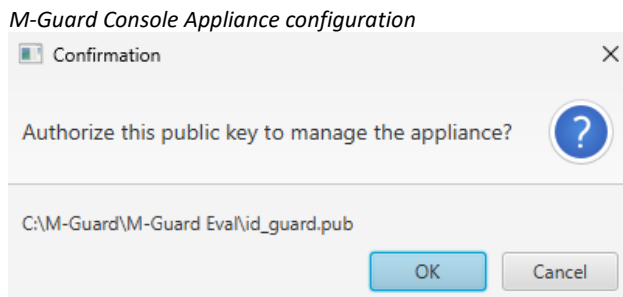


Enter Hostname (Your Choice), Click OK.

Next, we need to Authorize the SSH Key.



Right Click Setup-->Authorize SSH Key.



Click OK

Next, we need to Configure the other Interfaces.

M-Guard Console Appliance configuration

Interface Configuration

Interface: hn1

IP Address * | IP Aliases | Settings

hn1 is currently not enabled

IPv4

Address: 192.168.56.2 | Prefix Length: 24

IPv6

Address: | Prefix Length: 64

* Configuration on this tab has been modified

OK | Revert | Cancel

Select “hn1” the Red Network and set the IP to 192.168.56.2 as per your network map.

Then Click the “Settings” Tab.

M-Guard Console Appliance configuration

Interface Configuration

Interface: hn1

IP Address * | IP Aliases | Settings *

Name: hn1

Allow management services

Allow GCXP

Allow time services

* Configuration on this tab has been modified

OK | Revert | Cancel

Check “Allow GCXP”.

Click OK.

Repeat the process for “hn2”, the Black Network with IP Address 192.168.106.2 .

Run the Save Configuration Process.

You are now ready to Add a “Guard Instance”.

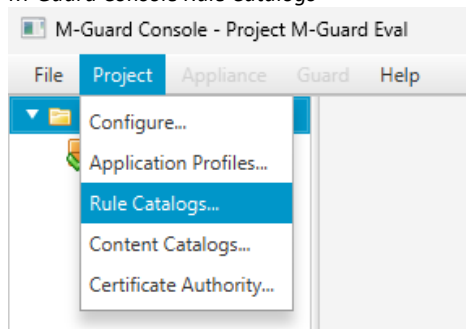
Prepare to Add an M-Guard Instance

At this point, we are ready to create a new M-Guard instance using the “Demo Protocol” profile. The Demo Protocol provides a simple protocol that is built into M-Guard Console and so can be used to demonstrate and test M-Guard without any external application.

There are default “Rule Catalogs” used by the “Demo Protocol” that are preloaded into the Appliance, to see these.

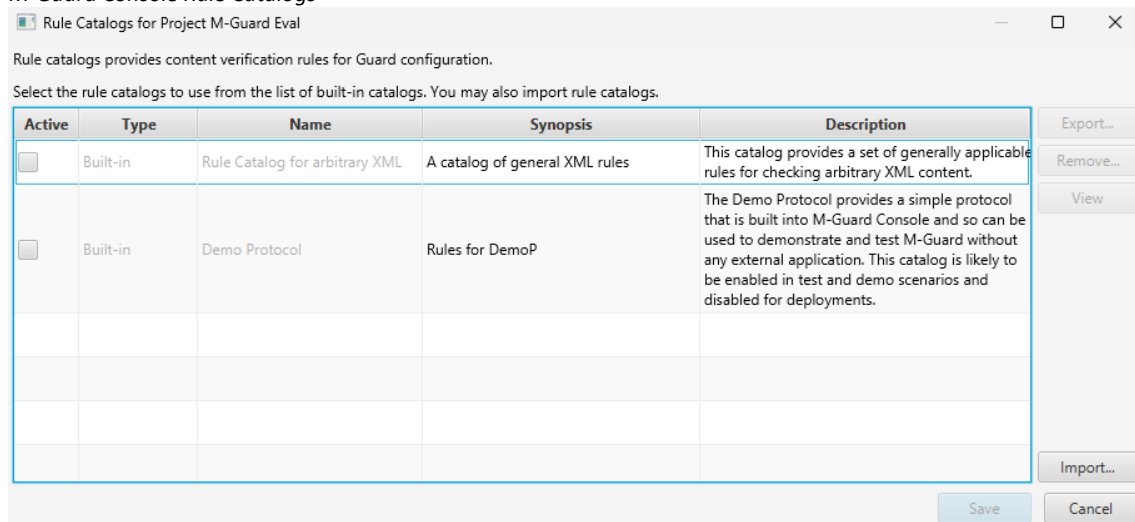
Select Project→Rule Catalogs.

M-Guard Console Rule Catalogs



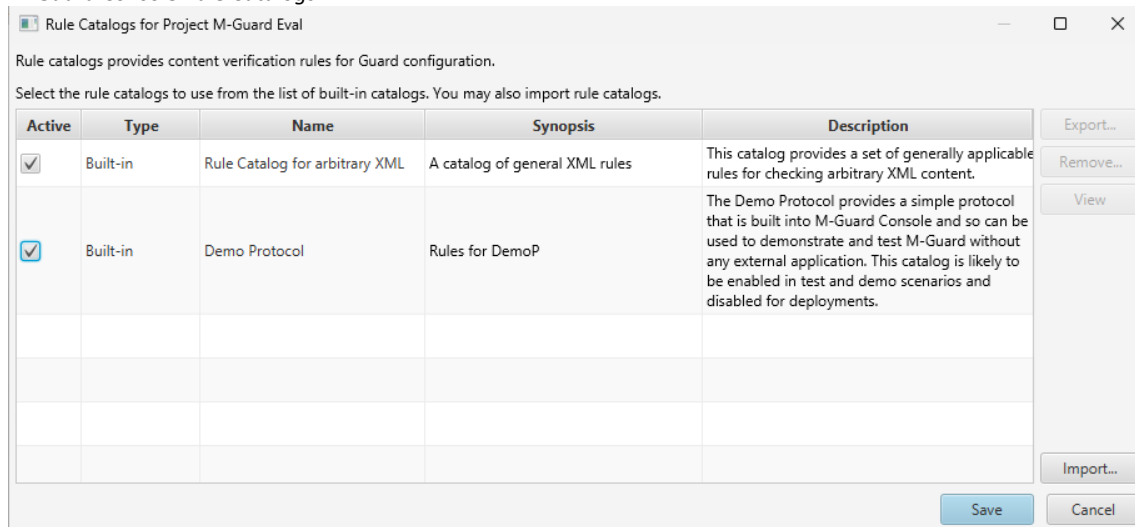
The following is displayed.

M-Guard Console Rule Catalogs



Check the two Checkboxes and Click “Save”.

M-Guard Console Rule Catalogs

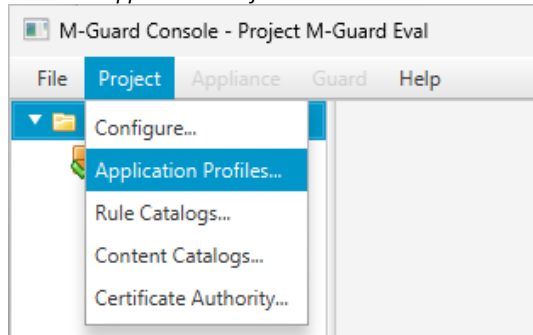


It is from here that we can import new Rule Catalogs e.g. for XMPP, Red/Black, FAB or Icon-5066 using the “Import...” button.

Each Guard will have an “Application Profile” specific for its use. There is a “Demo Protocol” built into the appliance but if you need to load another one, for example for XMPP, Red/Black, FAB or Icon-5066 you should do it now.

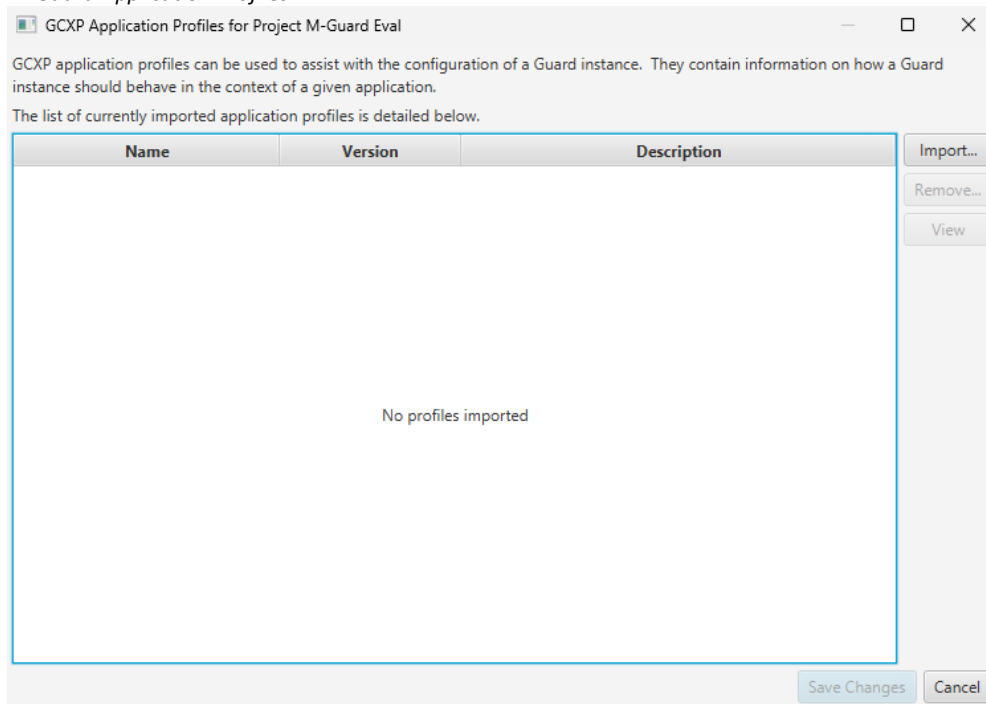
Select Project→Application Profiles...

M-Guard Application Profiles



The following is displayed.

M-Guard Application Profiles



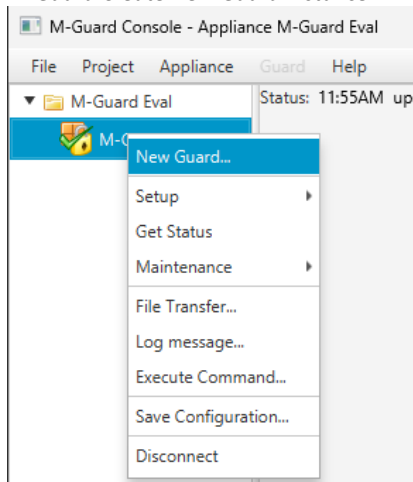
Use the “Import...” button to load new application profiles. Then Click “Save Changes” for now just Click “Cancel”, as the “Demo Protocol” profile is already built-in in the appliance.

Configuring a new M-Guard Instance

We are now ready to add a “Guard Instance” to our “Guard Appliance”, in this example it will be one for the “Demo Protocol” Application Profile.

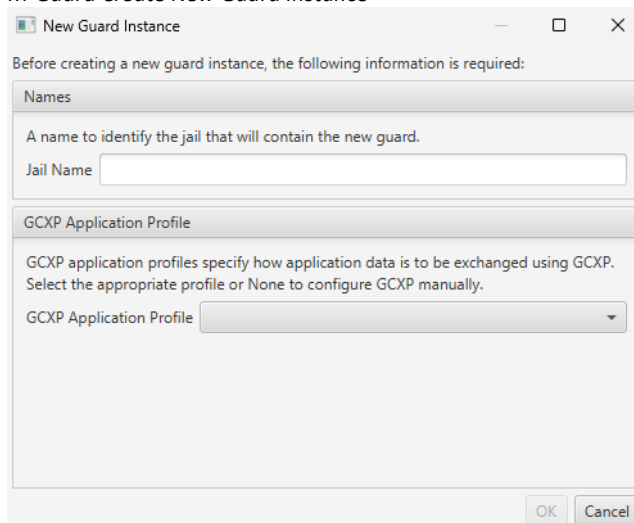
From the Guard Appliance Select “New Guard...”.

