Isode

M-Guard Evaluation Guide

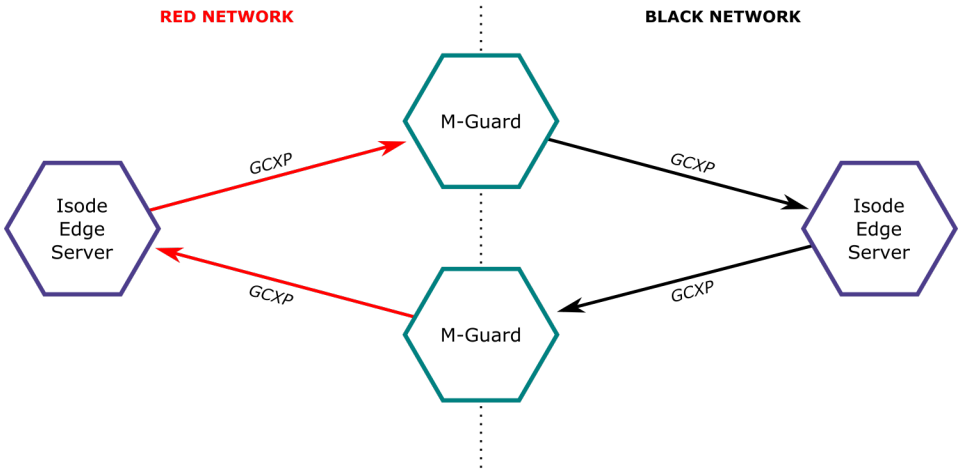
Setting up and testing Isode's XML Guard on VirtualBox or Hyper-V.

Contents

Introduction

M-Guard is an application level Data Diode that validates XML messages passing through it according to a set of rules. It will typically sit on a network security boundary e.g. Red/Black and be configured as a pair such that data in both directions can be validated. There can be different rules for Red→Black & Black→Red. M-Guard communicates using Guard Content eXchange Protocol (GCXP) as a secure protocol for communicating XML messages between M-Guard and processes on either side. Image 1 shows a typical deployment configuration.

Image 1: Typical Deployment Configuration



More information on M-Guard can be found at *www.isode.com/products/m-guard.html*.

Objectives

At the end of this evaluation you will have:

- Created an M-Guard Appliance on either VirtualBox or Hyper V.
- Created a "Guard Instance" for "Red to Black" on this M-Guard Appliance.
- Configured some "Basic Rules" for this "Guard Instance".
- Tested these rules using Isode Test Tools gcxp-producer and gcxp-consumer.
- Seen Alerts on the Syslog Server.

For the purposes of this evaluation the Host Operating System for running the Virtualization Software (Virtual Box or Hyper V), M-Guard Console & the Syslog Server will be Windows 10.

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.

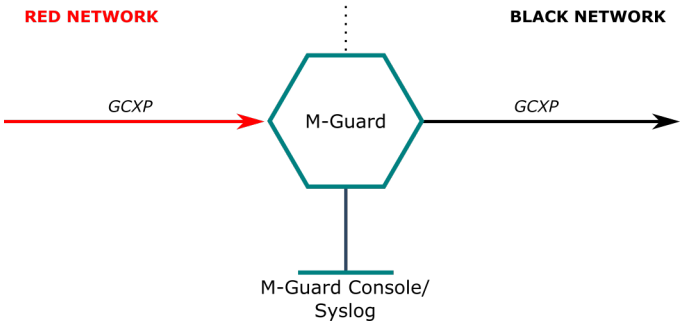
Preparation

M-Guard is available in the following formats:

- Hardware Appliance based on the Intel Atom processor.
- Oracle VirtualBox virtual machine.
- Microsoft Hyper-V virtual machine.

This guide covers Oracle VirtualBox and Microsoft Hyper-V installations. M-Guard is configured and managed using M-Guard Console, which is a Java GUI connecting to the Appliance using TCP/IP. As such, each M-Guard needs three Network Interfaces (Image 2).

Image 2: M-Guard Network Interfaces



The Management Network is how M-Console connects to the Guard Appliance and can also be used to host a "Syslog" Server to receive alerts from M-Guard.

Network Planning

As three network interfaces are required, it is worthwhile spending some time planning the interfaces for your deployment. In this guide we will be using the following:

	Red	Management	Black
VirtualBox NIC	VirtualBox Host Only Ethernet Adaptor #2	VirtualBox Host Only Ethernet Adaptor	VirtualBox Host Only Ethernet Adaptor #3
Hyper-V NIC	Red Network	M-Guard Management	Black Network
Host Machine IP	10.178.0.1	192.168.56.1	192.168.106.1
M-Guard IP	10.178.0.2	192.168.56.2	192.168.106.2
Netmask	255.255.255.0	255.255.255.0	255.255.255.0

Product Downloads

You will be given instructions on where to obtain the downloads you'll need for this evaluation.

In summary you should download and install the following:

- Microsoft Visual C++ Redistributable 2015
- Isode OpenJDK 11.0
- M-Vault R18.0 (or later)

- Visual Syslog Server

Note Network interfaces on the Appliance are em0,em1 & em2 on Virtual Box and hn0, hn1 & hn2 on Hyper-V.

In addition you should download the following:

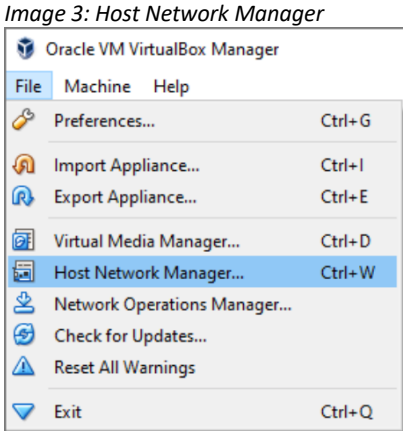
- M-Guard Appliance for VirtualBox or Hyper-V
- M-Guard console .jar file

The next two sections describe the initial installation for VirtualBox and Hyper-V.

Installation on VirtualBox

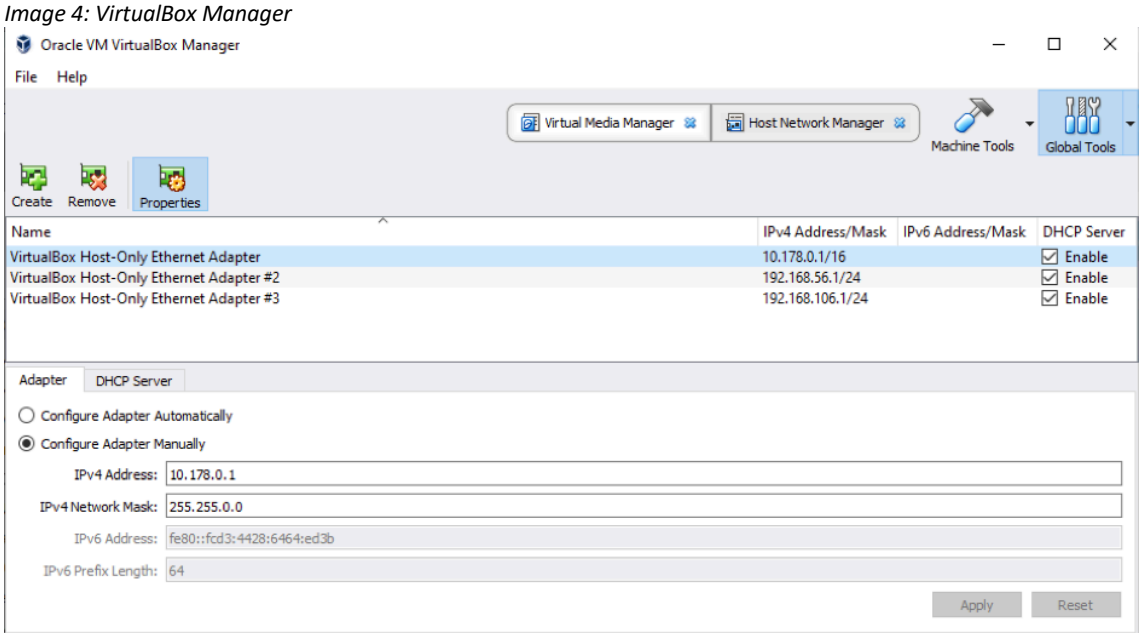
Configure the VirtualBox Host Only Networks, using “File > Host Network Manager...” from the VirtualBox Manager menu (Image 3).

Image 3: Host Network Manager



This will lead you to the screen shown in Image 4.

Image 4: VirtualBox Manager



Now select “File > Import Appliance” from the VirtualBox Manager menu and you’ll be promoted to choose a virtual appliance file to import (Image 4). Select the M-Guard Appliance file and click on [**Open**], then click on [**Import**] (Image 5).