M-Guard Create New Guard Instance



The following is displayed

M-Guard Create New Guard Instance

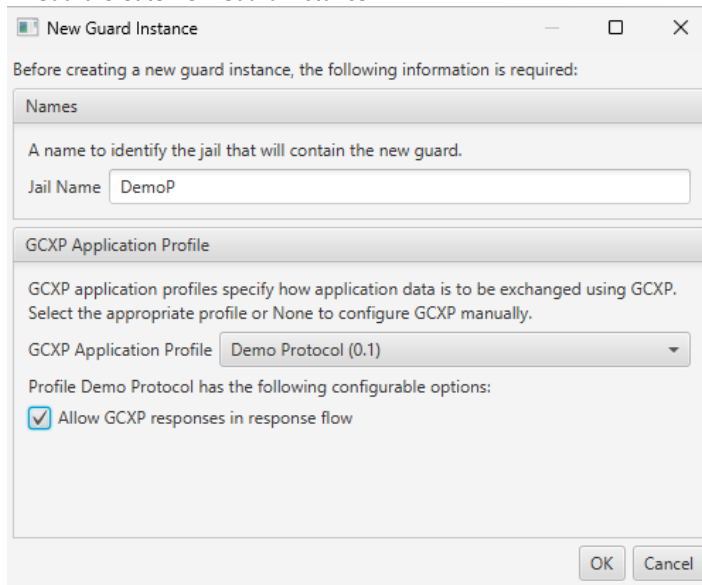


Give it a "Jail Name" (Can be anything)

Select "Demo Protocol (0.1)" from the drop down for "GCXP Application Profile".

Check the "Allow GCXP responses in flow" Checkbox.

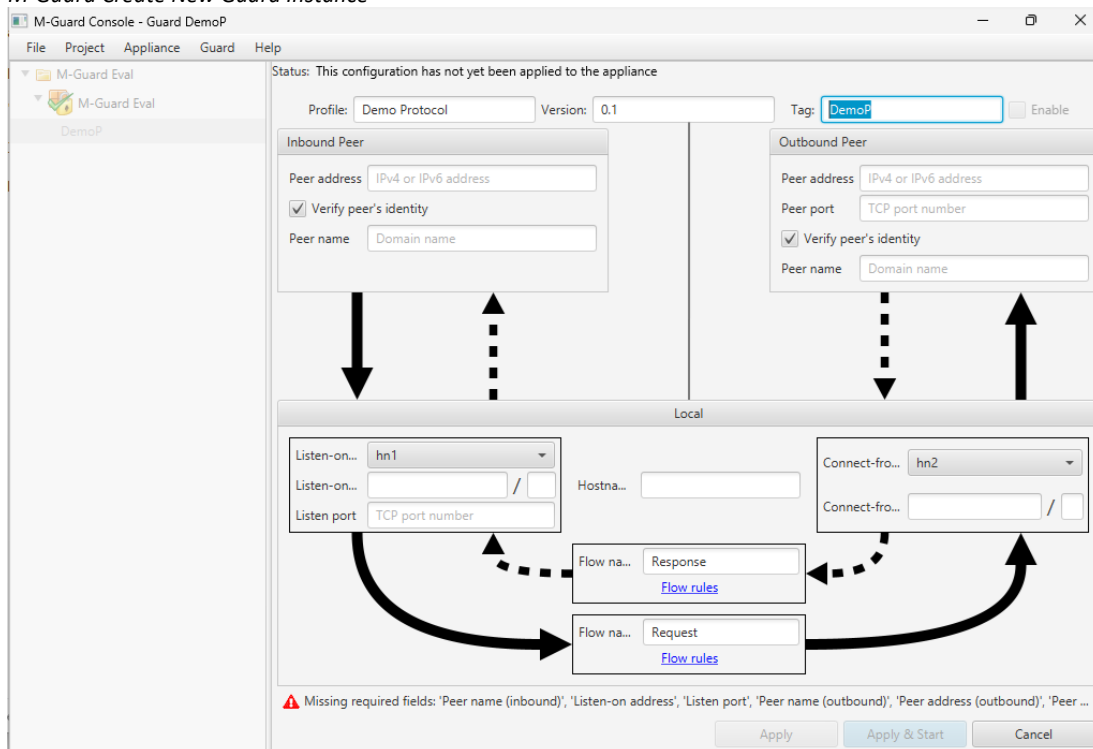
M-Guard Create New Guard Instance



Click "OK"

The following is displayed

M-Guard Create New Guard Instance



Some notes on filling in the fields.

Profile and Version give details of the GCXP application profile used to create the Guard, which cannot be edited, Tag is a (typically short) string used in syslog to identify this Guard, and Enable toggles whether the service created for this Guard will be automatically started when the appliance is booted or will have to be manually started.

On the Inbound Peer, which is the one connecting to the Guard:

- Peer Address: This is the IP Address that connections will come from.
- Verify Peer's Identity: This will check the "Peer Name" in the Certificate.
- Peer Name: The domain name of the inbound Peer.

On the Outbound Peer, which is the one the Guard will connect to:

- Peer Address: This is the IP Address that connections will connect to.
- Peer Port: This is the Port the Guard will connect to.
- Verify Peer's Identity: This will check the "Peer Name" in the Certificate.
- Peer Name: The domain name of the outbound Peer.

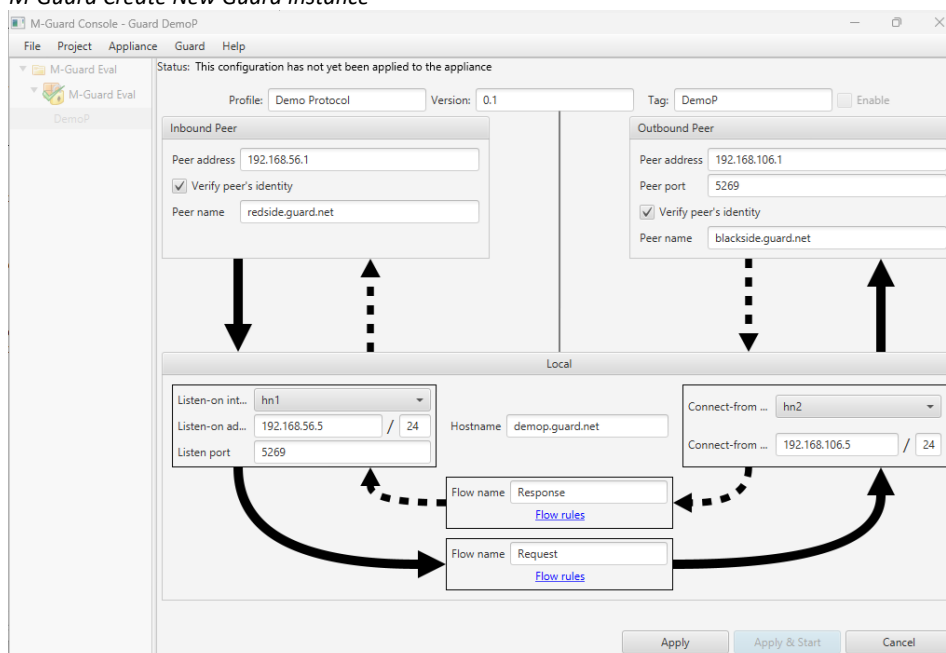
On the Guard networking, the options are as follows:

- Listen-on interface: Interface the Guard listens on for inbound connections.
- Listen-on address: IP address the Guard listens on for inbound connections.
- Listen Port: TCP port the Guard listens on for input side connections to it.
- Connect-from interface: Interface the Guard uses to make its outbound connection.
- Connect-form address: IP address the Guard uses to make its outbound connection.
- Hostname: The domain name of the Guard, included in the Guard's cert

The two Flow Name fields name the respective flows, and are used in event logging, while arrows indicate the direction of the flow, with the style of the arrow indicating whether any GCXP content (solid line), GCXP responses only (dotted line), or no content (blank), is allowed through the flow.

Below is how we have configured ours.

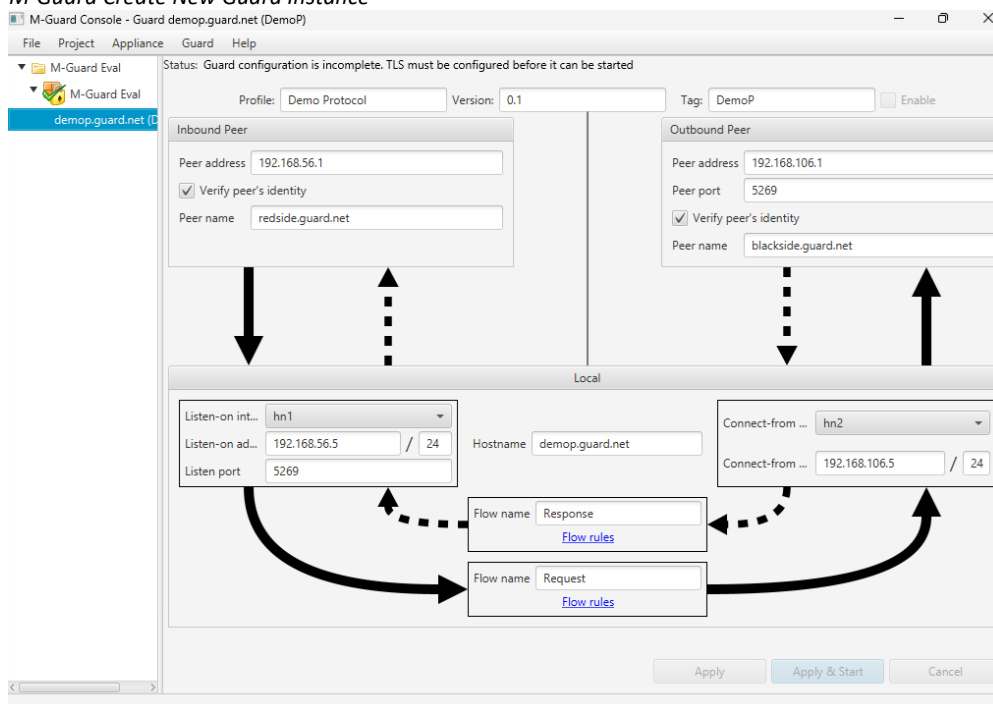
M-Guard Create New Guard Instance



Click "Apply".

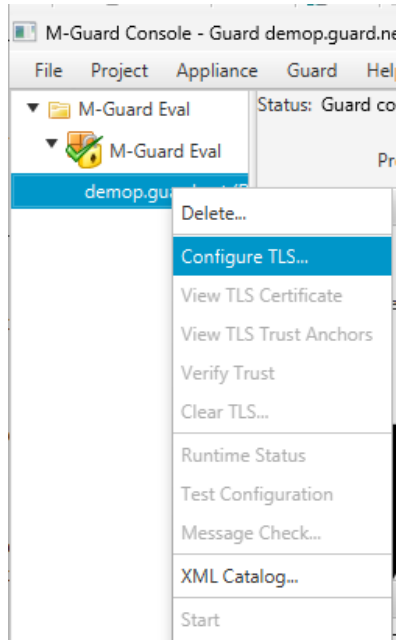
After a short period of time, the following is displayed, informing that TLS configuration is to be done before it can be started:

M-Guard Create New Guard Instance



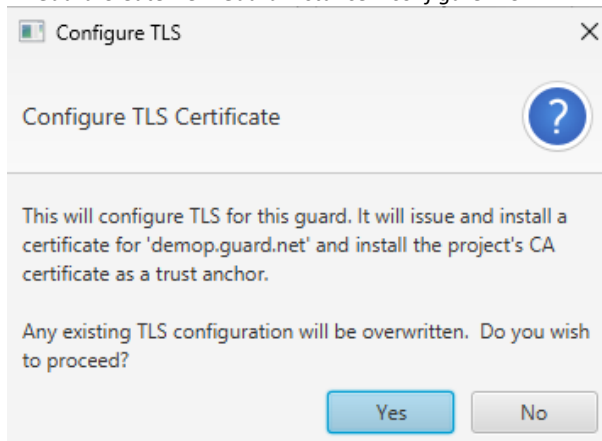
Now we need to configure the TLS for this M-Guard instance. Right click on the M-Guard instance and select “Configure TLS...”.

M-Guard Create New Guard Instance – configure TLS



The Following is displayed.

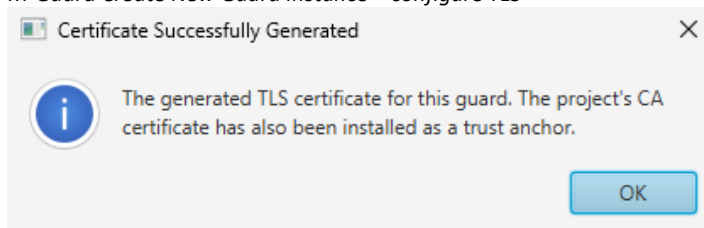
M-Guard Create New Guard Instance – configure TLS



Click "Yes".

After a Short period of time.

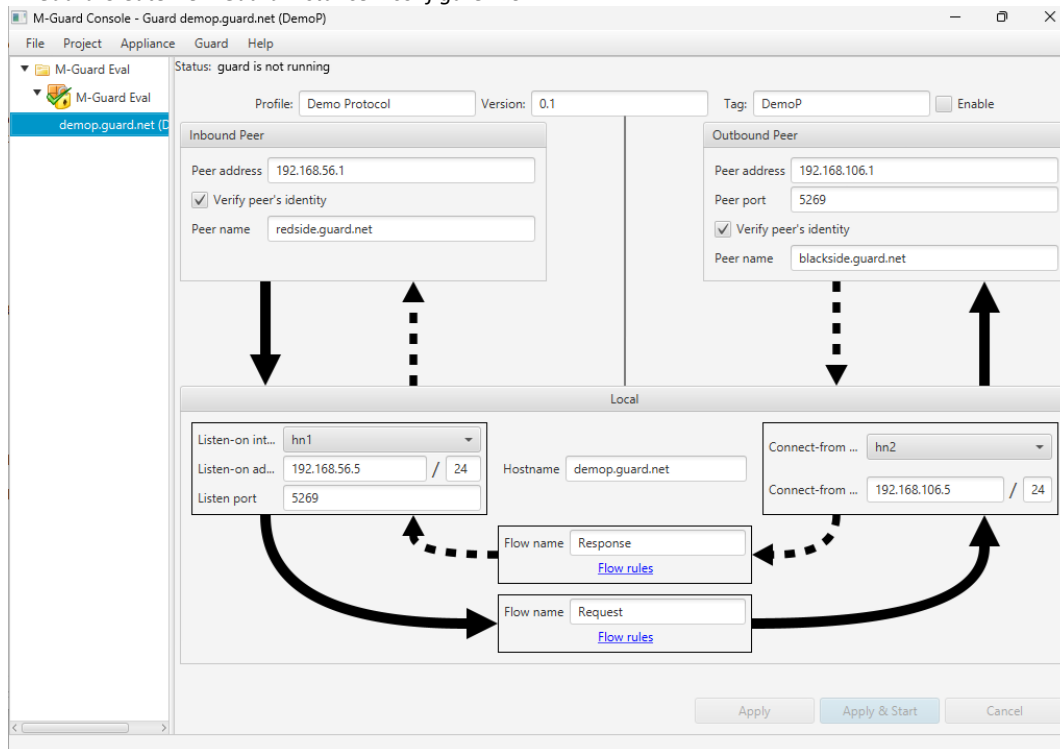
M-Guard Create New Guard Instance – configure TLS



Click "OK".

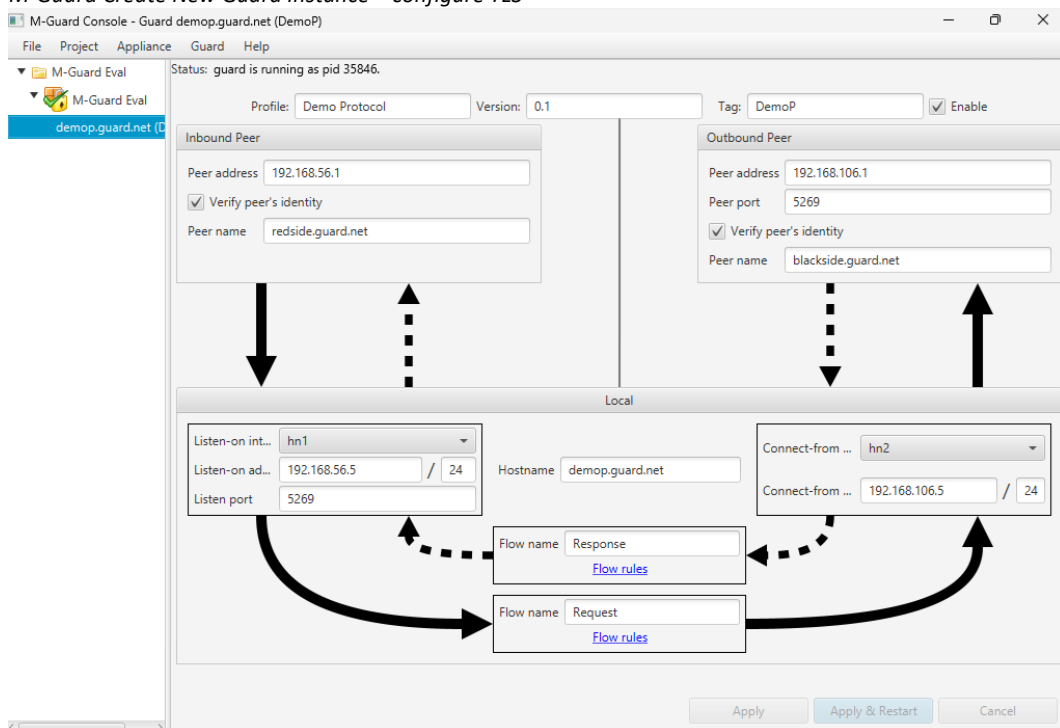
The Following is displayed.

M-Guard Create New Guard Instance – configure TLS



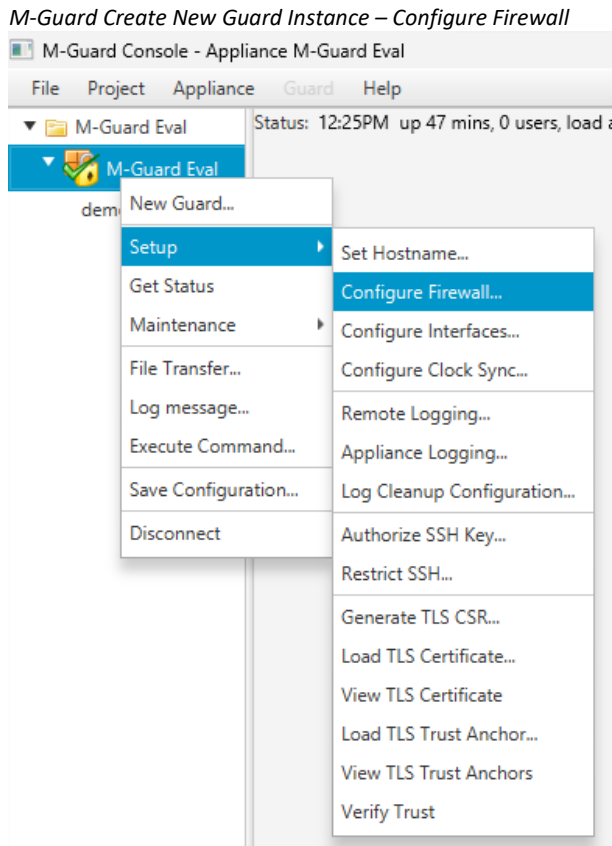
Check the "Enable" Checkbox, this will ensure the Guard Instance automatically starts on reboot. Click "Apply & Start".

M-Guard Create New Guard Instance – configure TLS

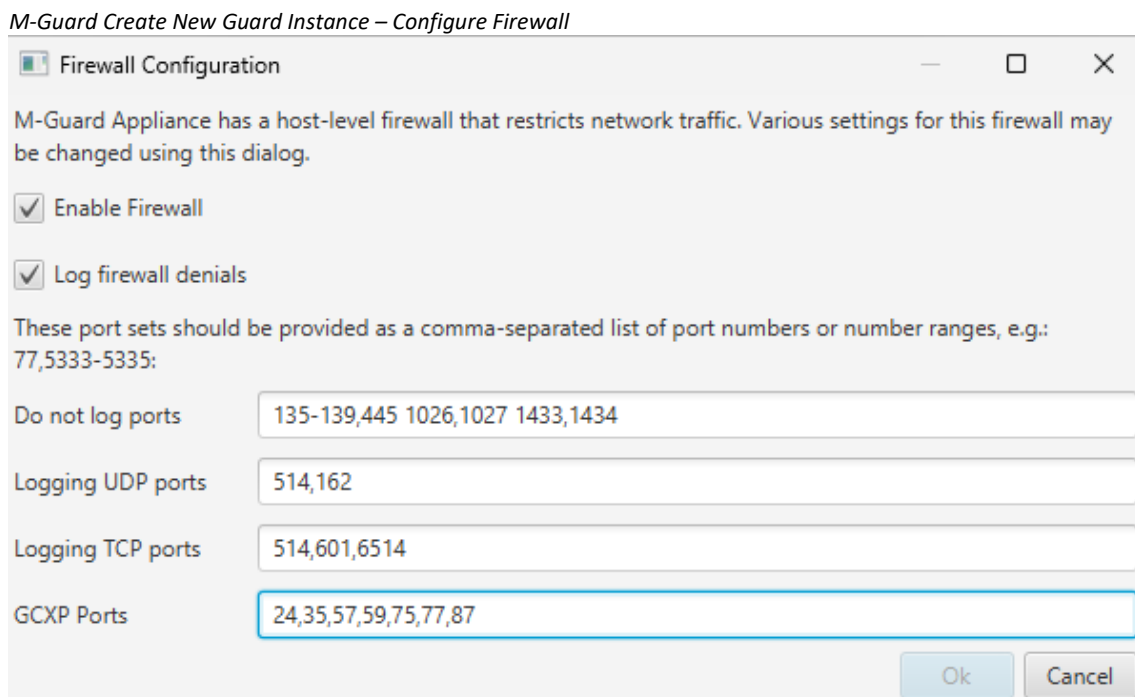


Save Configuration.

We now need to configure the Firewall on the Appliance select Setup→Configure Firewall...

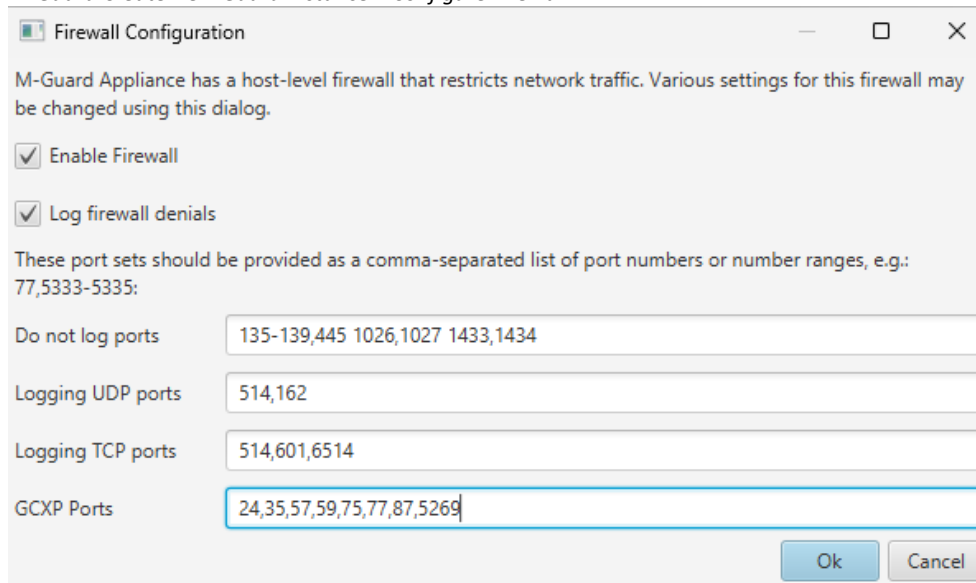


The following is displayed.



Add the GCXP Ports for your configured ports (5269 in our example).

M-Guard Create New Guard Instance – Configure Firewall

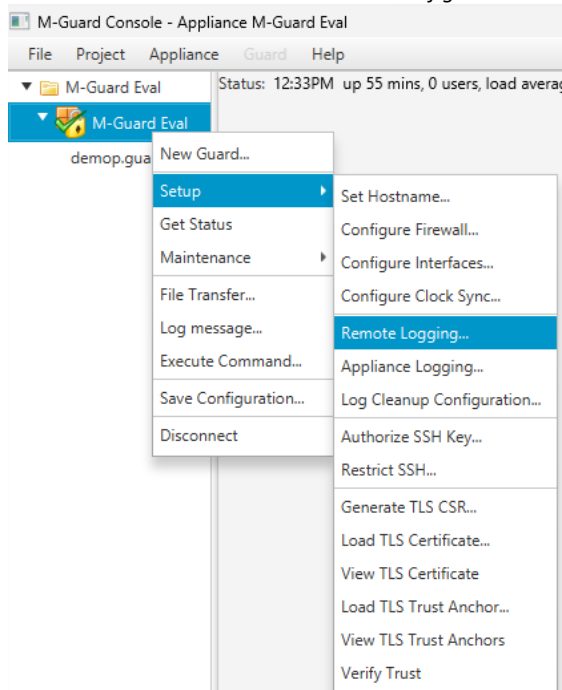


Click "OK".

Now we need to configure the “Syslog” logging. You should have installed and started the Visual Syslog Server on the Host Machine before starting this step.

Select Appliance→Setup→Remote Logging...

M-Guard Create New Guard Instance – Configure Remote Logging



The following is displayed.

M-Guard Create New Guard Instance – Configure Remote Logging

Remote Logging Configuration

The M-Guard Appliance can be configured to send its logging information to a remote logging server.

Selector:

Protocol/Transport:

Logging Server Address:

Logging Server Port:

Save Cancel

Complete as below.

M-Guard Create New Guard Instance – Configure Remote Logging

Remote Logging Configuration

The M-Guard Appliance can be configured to send its logging information to a remote logging server.