Image 4: Select Virtual Appliance

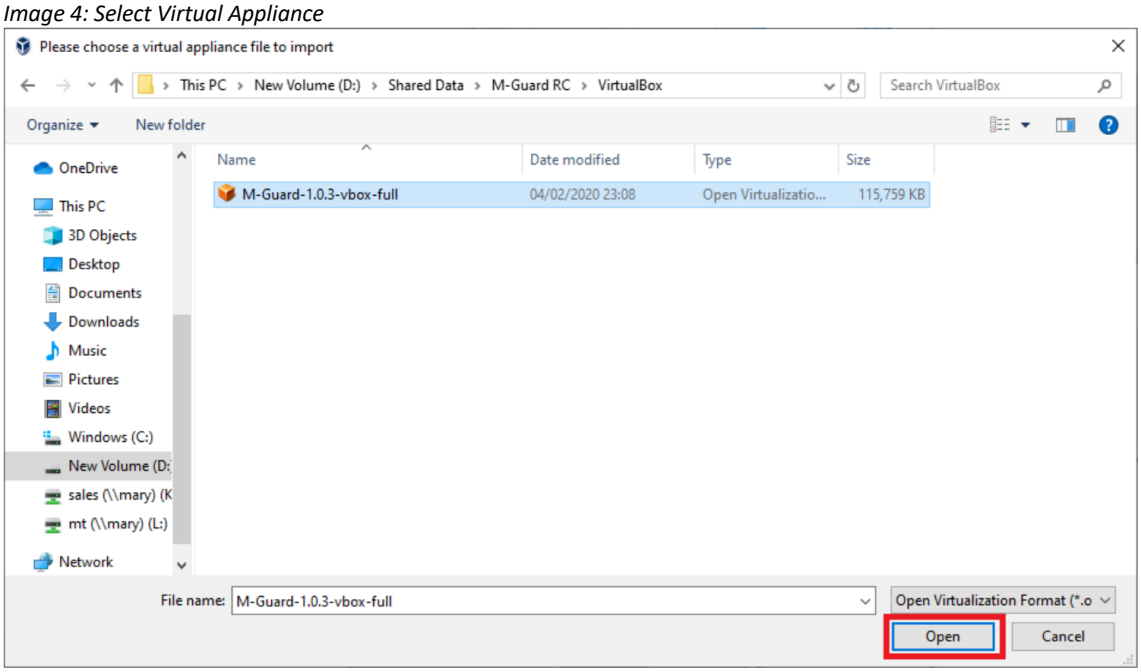
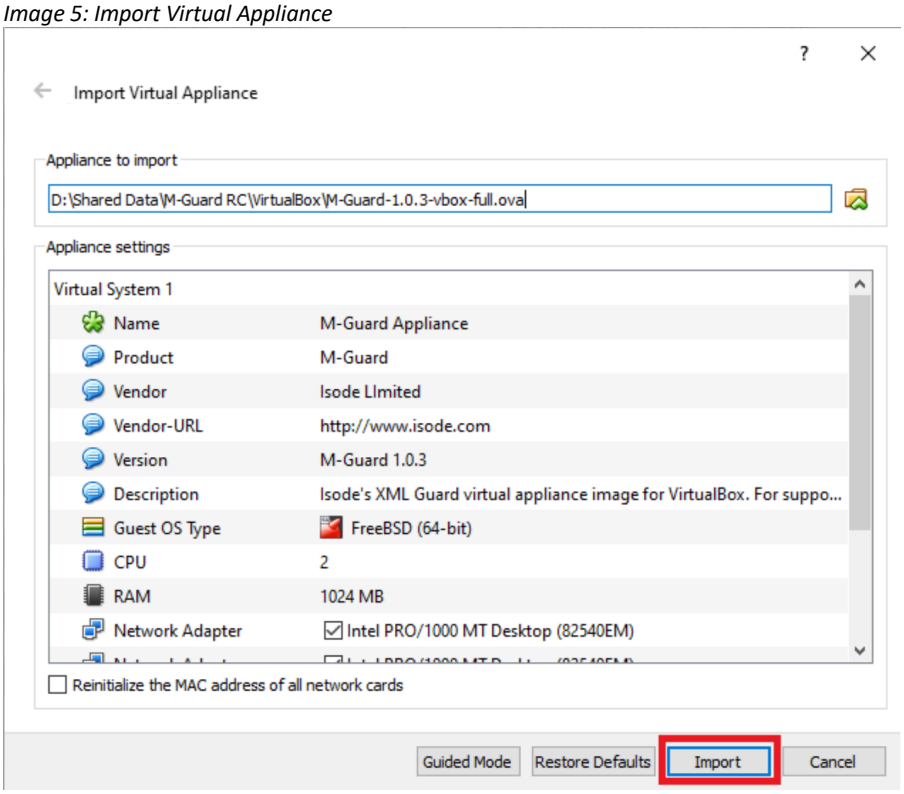
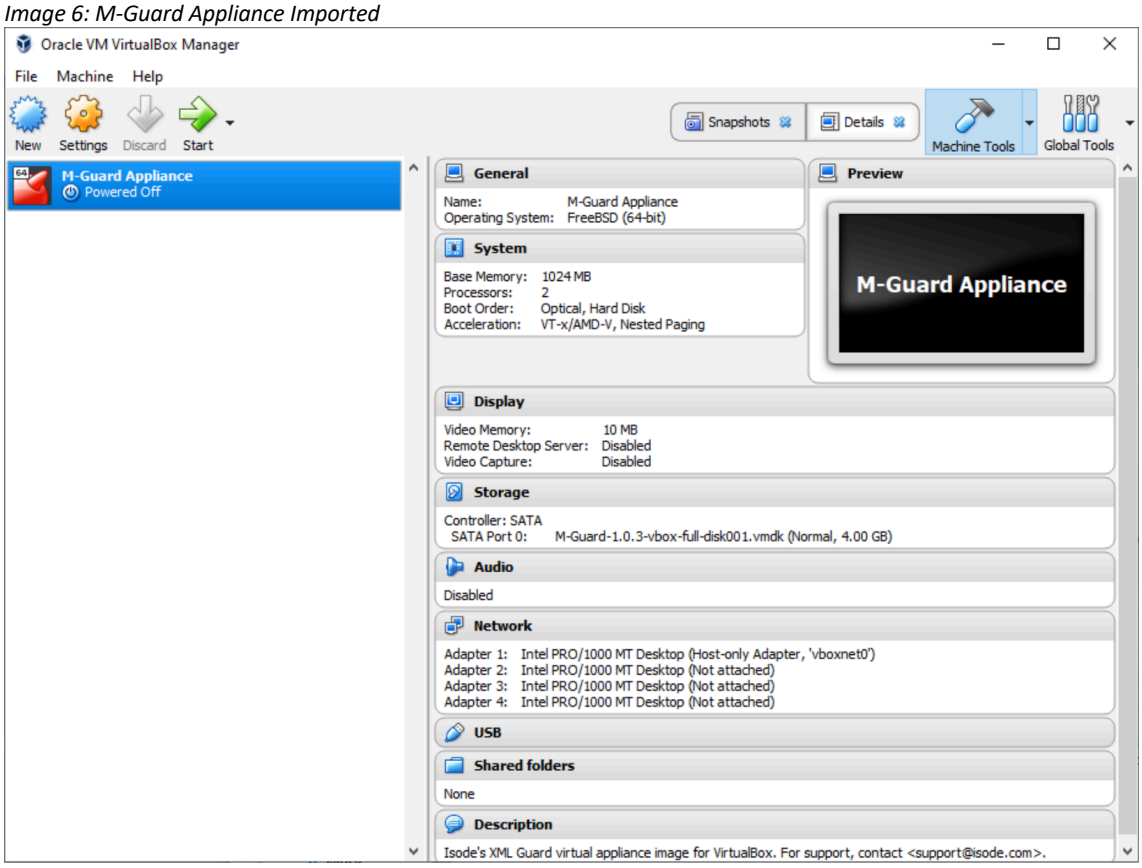


Image 5: Import Virtual Appliance



After clicking on [**Agree**] to accept the Software License Agreement, you will have successfully imported your M-Guard Appliance into VirtualBox (Image 6).

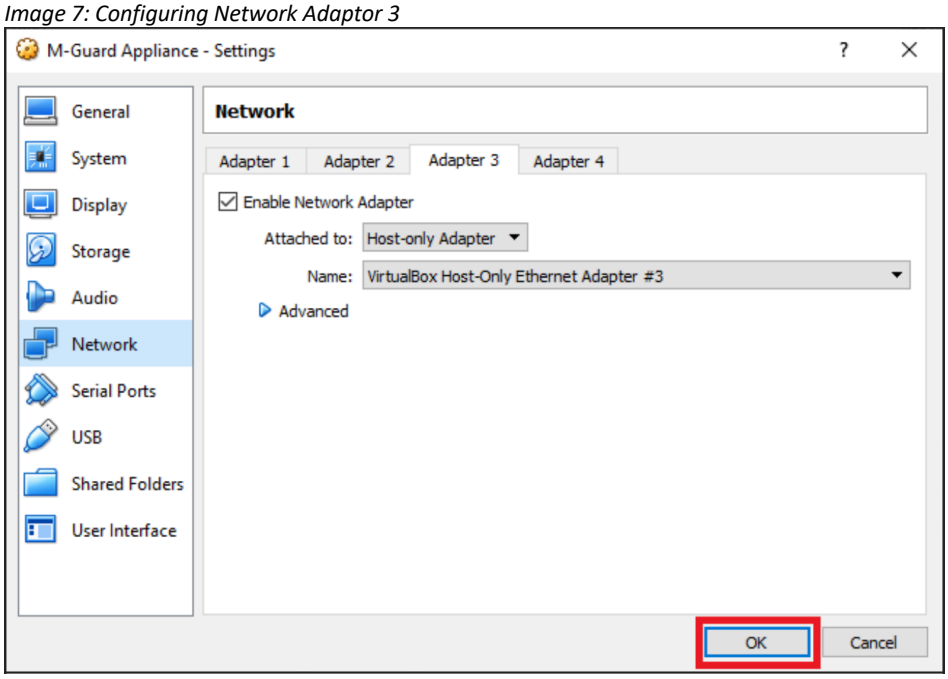
Image 6: M-Guard Appliance Imported



Configure Network Settings

Click the "Settings" icon, and select the "Network" option to configure Adaptor 1, 2 and 3 with the VirtualBox NIC names indicated in the earlier **Network Planning** section. Click [**OK**] after configuring each Adaptor. Image 7 shows the relevant configuration screen for Adaptor 2.

Image 7: Configuring Network Adaptor 3



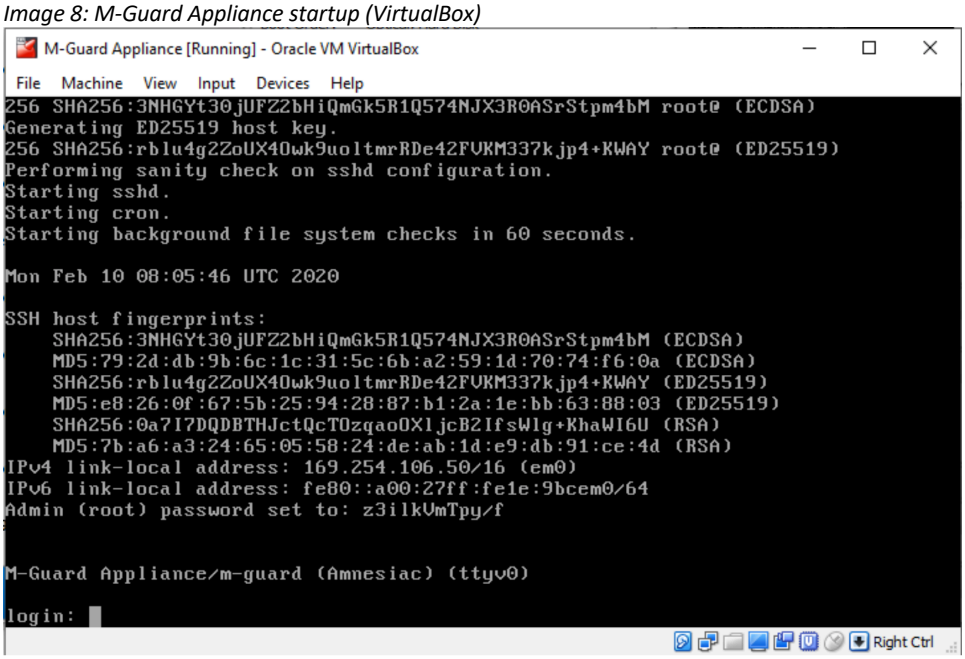
Once you have configured **all three Adaptors** in this way, disable Adaptors 2 and 3 for the "first

boot" and start your appliance.

When the startup screen (Image 8) is displayed, make a note of the following:

- Admin (root) password.
- IPv6 link-local address.
- The last fingerprint key "MD5/RSA".

Image 8: M-Guard Appliance startup (VirtualBox)

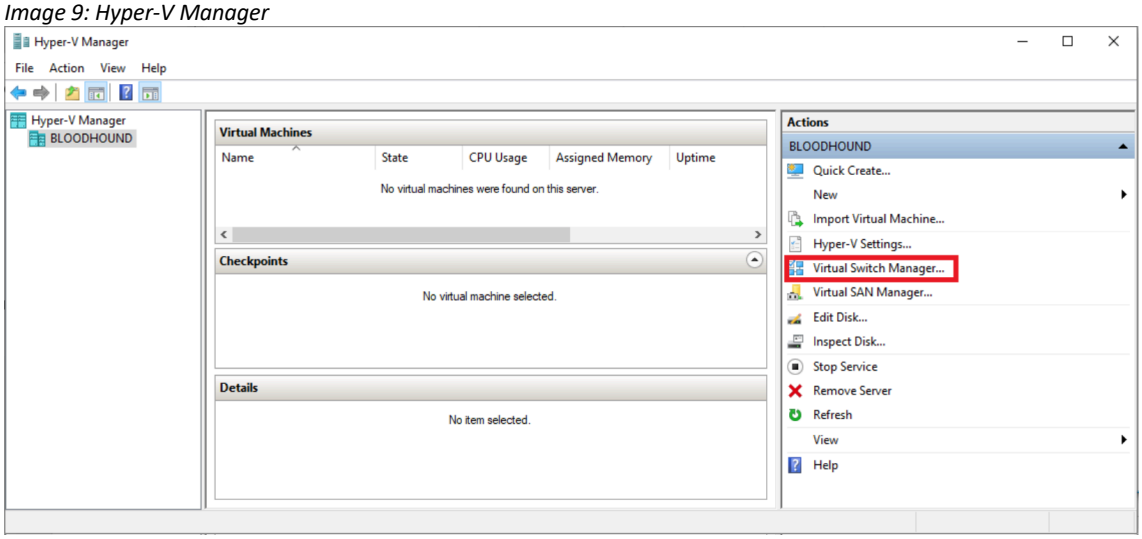


You are now ready to configure the M-Guard Appliance using M-Guard Console, as described in the section "**Configuring the M-Guard Appliance with M-Guard Console**".