Selector:

Protocol/Transport:

Logging Server Address:

Logging Server Port:

Save Cancel

The default settings are fine but you will need to enter the IP Address of the Host Machine in the “Logging Server Address”. The Logging Server Port on Visual Syslog Server is by default 514.

Click “Save”.

Save the Configuration.

The next steps are to configure your GCXP Producer and Consumer, following the next two chapters.

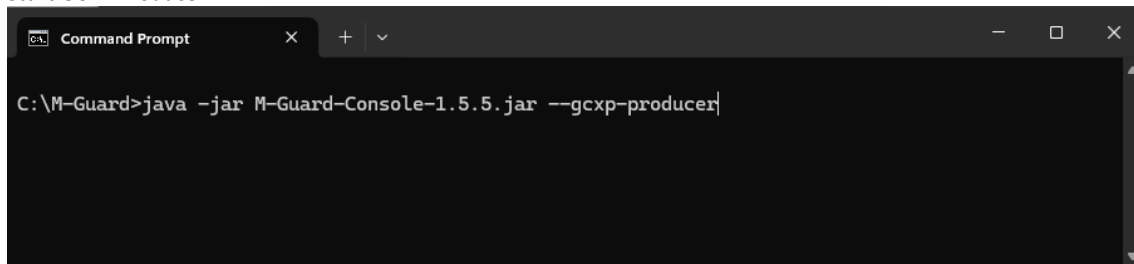
Setup up the GCXP Producer and Consumer Certificates

To test the Guard we run two custom instances of M-Guard Console that have additional command line options.

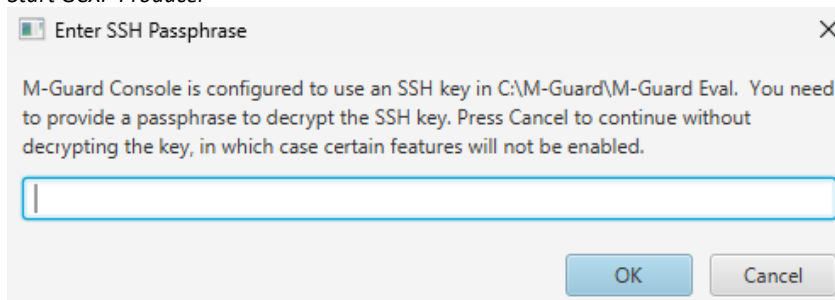
From a new “Command Prompt” navigate to the same folder that you are running M-Guard Console from and type the following command.

```
java -jar C:\Users\sales\Documents\M-Guard-Console-1.5.5.jar --gcxp-producer
```

Start GCXP Producer

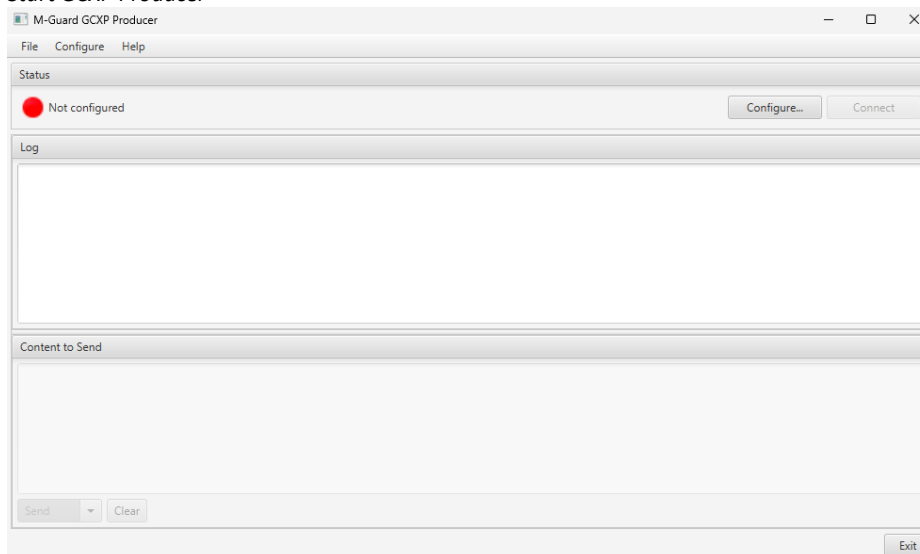


Start GCXP Producer



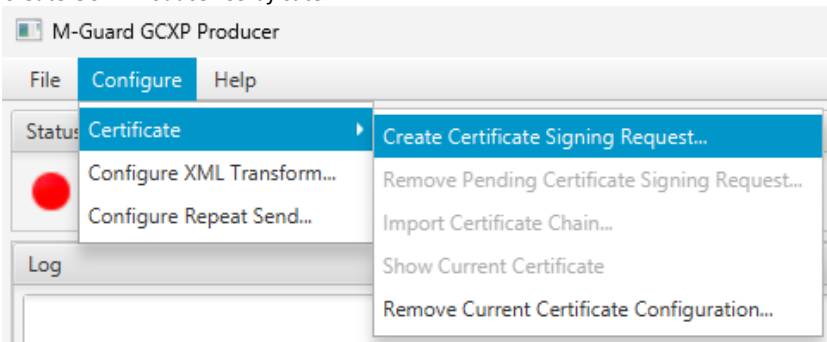
Enter the SSH Passphrase you use for M-Guard Console and Click “OK” and you should see the following screen.

Start GCXP Producer



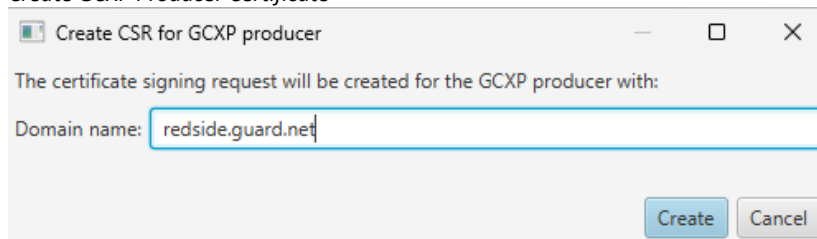
Click “Configure → Certificate → Create Certificate Signing Request...”

Create GCXP Producer Certificate



The following is displayed.

Create GCXP Producer Certificate

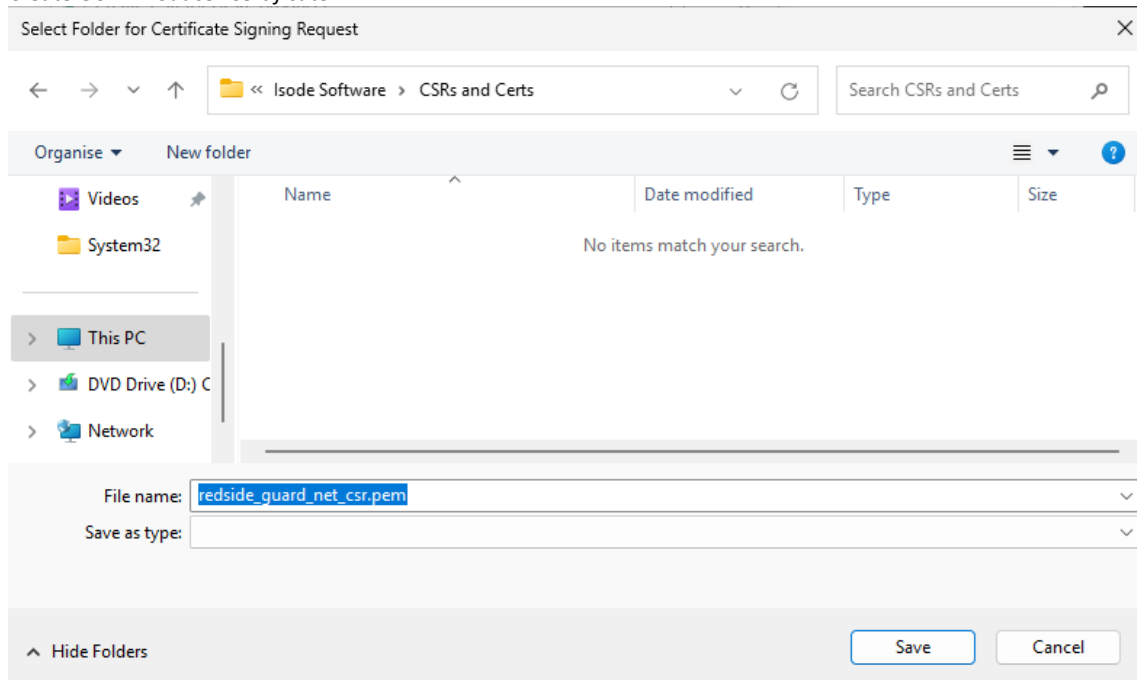


Use in our example "redside.guard.net".

Click "Create".

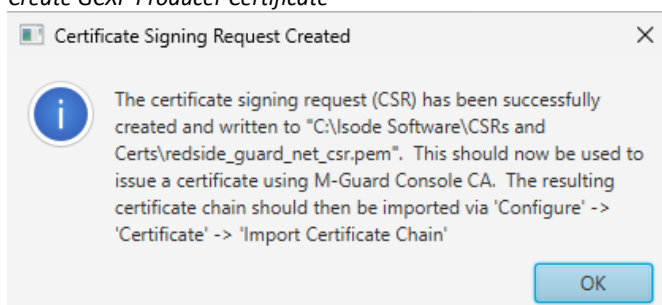
And save the request on your local disk, for example:

Create GCXP Producer Certificate



You should get a confirmation dialog of the created signing request:

Create GCXP Producer Certificate

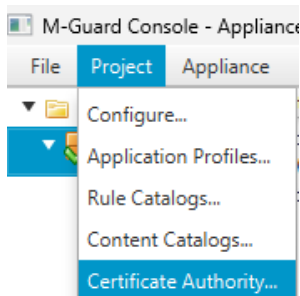


Click "OK".

At this stage, we can go back to M-Guard Console to process the CSR and issue the certificate for the Producer.

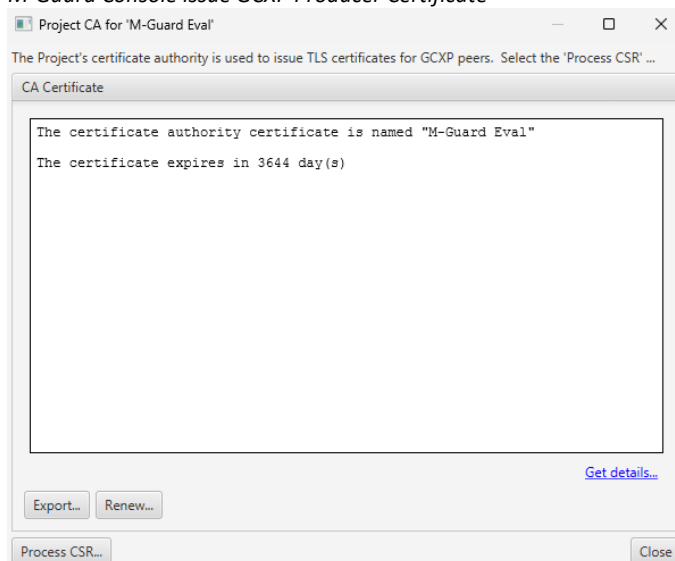
On the M-Guard Console, click on “Project → Certificate Authority...”.

M-Guard Console issue GCXP Producer Certificate



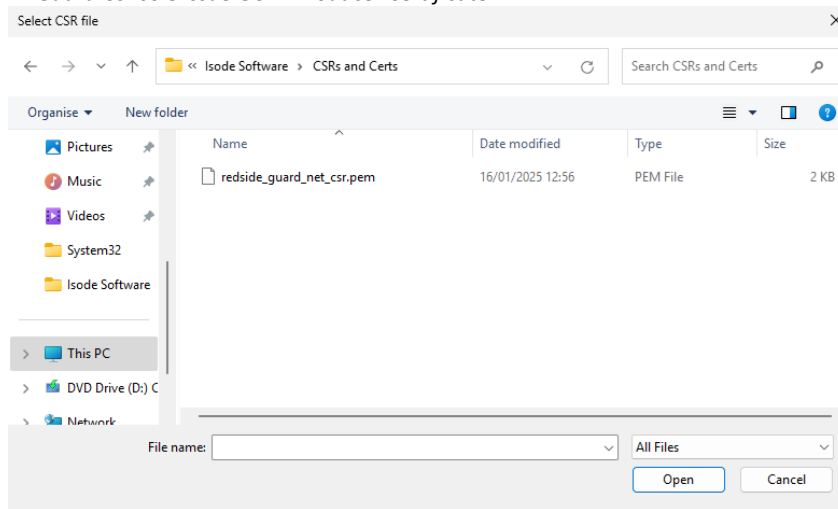
The following is displayed.

M-Guard Console issue GCXP Producer Certificate



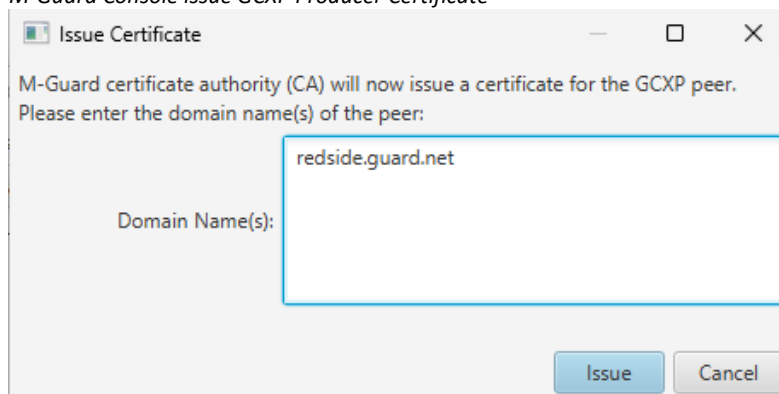
Click on the “Process CSR...” button and navigate where you saved the request from the producer.

M-Guard Console issue GCXP Producer Certificate



Select the CSR File and Click “Open”.

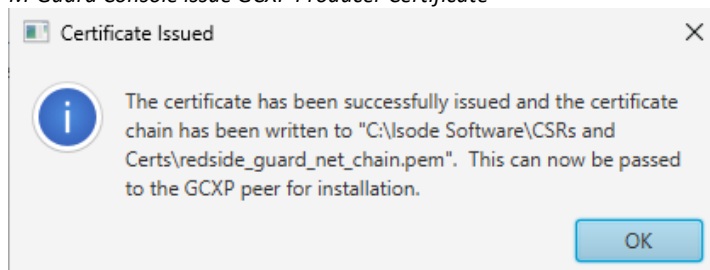
M-Guard Console issue GCXP Producer Certificate



M-Guard Console will show you the Domain Name(s) of the peer for which the certificate will be issued:

Once you click on “Issue”, the certificate will be generated and the following confirmation dialog should appear:

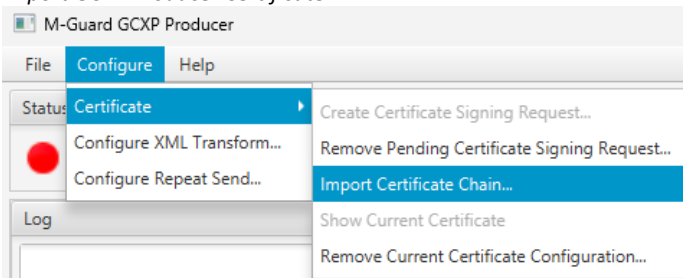
M-Guard Console issue GCXP Producer Certificate



Click "OK".

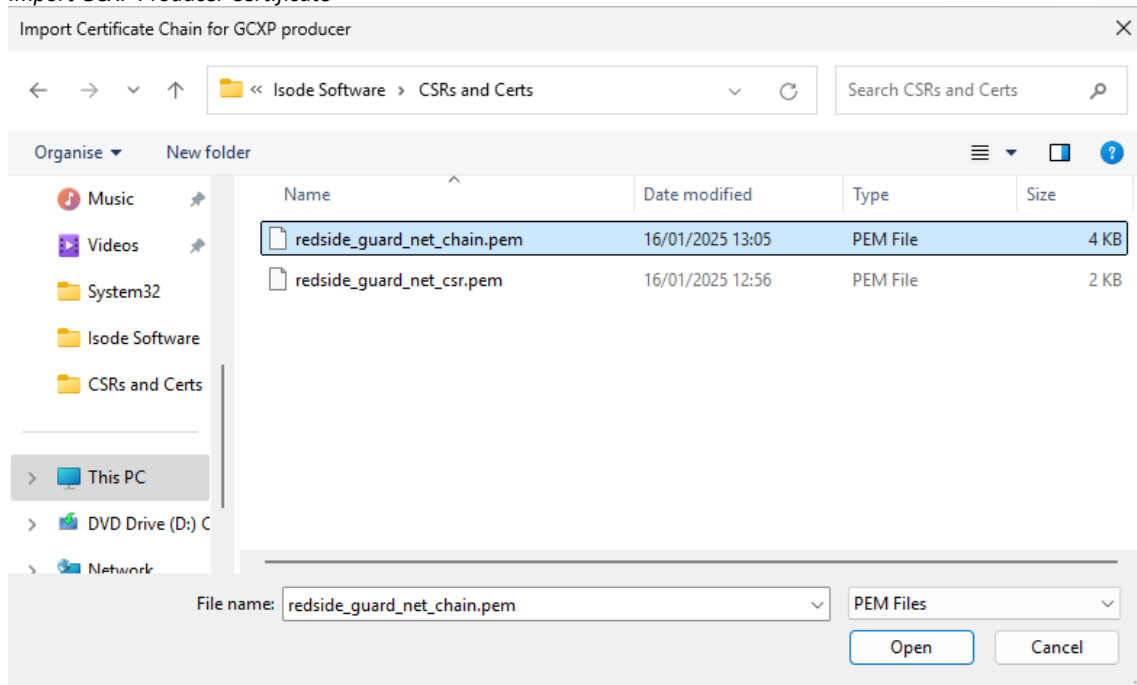
Now go back to your GCXP Producer and import the certificate chain. Click on “Configure → Certificate → Import Certificate Chain...”

Import GCXP Producer Certificate



This will show you a dialog to navigate to the location the M-Guard Console saved the Certificate .pem file.

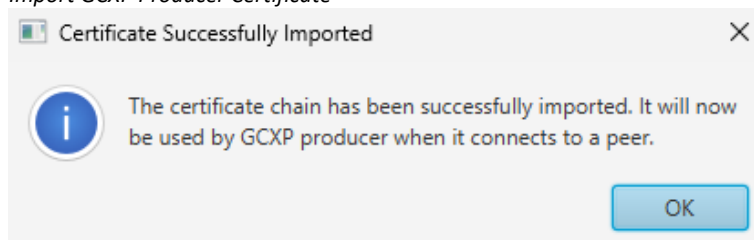
Import GCXP Producer Certificate



Select the “chain” file and not the “csr” file and Click “Open”.

A confirmation dialog confirming the successful import of the chain will be displayed:

Import GCXP Producer Certificate



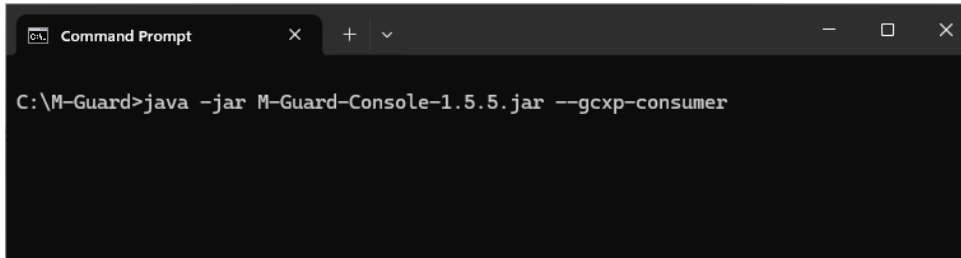
Click "OK"

Now we need to repeat the exact same steps but for the GCXP Consumer.

From a new “Command Prompt” navigate to the same folder that you are running M-Guard Console from and type the following command.

```
java -jar M-Guard-Console-1.5.5.jar --gcxp-consumer
```

Start GCXP Consumer



As before, enter the SSH Passphrase you use for M-Guard Console and Click “OK” and you should see the screen below.

We are not going to show all the steps for this.

Follow the exact same steps used before to create the certificate request for the GCXP Producer with “Configure → Certificate → Create Certificate Signing Request...”, making sure that now the Domain Name is going to be “blackside.guard.net”.

Similarly, use M-Guard Console’s “Project → Certificate Authority...” to issue the certificate for this request from the consumer.

And finally, back to the GCXP Consumer, import the issued certificate for “blackside.guard.net” with “Configure → Certificate → Import Certificate Chain...”

You are now in a position to configure the GCXP Producer and the GCXP Consumer to start sending and receiving messages.

Configure GCXP Producer and Consumer

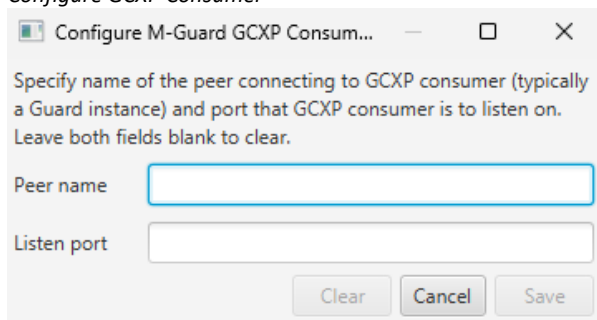
First step before sending messages is to make the GCXP Consumer listen for those messages. Go back to the GCXP Consumer.

Configure GCXP Consumer



Click on the “Configure...” button:

Configure GCXP Consumer



Fill in the details for the peer connecting to the consumer as specified in the M-Guard Appliance we set up with M-Guard Console. In our case, these are:

Configure GCXP Consumer

Specify name of the peer connecting to GCXP consumer (typically a Guard instance) and port that GCXP consumer is to listen on. Leave both fields blank to clear.

Peer name

Listen port

Click on “Save”.

Configure GCXP Consumer

M-Guard GCXP Consumer

File Configure Help

Status

Ready to listen for peer demop.guard.net

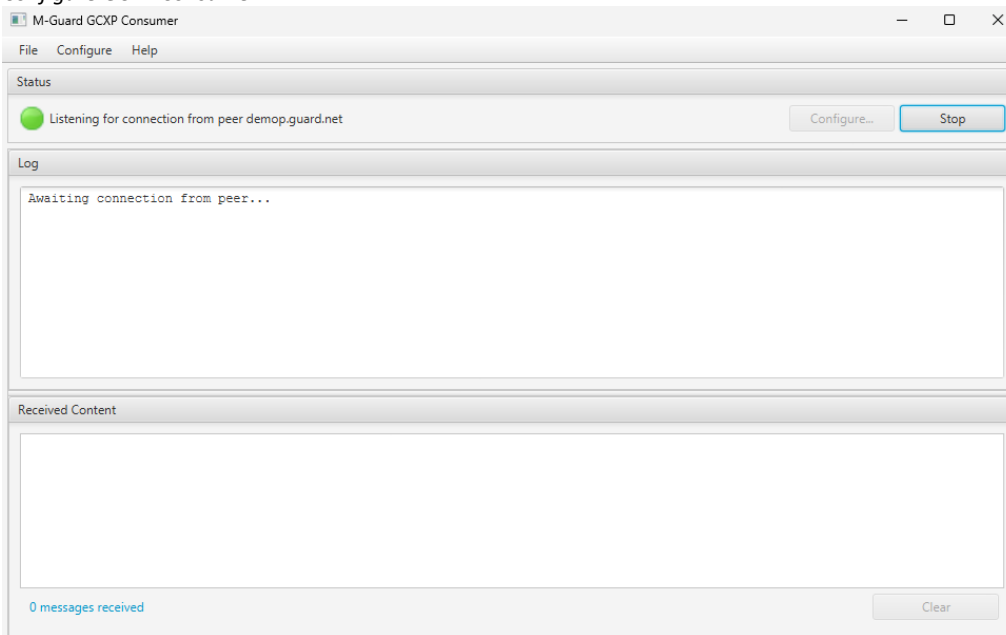
Log

Received Content

0 messages received

Click “Listen”.

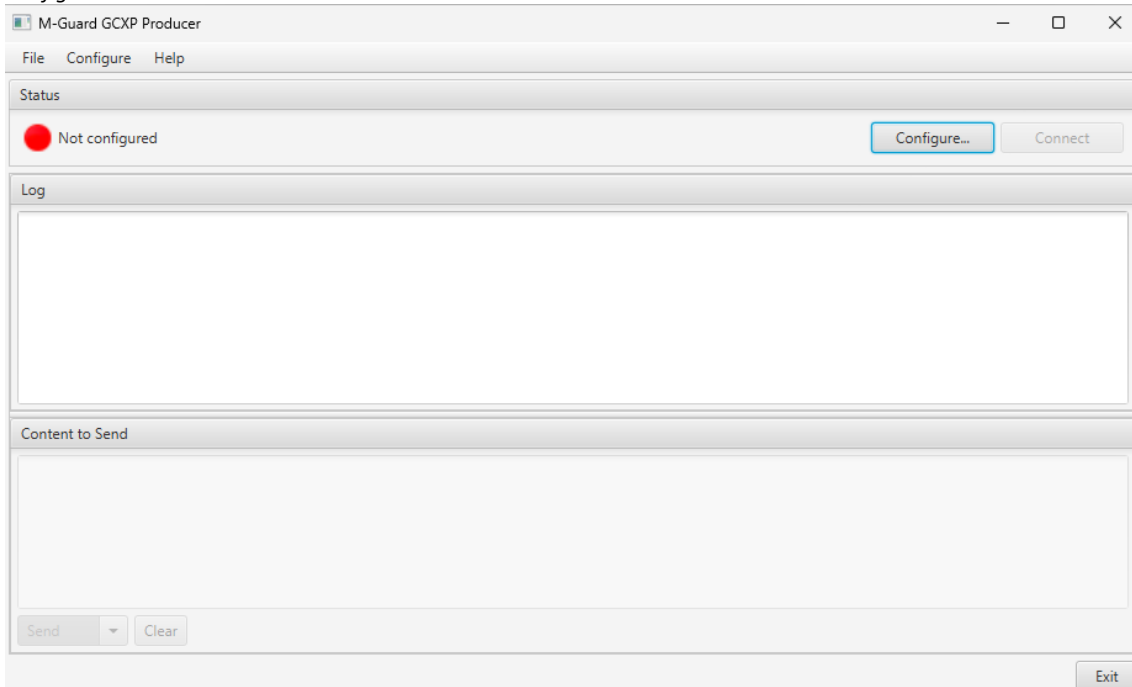
Configure GCXP Consumer



The Consumer is now successfully connected to the M-Guard Instance and is awaiting a connection from the Producer.