Installation on Hyper-V

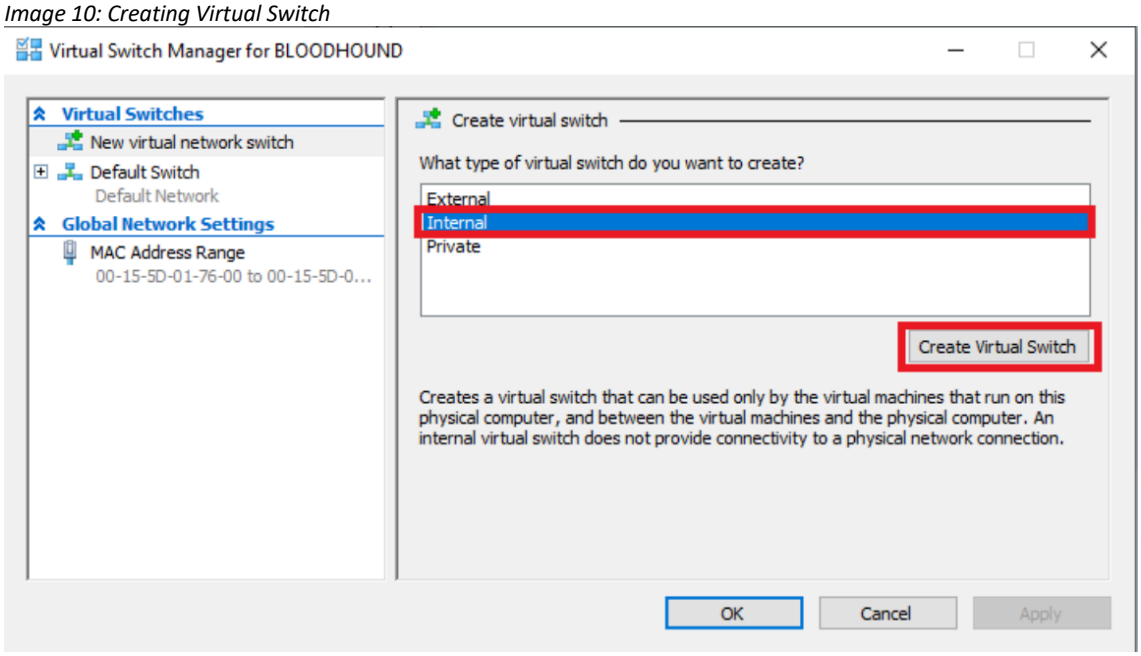
You'll need to configure three Hyper-V "virtual switches" using the Virtual Switch Manager. From the Hyper-V Manager select [**Virtual Switch Manager...**], as shown in Image 9.

Image 9: Hyper-V Manager



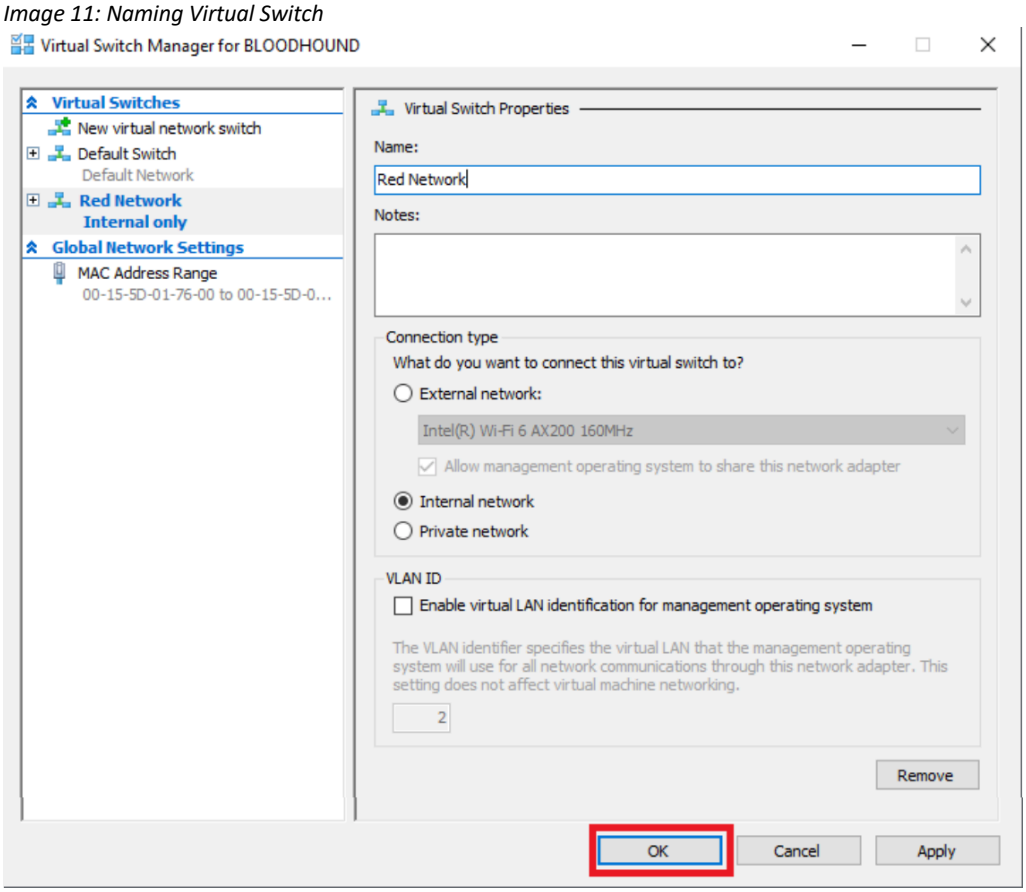
In the Virtual Switch Manager (Image 10) select "Internal" for the type of virtual switch and then click [**Create Virtual Switch**].

Image 10: Creating Virtual Switch



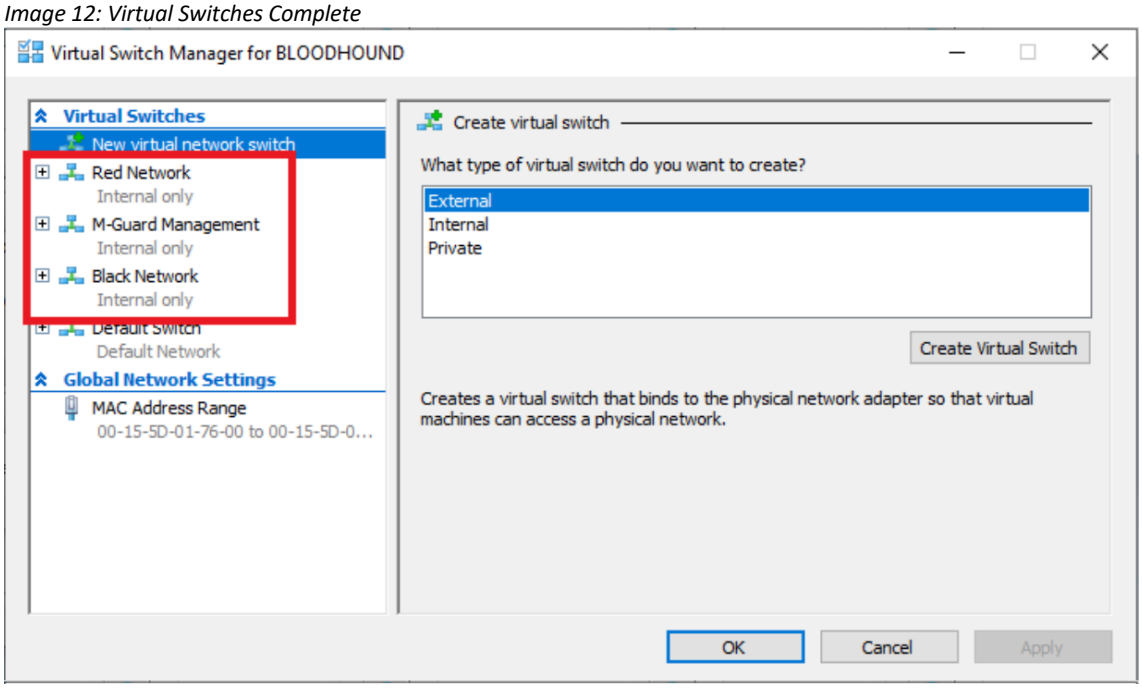
Enter a name for the Virtual Switch, in this case "Red Network" (Image 11) and click [**OK**].

Image 11: Naming Virtual Switch



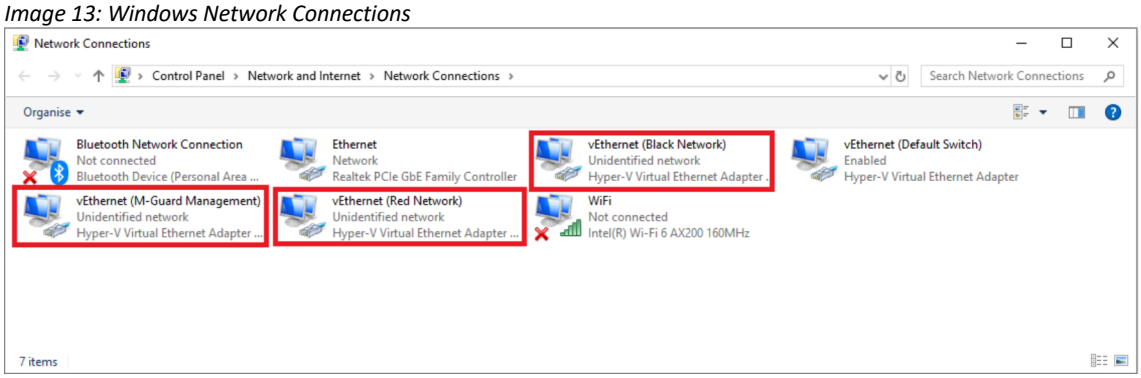
You will need to repeat this creation/naming process two more times so that you have three Virtual Switches, as shown in Image 12. As per the **Network Planning** table, these have been named "Red Network", "Black Network" and "M-Guard Management".