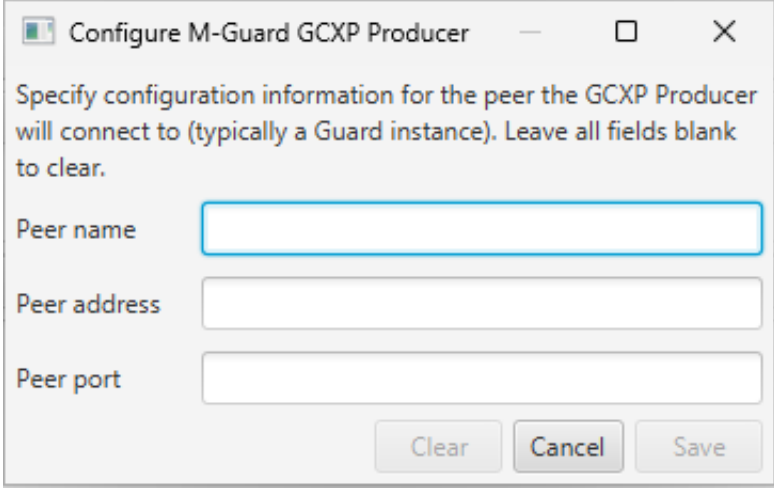
Now, go back to the GCXP Producer, and similarly, click on the “Configure...” button:

Configure GCXP Producer



Click on the “Configure...” button:

Configure GCXP Producer



Configure M-Guard GCXP Producer

Specify configuration information for the peer the GCXP Producer will connect to (typically a Guard instance). Leave all fields blank to clear.

Peer name

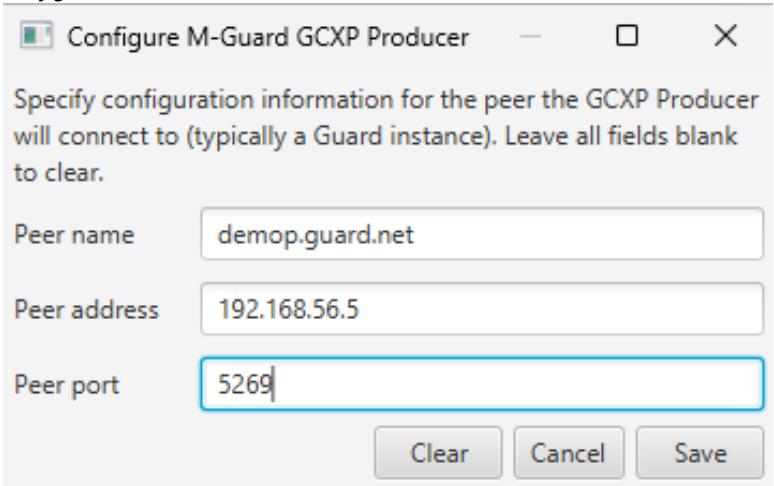
Peer address

Peer port

Clear Cancel Save

Fill with the details for the peer the producer will connect to as specified in the M-Guard Appliance we set up with M-Guard Console. In our case, these are:

Configure GCXP Producer



Configure M-Guard GCXP Producer

Specify configuration information for the peer the GCXP Producer will connect to (typically a Guard instance). Leave all fields blank to clear.

Peer name

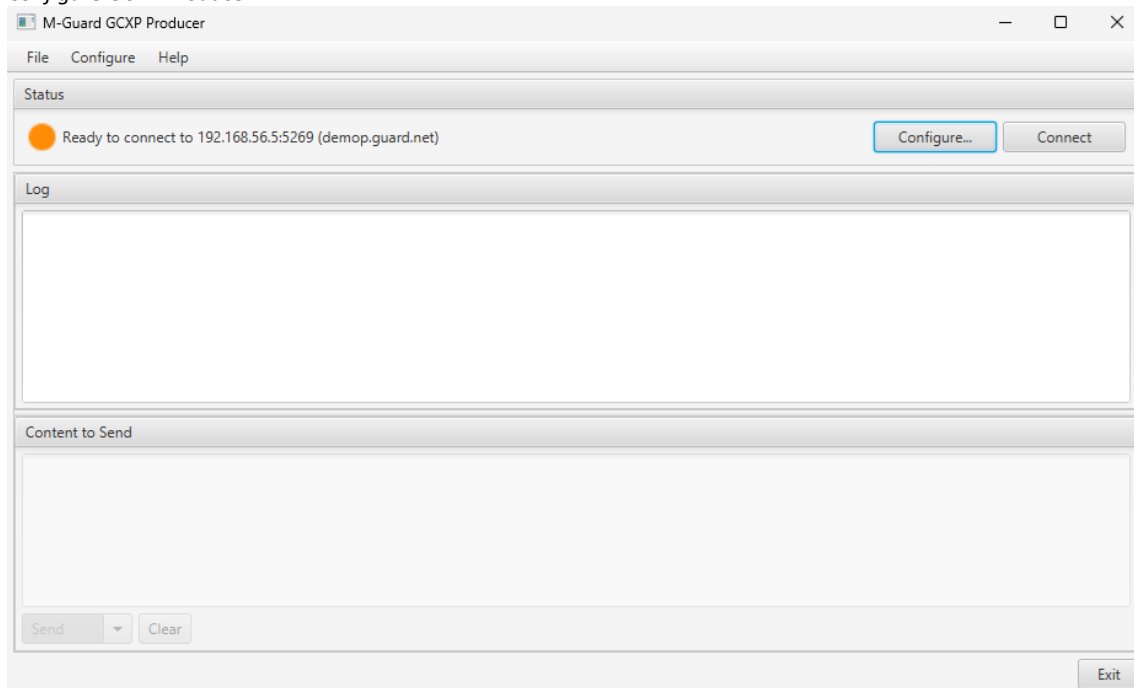
Peer address

Peer port

Clear Cancel Save

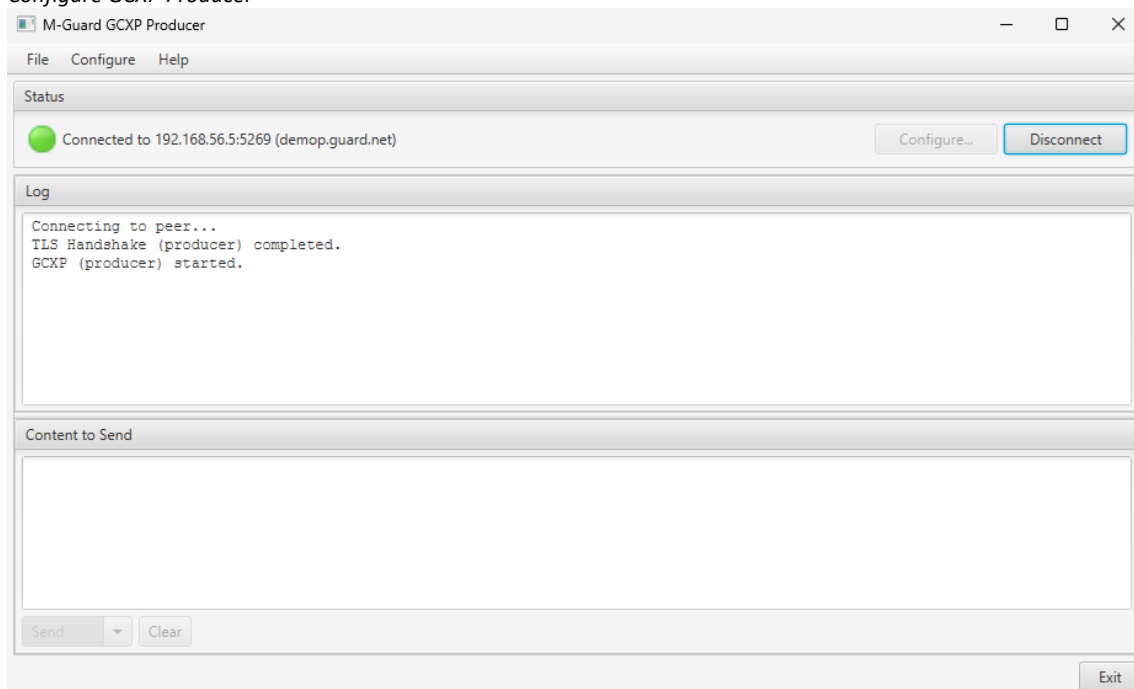
Click "Save"

Configure GCXP Producer



Click on the “Connect...” button

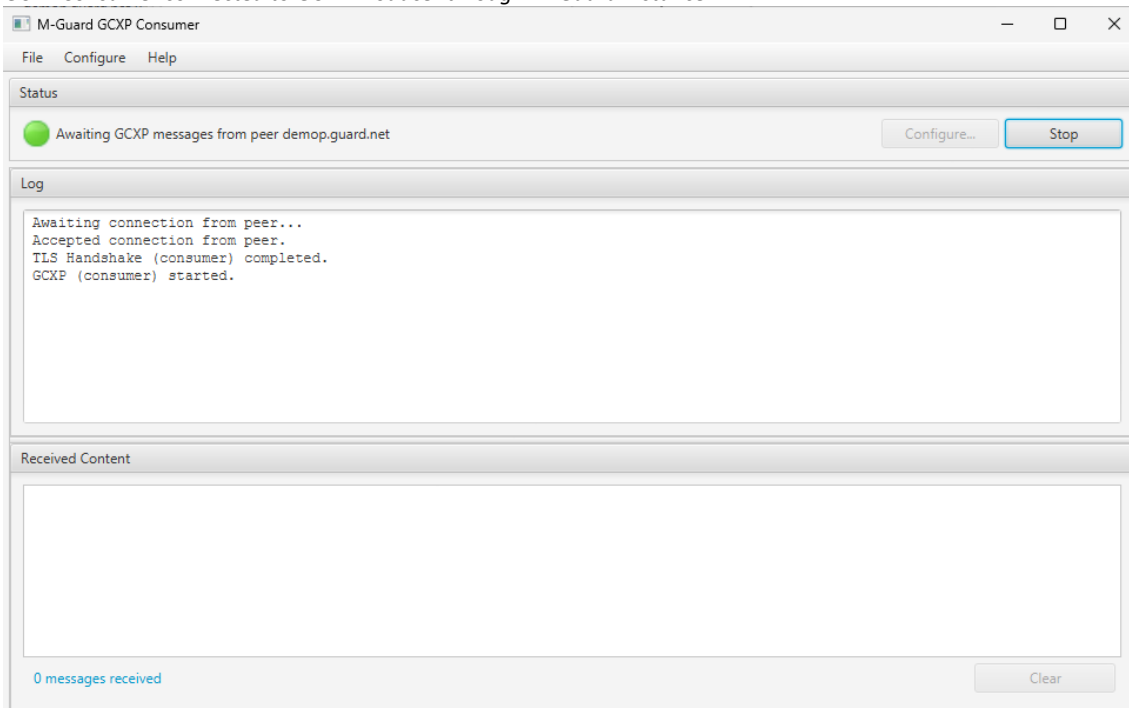
Configure GCXP Producer



This will establish a connection with the GCXP Consumer through the M-Guard Instance:

Similarly, the GCXP Consumer at this stage will show that the TLS Handshake is also completed:

GCXP Consumer connected to GCXP Producer through M-Guard Instance

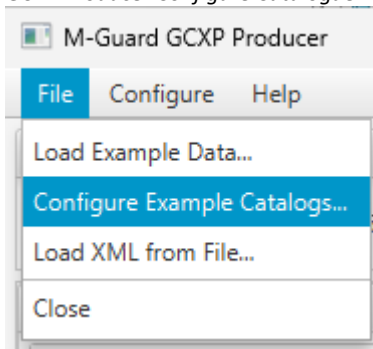


Send messages between GCXP Producer and Consumer

As we have configured an M-Guard Appliance based on the “DemoP protocol” profile, we will first need to load the example messages for this profile.