Image 12: Virtual Switches Complete



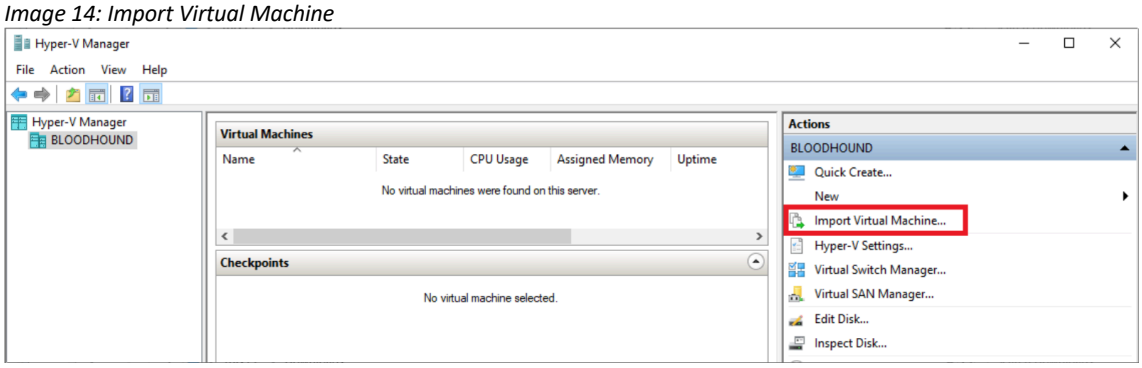
Click [**OK**]. You will see these networks on your Windows Network Connections (Image 13).

Image 13: Windows Network Connections



Extract the "M-Guard-1.0.3-hyperv-full.zip" compressed folder, downloaded earlier, to a folder of your choice. From Hyper-V Manager select "Import Virtual Machine..." (Image 14).

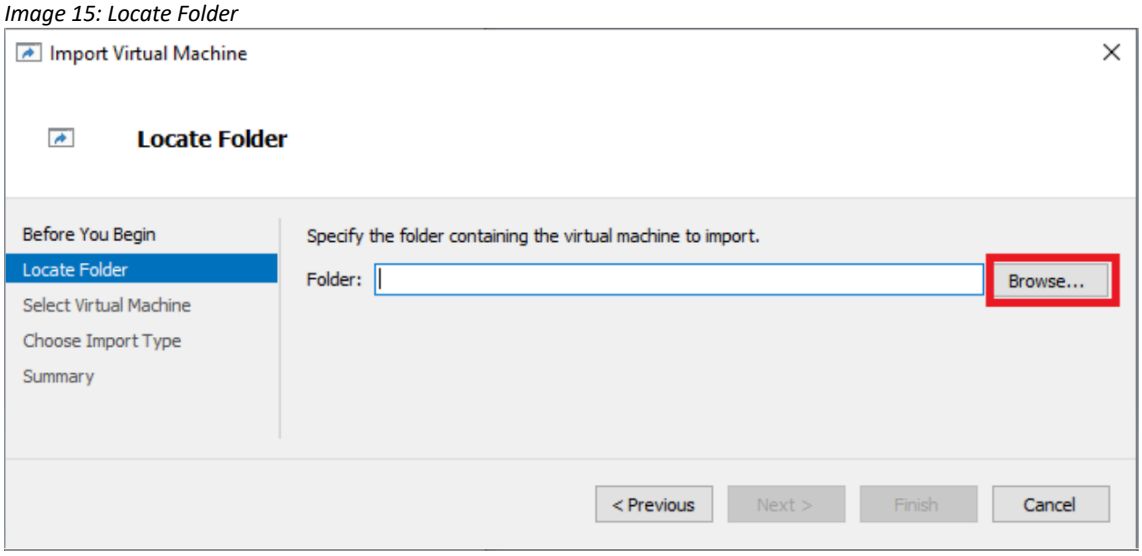
Image 14: Import Virtual Machine



Click [**Next**] on the "Before you begin screen".

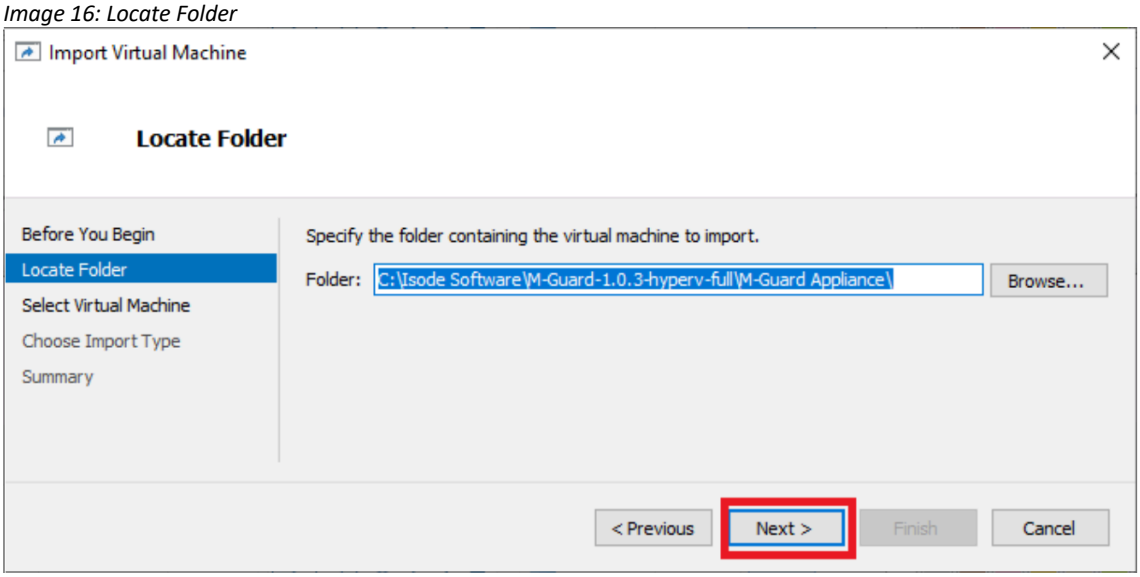
On the "Locate Folder" screen (Image 15) click on [**Browse**] to navigate to the "M-Guard Appliance" folder extracted from the .zip file.

Image 15: Locate Folder



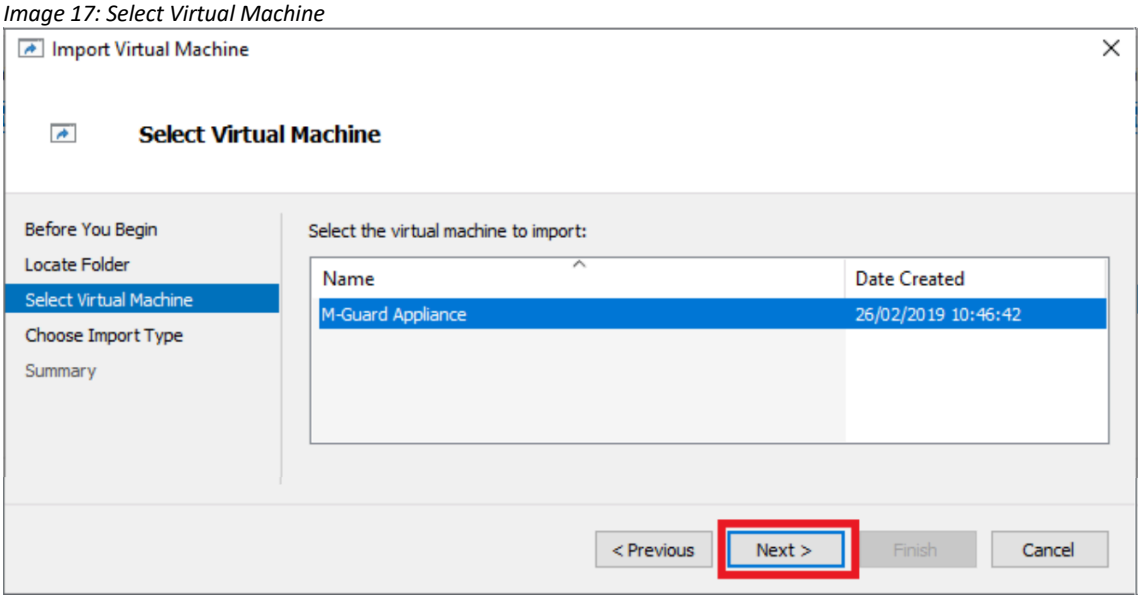
Select that folder, returning to the "Locate Folder" screen (Image 16).

Image 16: Locate Folder



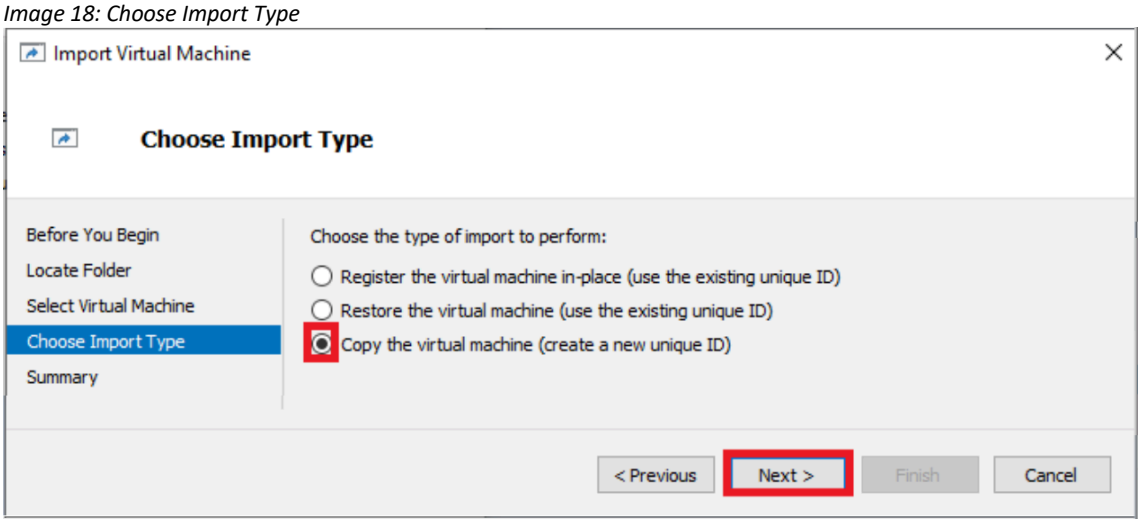
Click [**Next**] and in the Select Virtual Machine screen (Image 17), select the M-Guard Appliance before clicking [**Next**] again.

Image 17: Select Virtual Machine



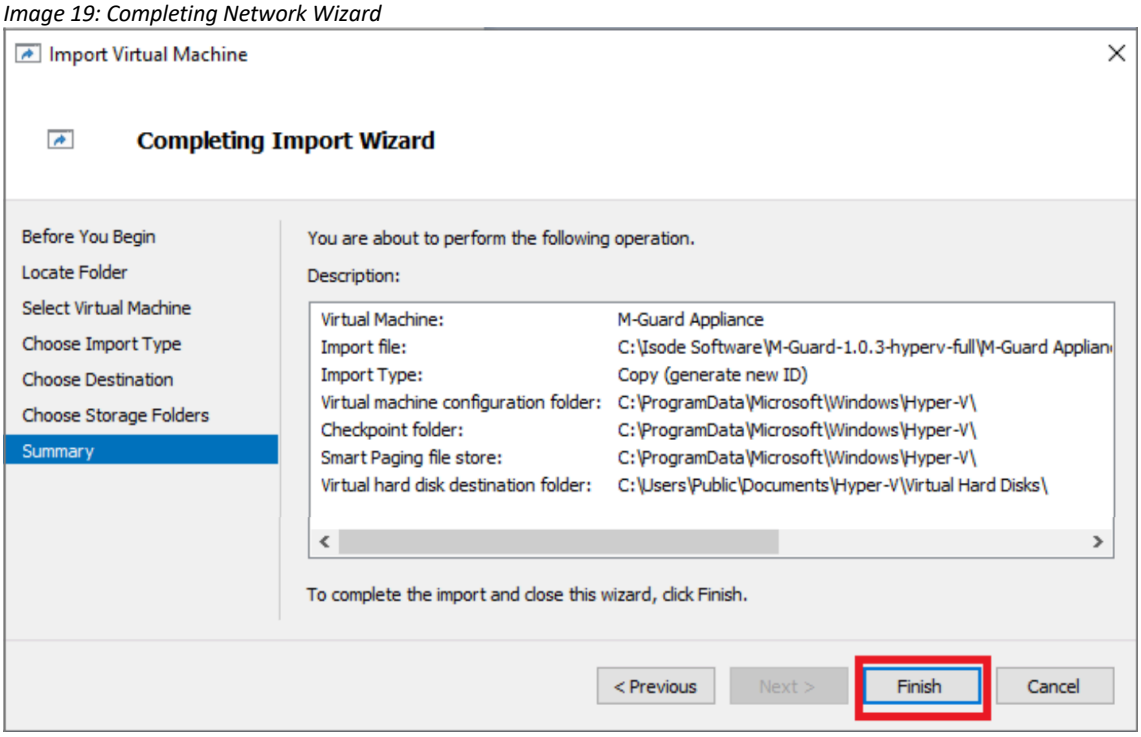
In the "Choose Import Type" screen (Image 18), select the [**Copy the virtual machine (create a new unique ID)**] radio button and click [**Next**].