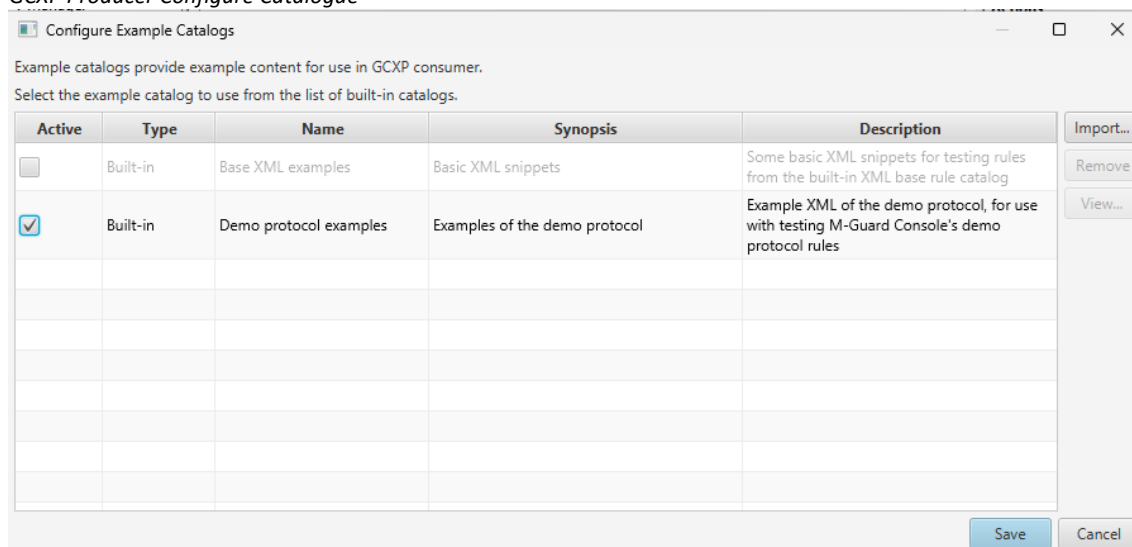
On the GCXP Producer application, click on “Configure Example Catalogs...”

GCXP Producer Configure Catalogue



The following will be displayed.

GCXP Producer Configure Catalogue

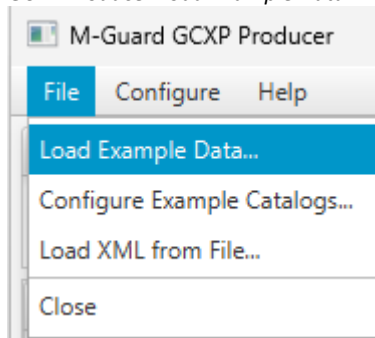


Enable the Built-in “Demo protocol examples” option.

Click “Save”.

Select “File → Load Example Data...”

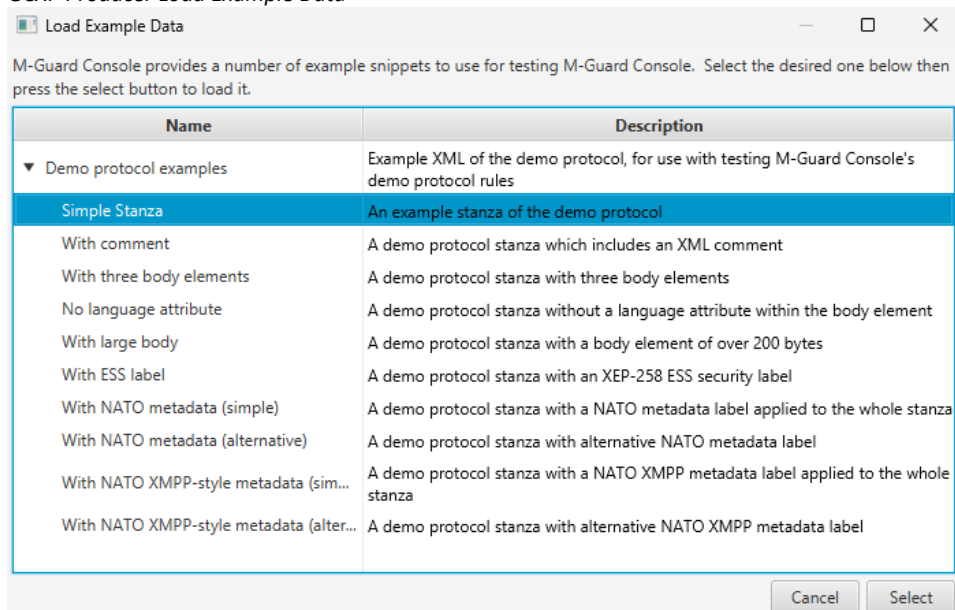
GCXP Producer Load Example Data



Expand "Demo Protocol Examples"

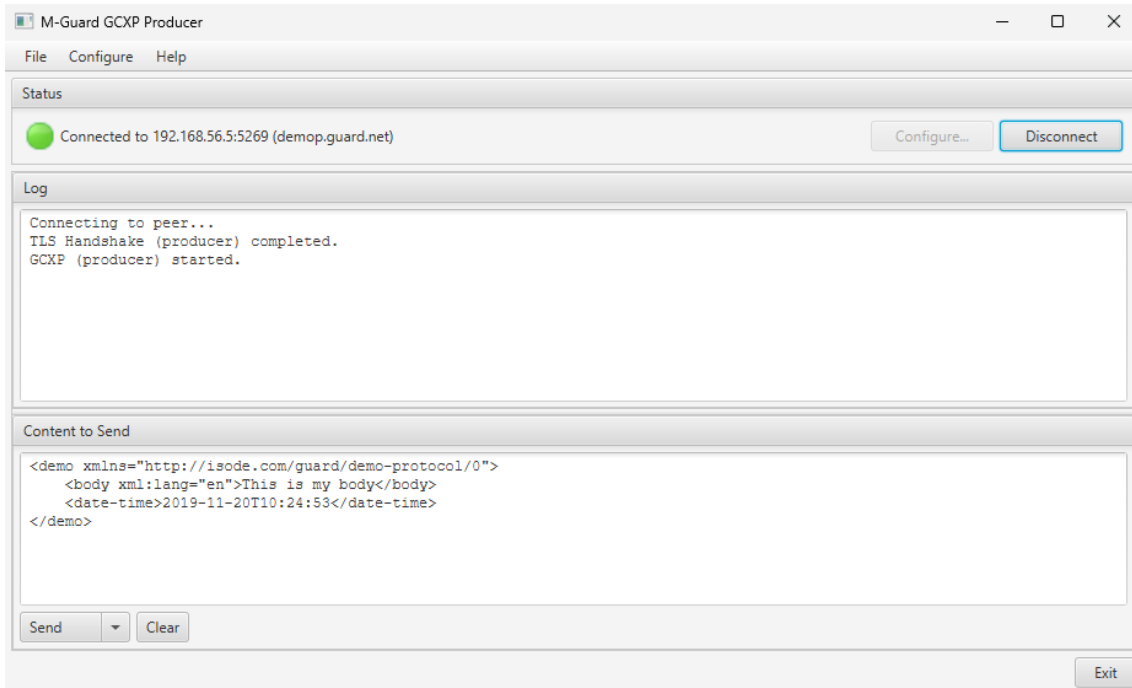
The following is displayed.

GCXP Producer Load Example Data



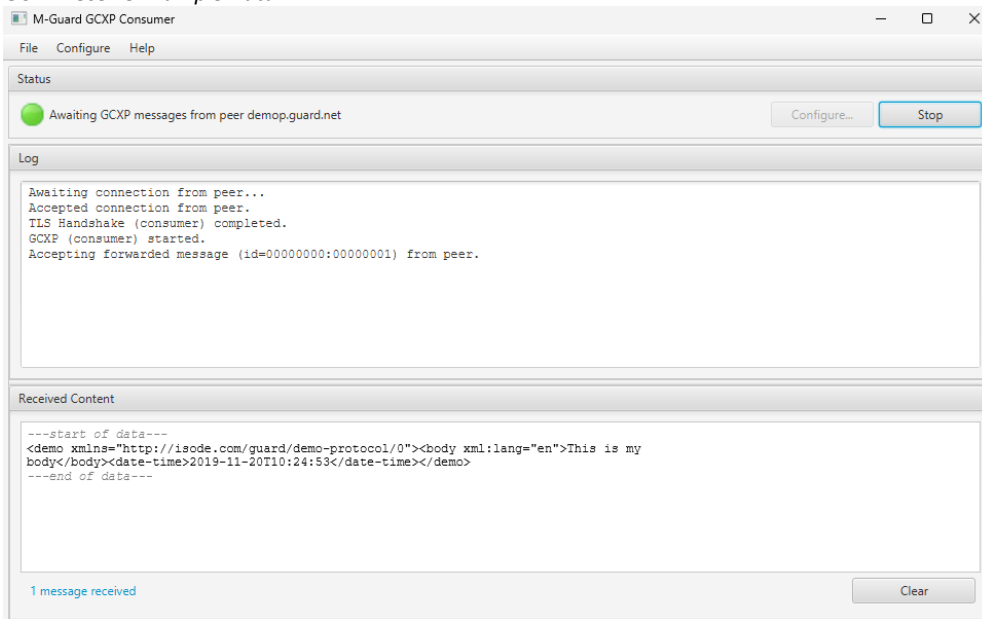
Select “Simple Stanza”

GCXP Producer Load Example Data



This simple stanza will be loaded into the dialog, and you can then Click on “Send” to send it to the GCXP Consumer. Look at the GCXP Consumer

GCXP Receive Example Data

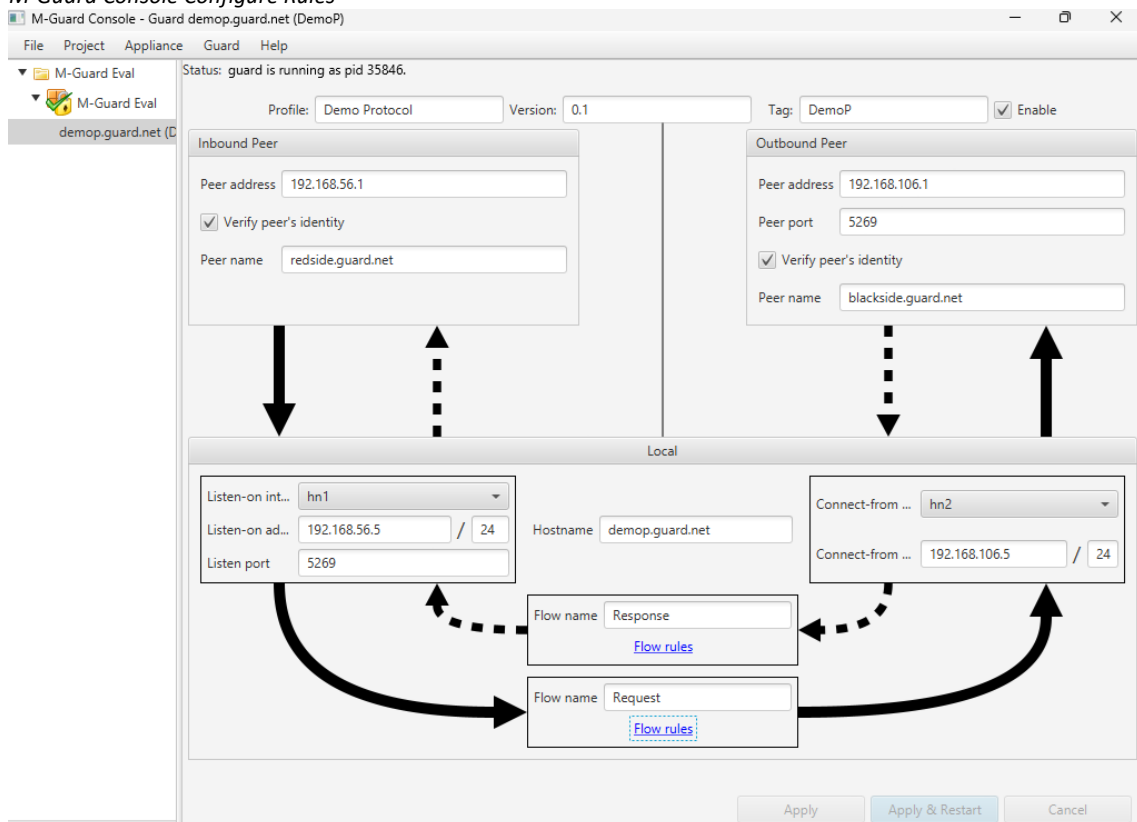


Your Guard is successfully passing Data.

Now to test some Rules.