Image 18: Choose Import Type



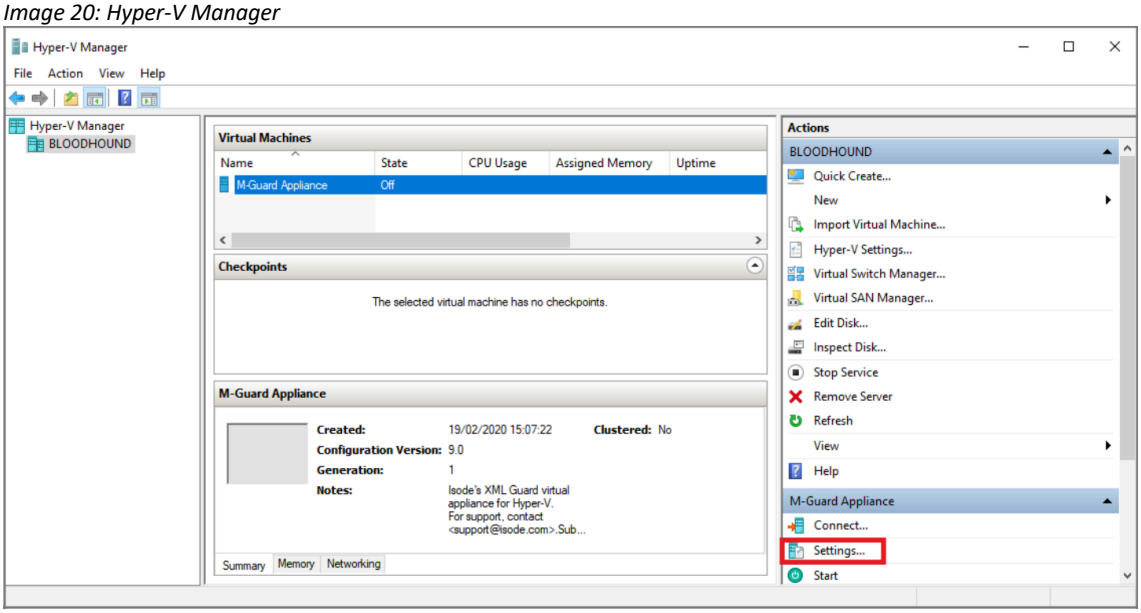
When prompted to "**Choose Destination**" and "Choose Storage folders" on the following two screens (not shown) accept the defaults and click [**Next**]. You'll then arrive at the "**Completing Network Wizard**" summary screen (Image 19). Click [**Finish**].

Image 19: Completing Network Wizard



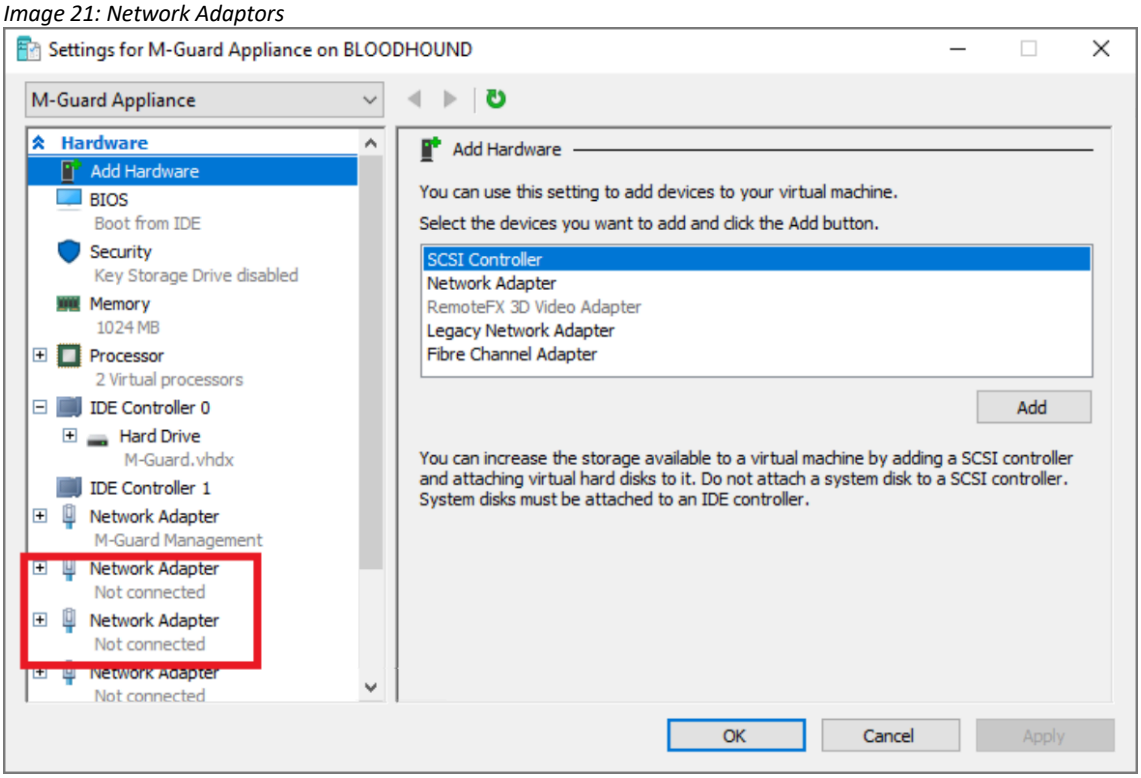
Back in the Hyper-V Manager (Image 20), select the M-Guard Appliance and click [**Settings...**]

Image 20: Hyper-V Manager



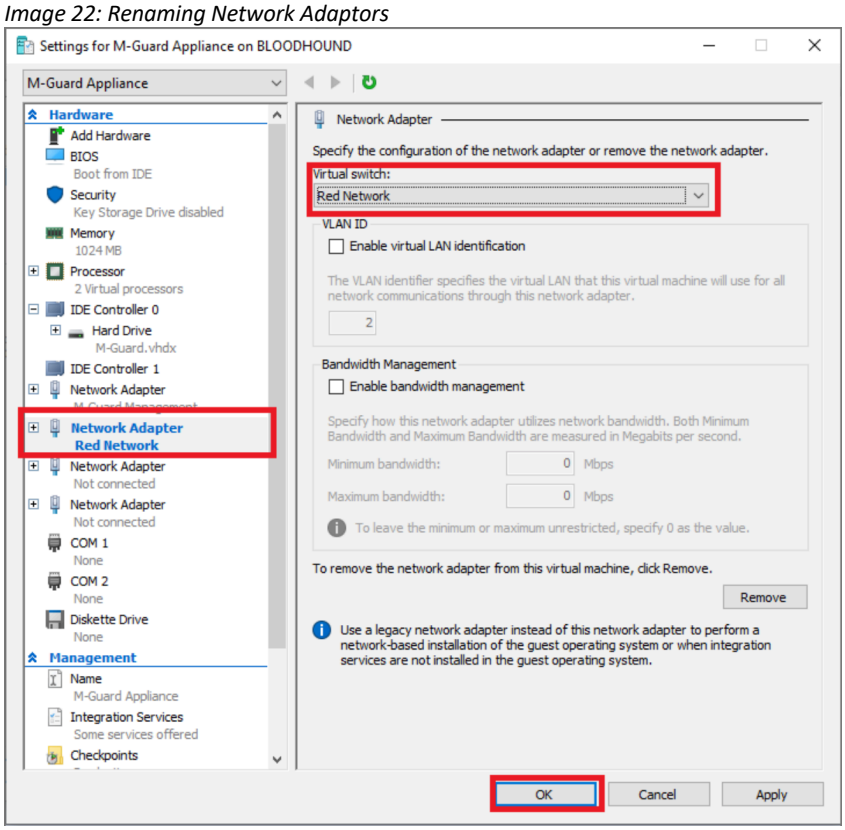
You will see (Image 21) that there are 4 Network Adapters the first one being called "M-Guard Management". Later (see Page 24, do not do this now it will cause problems) you will need to change two of these to "Red Network" and "Black Network", using the method that follows.

Image 21: Network Adaptors



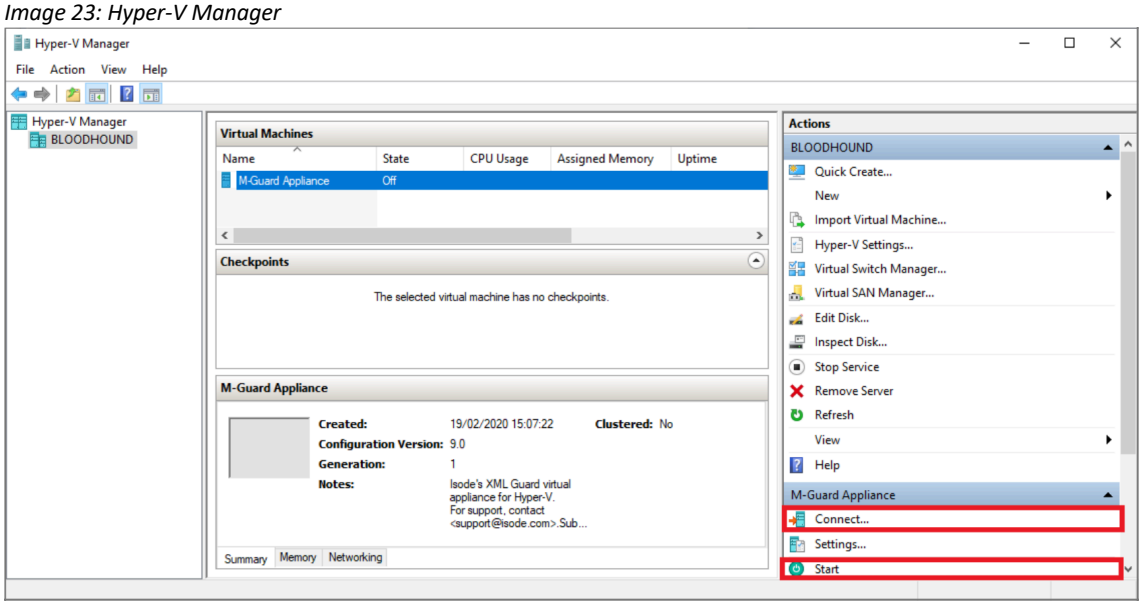
As shown in Image 22, select the "Virtual Switch" on the left-hand pane, then select the "Red Network" from drop down for the "Network Adapter" and Click [**OK**]. Repeat this for the "Black Network".

Image 22: Renaming Network Adaptors



Return to the main "Hyper-V Manager" screen and select the "M-Guard Appliance" (Image 23).

Image 23: Hyper-V Manager

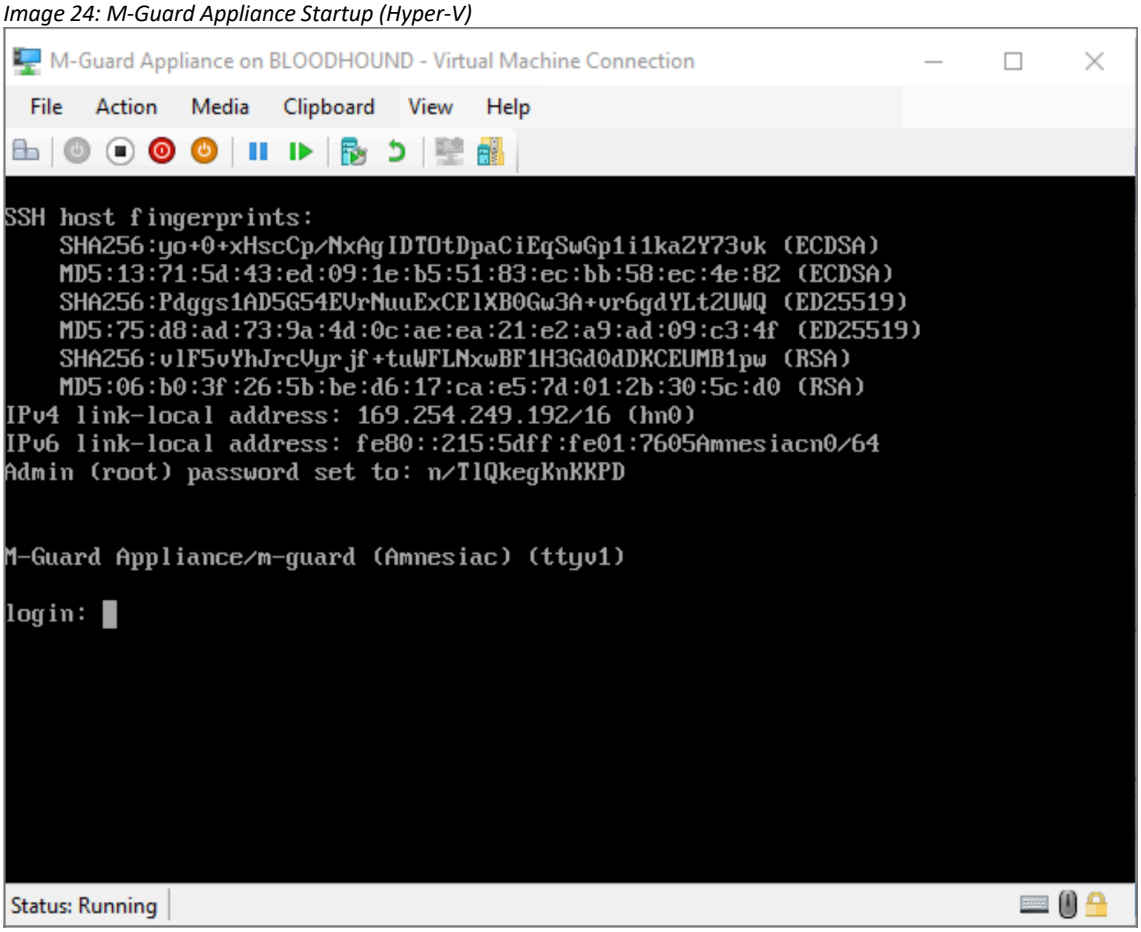


Click [**Connect...**] and then [**Start**] you will see the "M-Guard Appliance" window open and boot up (Image 24).

When the startup screen (Image 24) is displayed, make a note of the following:

- Admin (root) password.
- IPv6 link-local address.
- The last fingerprint key "MD5/RSA".

Image 24: M-Guard Appliance Startup (Hyper-V)



You are now ready to configure the M-Guard Appliance using M-Guard Console, as described in the section "**Configuring the M-Guard Appliance with M-Guard Console**".

Configuring the M-Guard Appliance with M-Guard Console (Part 1)

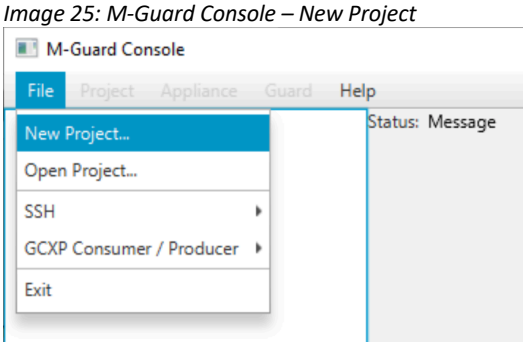
Open a Windows Command Prompt and navigate to the folder where you have M-Guard Console installed and run the following command to open M-Guard Console:

```
C:\Program Files\OpenJDK for Isode\openjdk\jdk-
11.0.2\bin\java.exe" -jar M-Guard-Console-1.0.2.jar
```

Setting up and Connecting to the Appliance

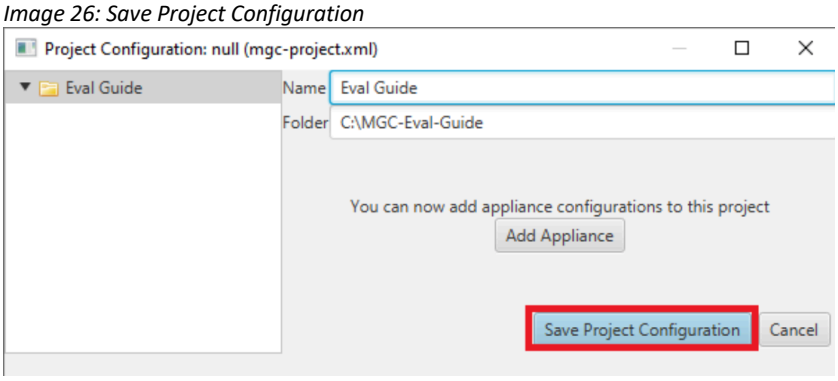
In the M-Guard Console screen (Image 25) select "File > New Project…", navigate to an empty folder you want to use to store tour new project and select that folder.

Image 25: M-Guard Console – New Project



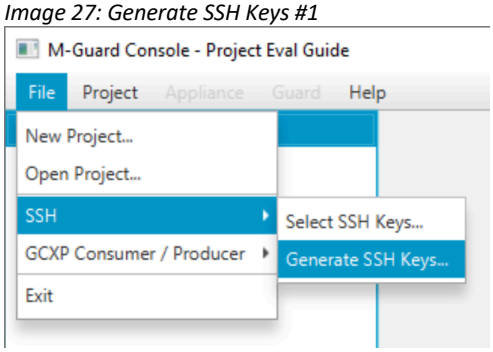
Enter a name for the project (Image 26) and then click on [**Save Project Configuration**].

Image 26: Save Project Configuration



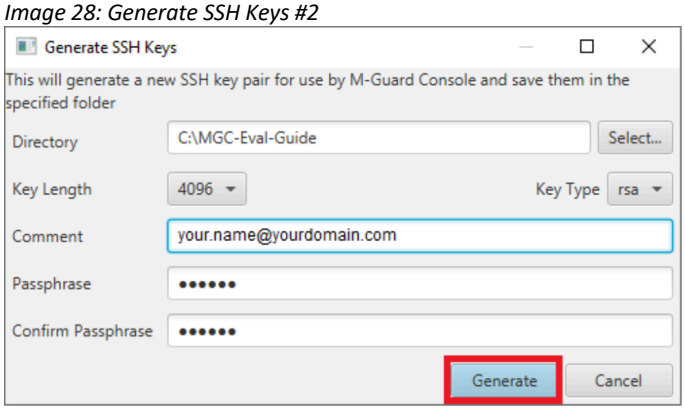
Now from the M-Guard console screen select "File > SSH > Generate SSH Keys…" (Image 27).

Image 27: Generate SSH Keys #1



Select a directory in which to save the SSH key pair, leave "Key Length" and "Key Type" at the default settings, enter your email address in the "Comment" field and finally enter and confirm a passphrase (Image 28). Then click on [**Generate**].

Image 28: Generate SSH Keys #2



In the M-Guard Console main screen, right-click on the project you have just created ("Eval Guide" in this case) and select [**Configure...**] and in the dialog box click [**Add Appliance**], (Images 29 & 30).

Image 29: Configure Project

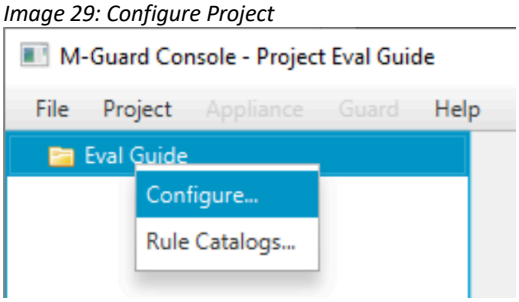
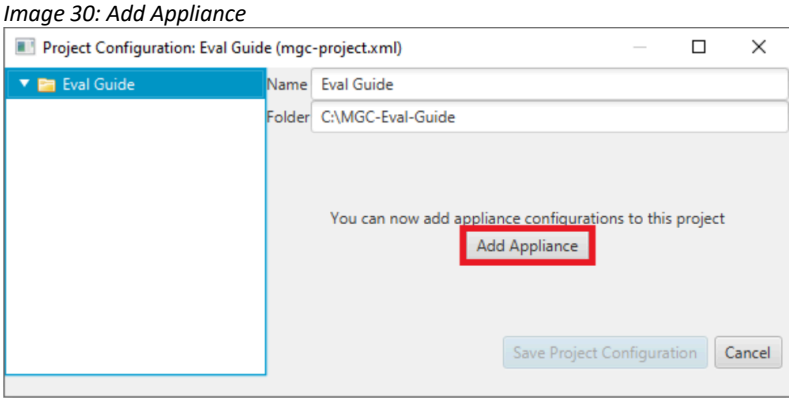


Image 30: Add Appliance

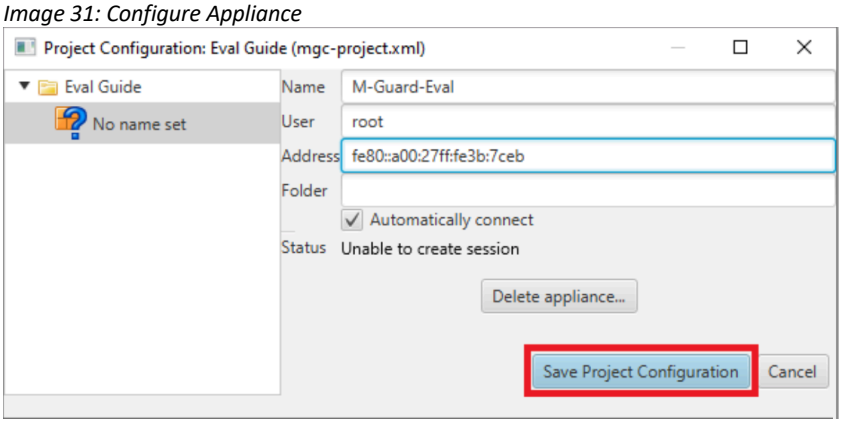


Now in the configuration screen (Image 31) you should add:

- A "Name" for the Appliance – here we've used "M-Guard-Eval".
- An "Address" – this is the IPv6 Link Local Address displayed on the First Boot Screen (Image 8 for VirtualBox, Image 24 for Hyper-V)

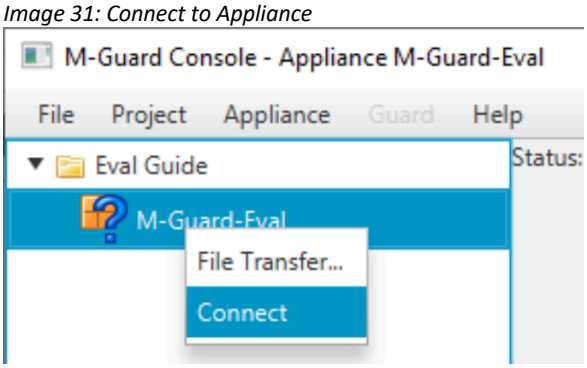
Then click [**Save Project Configuration**].