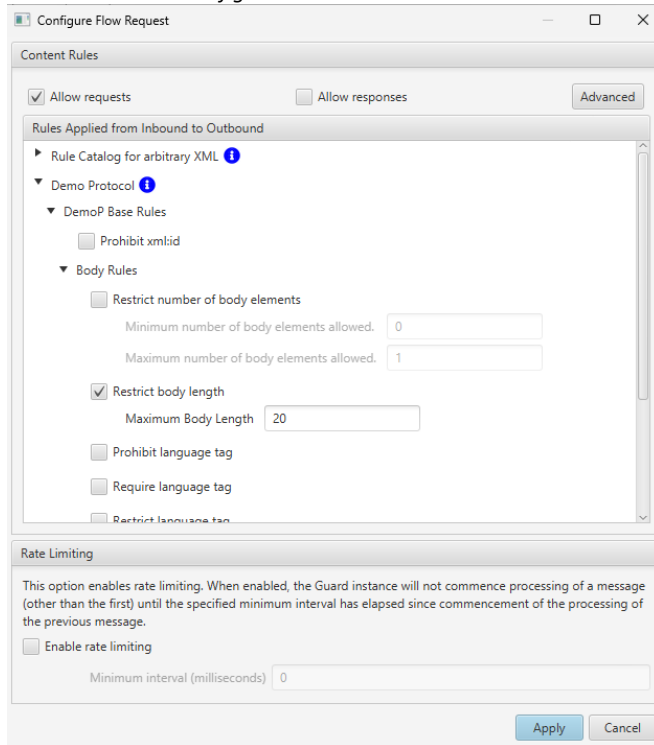
Return to M-Guard Console and select the Guard.

M-Guard Console Configure Rules



Select the "Flow rules" for from Inbound to Outbound.

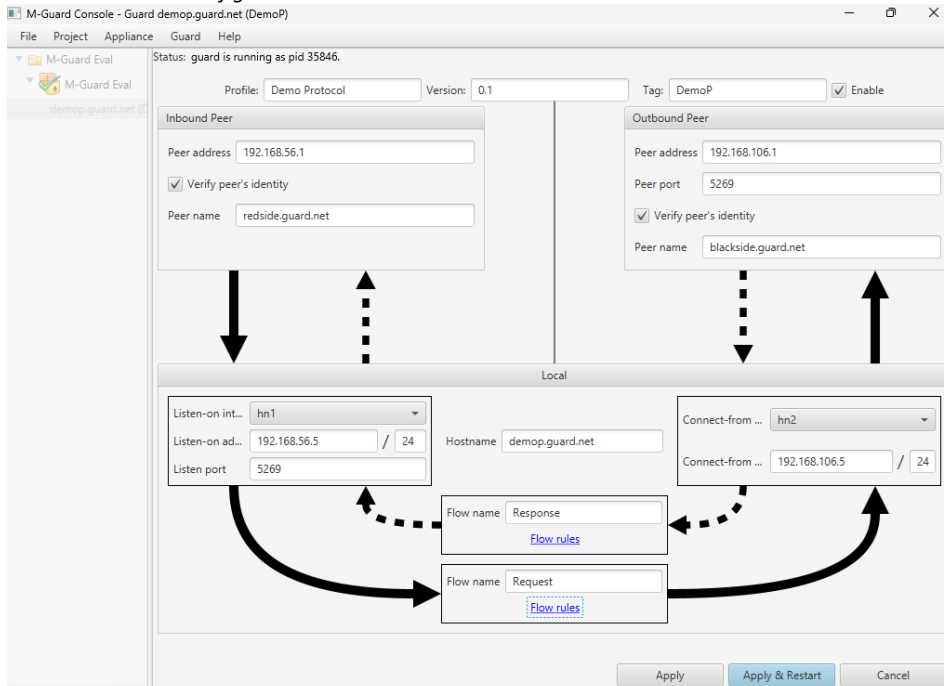
M-Guard Console Configure Rules



Expand the “DemoP Base Rules” and then the “Body Rules”. A simple test of the guard is to set the “Restrict body length” to a low number e.g. 20.

Click “Apply”.

M-Guard Console Configure Rules

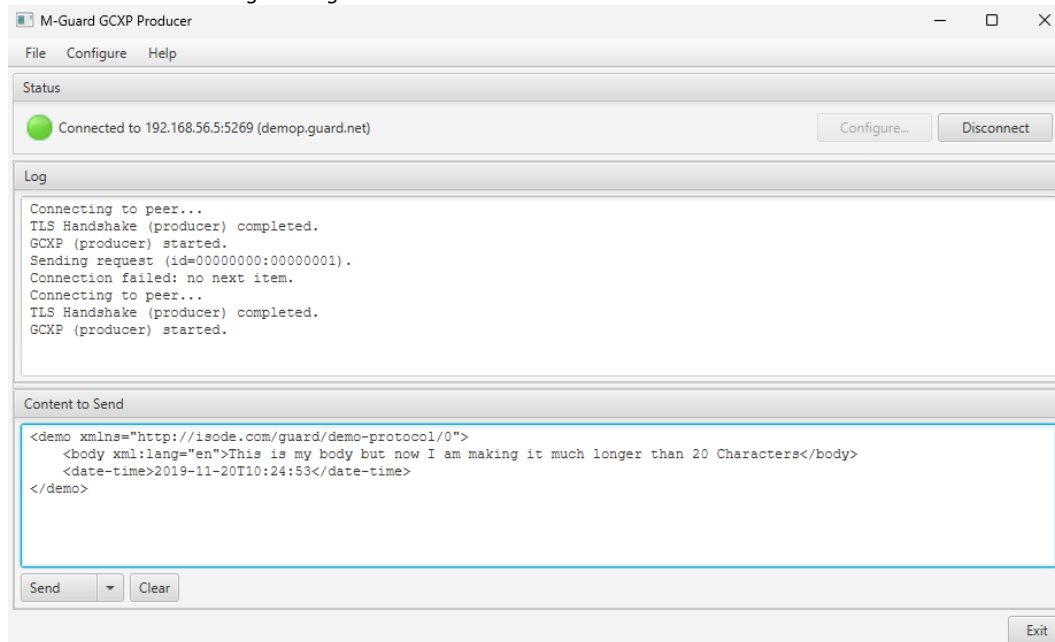


Then click on “Apply & Restart” on the Guard:

As the Guard Appliance will have restarted, you will need to also restart both the GCXP Consumer and Producer, ie, via “Stop” and “Listen” buttons on the Consumer, and the “Retry” button on the Producer.

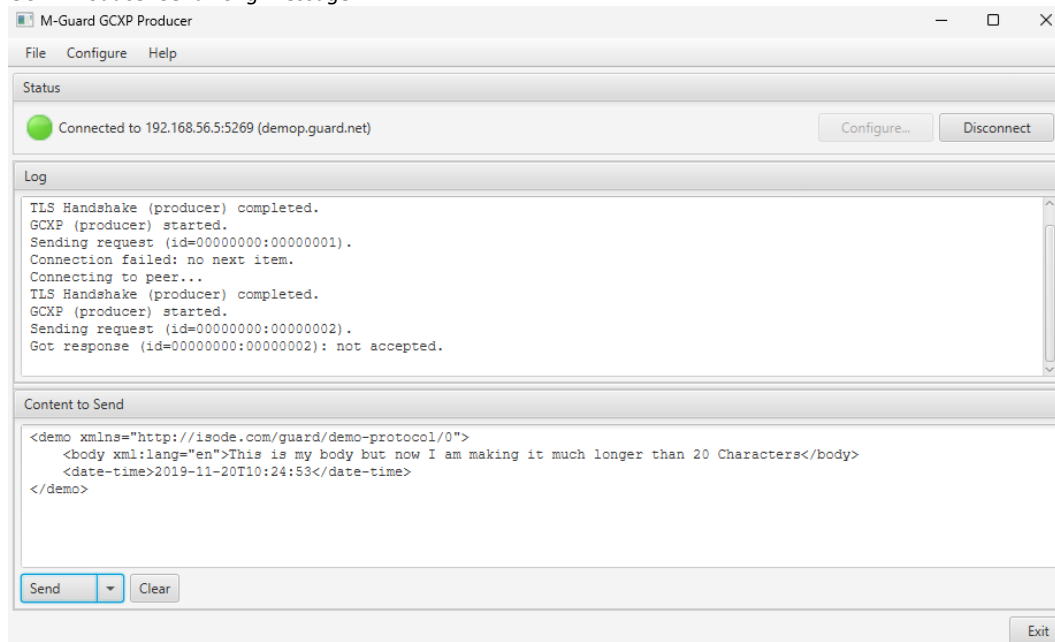
Load the Example Data as before on the Producer but edit the “Body Text” to make it much longer (over 20 characters).

GCXP Producer Send Long Message



Click “Send”.

GCXP Producer Send Long Message



You will note on the Producer that the message has been blocked.

Also, nothing is received on the Consumer.

Additionally, an “Alert” is received on the Syslog server.

Syslog Server Alert

Time	IP	Host	Facility	Priority	Tag	Message
Jan 16 13:32:57	10.178.0.2	demop.guard.net	daemon	notice	DemoP[35847] blackside.guard.net	start
Jan 16 13:45:50	10.178.0.2	demop.guard.net	daemon	info	DemoP[35847] redside.guard.net Pas	message id=00000000:00000001 type=Request: okay
Jan 16 13:45:50	10.178.0.2	demop.guard.net	daemon	debug	DemoP[35847] blackside.guard.net	deliver id=00000000:00000001 type=Request
Jan 16 13:45:50	10.178.0.2	demop.guard.net	daemon	debug	DemoP[35847] blackside.guard.net	write complete, queue empty
Jan 16 14:04:51	10.178.0.2	demop.guard.net	daemon	notice		DemoP[35847] M-Guard stopped
Jan 16 14:04:52	10.178.0.2	demop.guard.net	daemon	notice		DemoP[64605] M-Guard running
Jan 16 14:04:52	10.178.0.2	demop.guard.net	daemon	notice	DemoP[64605] dst	192.168.106.1:5269 (blackside.guard.net)
Jan 16 14:04:52	10.178.0.2	demop.guard.net	daemon	notice	DemoP[64605] src	192.168.56.5:5269 (redside.guard.net)
Jan 16 14:04:52	10.178.0.2	demop.guard.net	daemon	notice		DemoP[64605] Accepting on 192.168.56.5:5269 (redside.guard
Jan 16 14:06:30	10.178.0.2	demop.guard.net	daemon	notice		DemoP[64605] Incoming connection from 192.168.56.1:51895 o
Jan 16 14:06:30	10.178.0.2	demop.guard.net	daemon	debug		DemoP[64605] Incoming connection accepted, proceeding with T
Jan 16 14:06:30	10.178.0.2	demop.guard.net	daemon	debug		DemoP[64605] Incoming connection TLS negotiation successful.
Jan 16 14:06:30	10.178.0.2	demop.guard.net	daemon	notice		DemoP[64605] Connecting to 192.168.106.1:5269 (blackside.gu
Jan 16 14:06:30	10.178.0.2	demop.guard.net	daemon	debug		DemoP[64605] Outgoing connection TLS negotiation successful.
Jan 16 14:06:30	10.178.0.2	demop.guard.net	daemon	notice	DemoP[64605] redside.guard.net	start
Jan 16 14:06:30	10.178.0.2	demop.guard.net	daemon	notice	DemoP[64605] blackside.guard.net	start
Jan 16 14:08:09	10.178.0.2	demop.guard.net	daemon	alert		DemoP[64605] redside.guard.net Content Alert - reject (Drop):
Jan 16 14:08:09	10.178.0.2	demop.guard.net	daemon	debug	DemoP[64605] redside.guard.net	deliver id=00000000:00000002 type=Response
Jan 16 14:08:09	10.178.0.2	demop.guard.net	daemon	debug	DemoP[64605] redside.guard.net	write complete, queue empty

Your Guard is now working to Block some “Content” and to Allow other “Content” through.

You can confirm that the original message still goes through by reducing the message length to the original and sending it. It will be received by the Consumer and there will be no Alert on the Syslog Server.

You can now configure other Guard Instances by following the instructions in the appropriate Evaluation Guides such as Red Black.

What Next?

More information on M-Guard can be found on the Isode website at <https://www.isode.com/product/xml-guard/>.

Whitepapers

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

Copyright

The Isode Logo and Isode are trade and service marks of Isode Limited.

All products and services mentioned in this document are identified by the trademarks or service marks of their respective companies or organizations, and Isode Limited disclaims any responsibility for specifying which marks are owned by which companies or organizations.

Isode software is © copyright Isode Limited 2002-2025, All rights reserved.

Isode software is a compilation of software of which Isode Limited is either the copyright holder or licensee. Acquisition and use of this software and related materials for any purpose requires a written licence agreement from Isode Limited, or a written licence from an organization licensed by Isode Limited to grant such a licence.

This manual is © copyright Isode Limited 2025.