Image 31: Configure Appliance



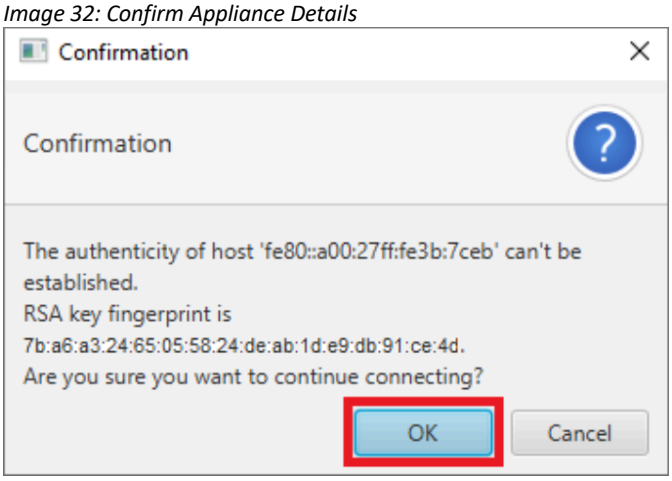
Now right-click on this new Appliance (Image 31) and select [**Connect...**].

Image 31: Connect to Appliance



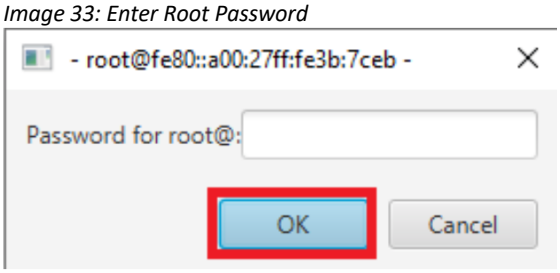
In the dialog box that opens (Image 32), check that the RSA Key fingerprint matches the one you noted down earlier (Image 8 for VirtualBox, Image 24 for Hyper) and click on [**OK**].

Image 32: Confirm Appliance Details



You will then be prompted for the root password that was also displayed on the "First Boot" screen (Image 8 for VirtualBox, Image 24 for Hyper-V), enter that password (Image 33) and click [**OK**].

Image 33: Enter Root Password



You are now connected to the Appliance and can start configuring it.

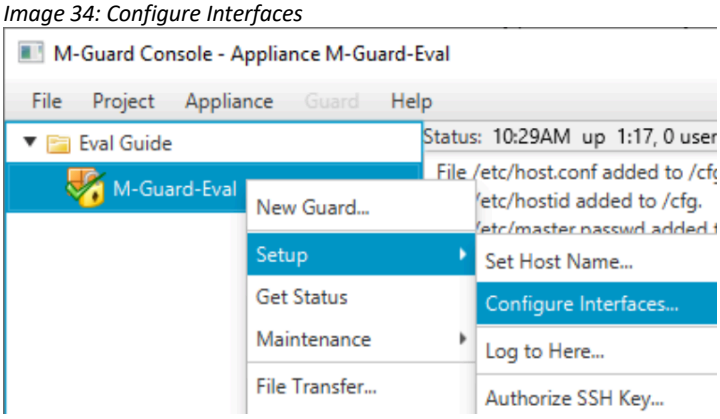
***Changing the Root Password**: At this stage you may wish to change the Root password to one of your choice. This can be done by right-clicking on the M-Guard-Eval Appliance and selecting "Maintenance > Change Password"*

Configuring the Appliance

We're now going to configure the M-Guard Management Network Interface. Right click on the

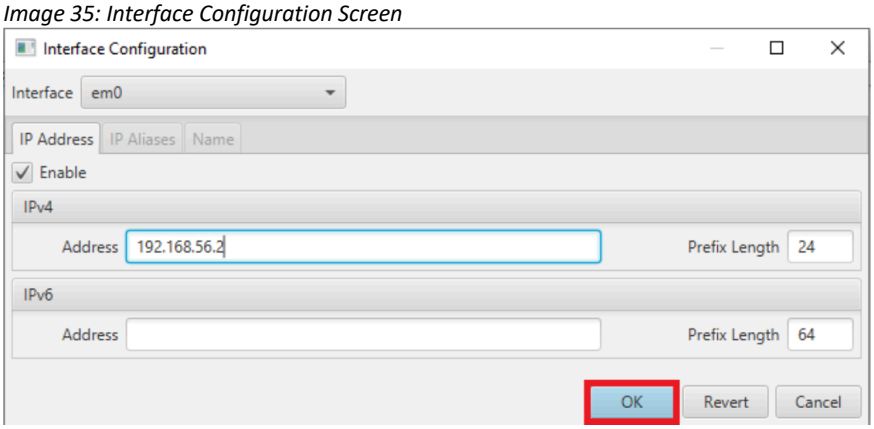
Appliance (Image 34) and select [**Setup** > **Configure Interfaces...**].

Image 34: Configure Interfaces



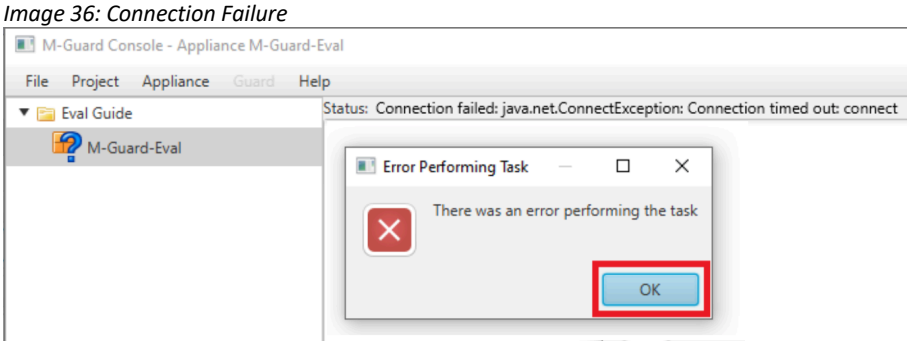
In the Interface Configuration Screen (Image 35) enter the IPv4 address for the NIC and click [**OK**].

Image 35: Interface Configuration Screen



After a short period of time the Appliance with disconnect because the IP Address of the Management Connection has now changed on the Appliance (Image 36).

Image 36: Connection Failure

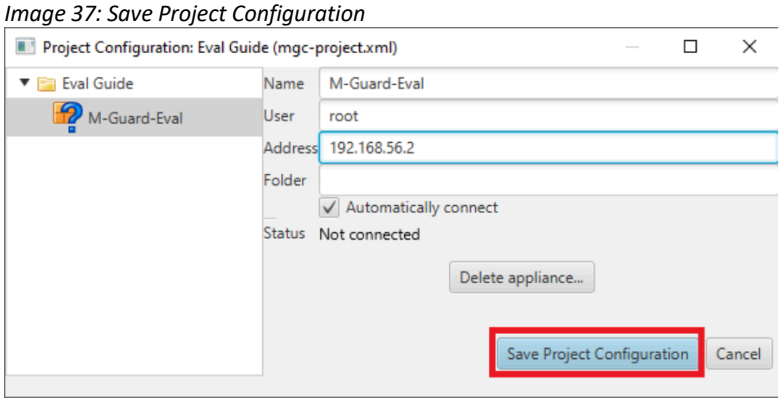


Click [**OK**] to close the error notification. You will now need to change the Network Address on M-Guard Console.

Right-click on the top level of the Project ("Eval Guide") and select Configure, then navigate to your appliance ("M-Guard-Eval").

Enter the New IP Address you created and click [**Save Project Configuration**] (Image 37).

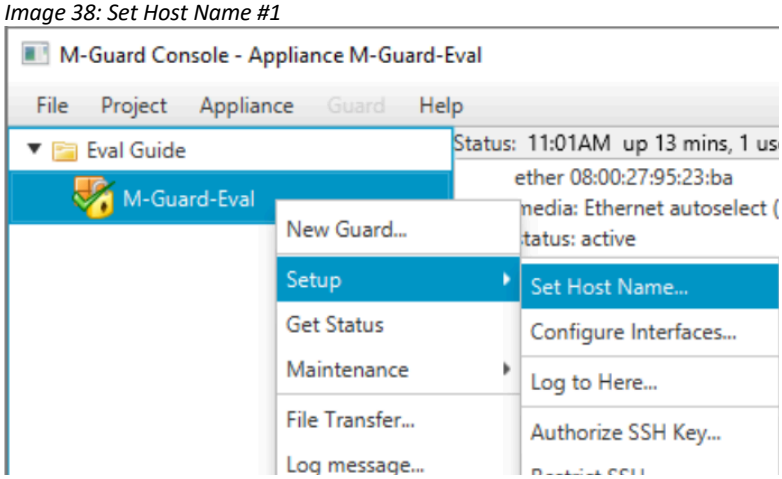
Image 37: Save Project Configuration



Right-click on the Appliance and Click [**Connect**]. Now "Save the Appliance Configuration" as previously described (see Image 31).

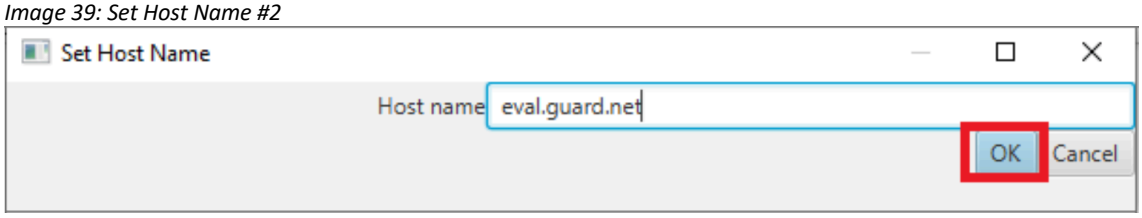
Now you can set the Host Name of the Appliance. Right-click on the Appliance and select "Setup > Set Host Name..." (Image 38).

Image 38: Set Host Name #1



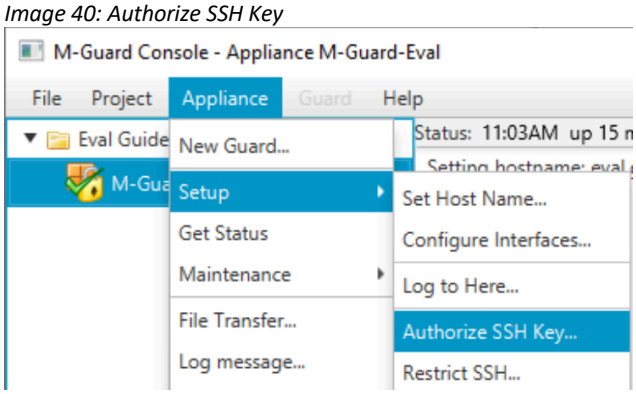
Enter a hostname for the Appliance ("eval.guard.net" in this example) and Click [**OK**].

Image 39: Set Host Name #2



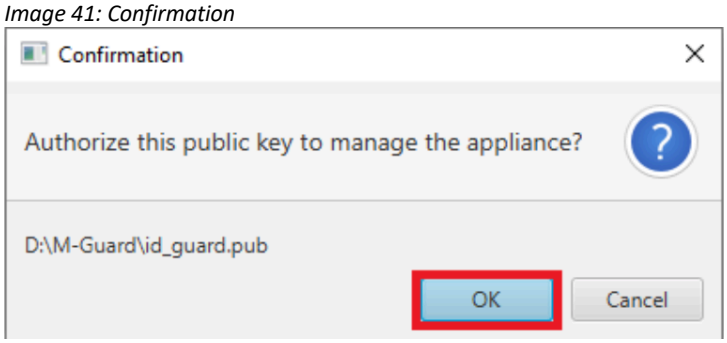
You should now Authorize the SSH Key you are using by selecting "Appliance > Setup > Authorize SSH Key.." from the M-Guard Console menu (Image 40).

Image 40: Authorize SSH Key



Click [**OK**] to complete this section (Image 41).

Image 41: Confirmation



If you are using VirtualBox, you should now shutdown the Appliance, enable the two other Network Interfaces and then start the Appliance. This completes the instructions for VirtualBox.

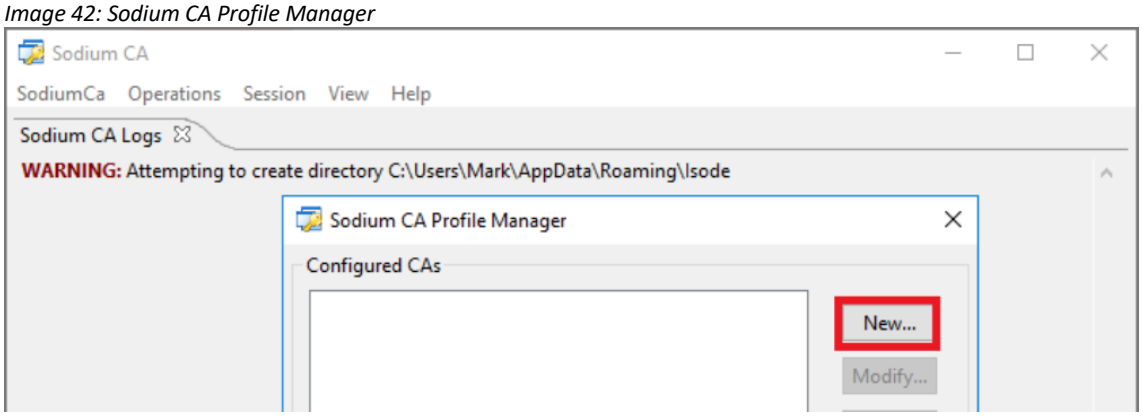
The next step is to Create Certificates for the Appliance and this requires setting up Sodium CA so Save the Appliance Configuration as previously described and pause the configuration process while we setup Sodium CA.

Setting up Sodium CA to provide the Certificates M-Guard

To run Sodium CA from the Windows Start Menu select "Start > Isode R18.0 > SodiumCA". Note there is another program installed called "Sodium" so be sure to use the correct one.

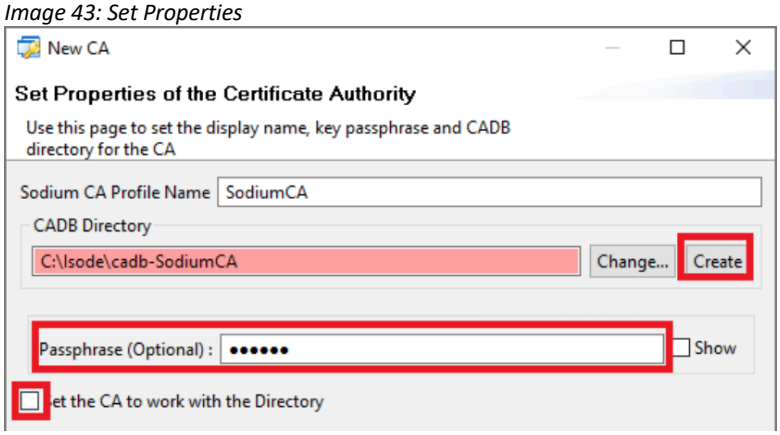
Ignore the warning that automatically pops up and click on [**New**] in the Profile Manager (Image 42).

Image 42: Sodium CA Profile Manager



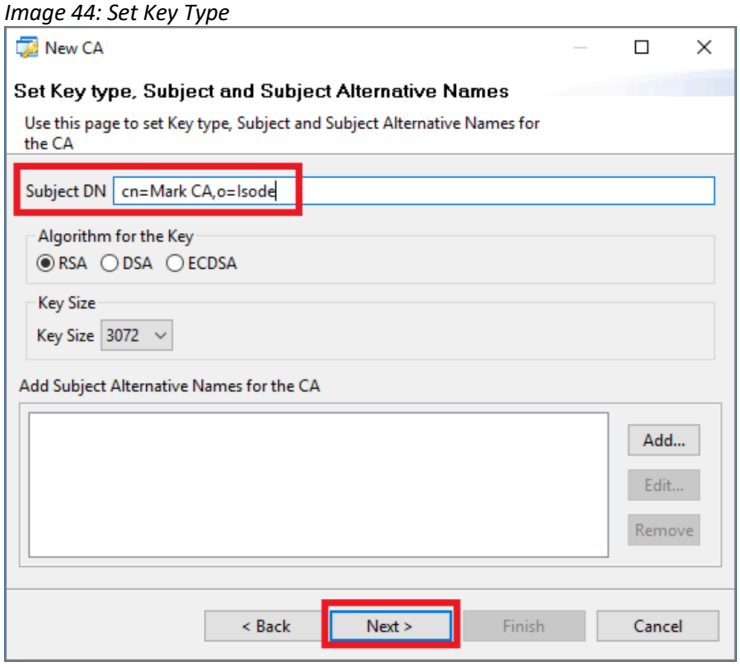
In the Set Properties screen (Image 43) you should uncheck the "Set the CA to work with the Directory" checkbox as there is no Directory. It is recommended that you create a passphrase for using Sodium CA then Click the [**Create**] button next to the CADB Directory.

Image 43: Set Properties



You should now click the now activated [**Next**] button to move onto the Set Key Type screen (Image 44). In this screen enter a Subject DN in the form shown in the screenshot, then click [**Next**].

Image 44: Set Key Type

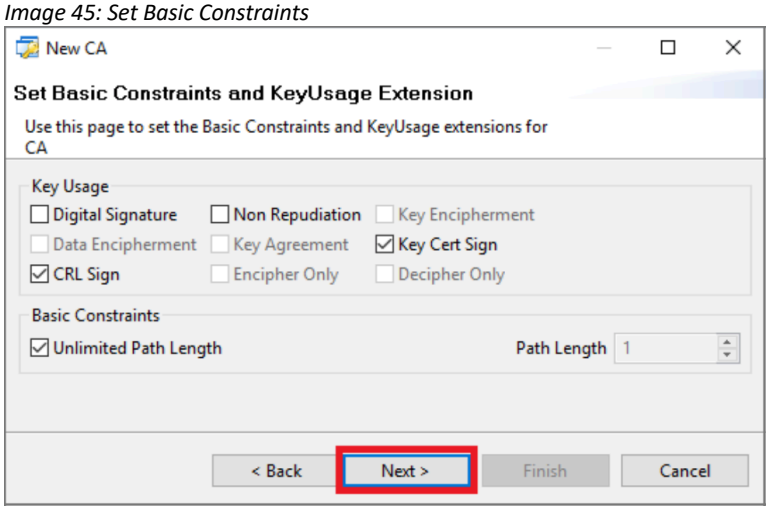


In the screen "Set the CRL Distribution Point for the CA" (not shown), click [**Next**] without making any changes.

In the screen "Set the Access Description List for the CA" (not shown), click [**Next**] without making any changes.

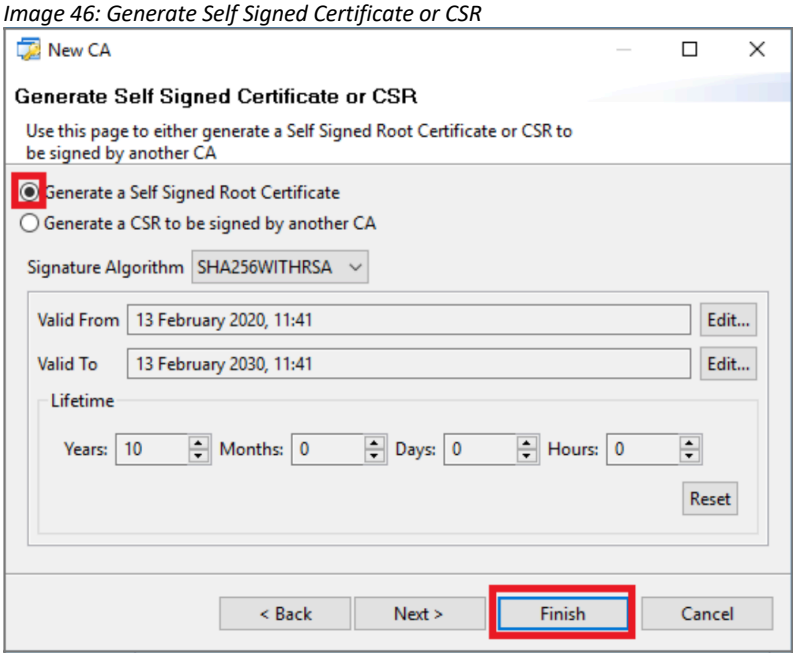
In the "Set Basic Constraints and KeyUsage Extensions" (Image 45) ensure that the "CRL Sign", "Key Cert Sign" and "Unlimited Path Length" checkboxes are ticked and click [**Next**].

Image 45: Set Basic Constraints



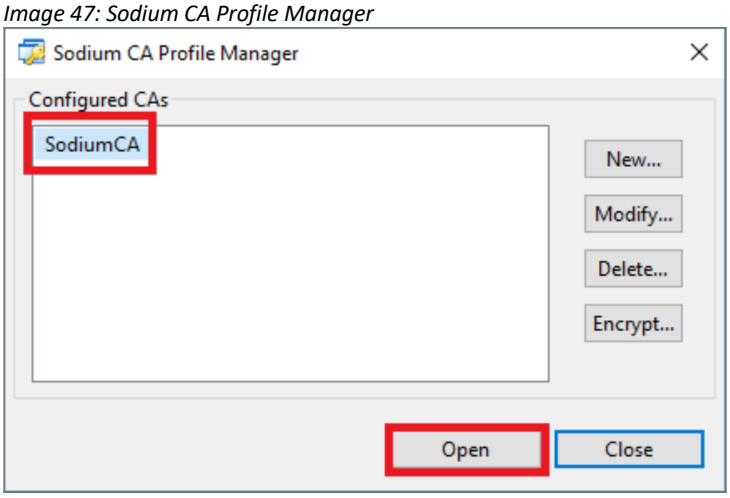
In the "Generate Self Signed Certificate or CSR" screen (Image 46) select the "Generate a Self Signed Root Certificate" radio button and click [**Finish**].

Image 46: Generate Self Signed Certificate or CSR



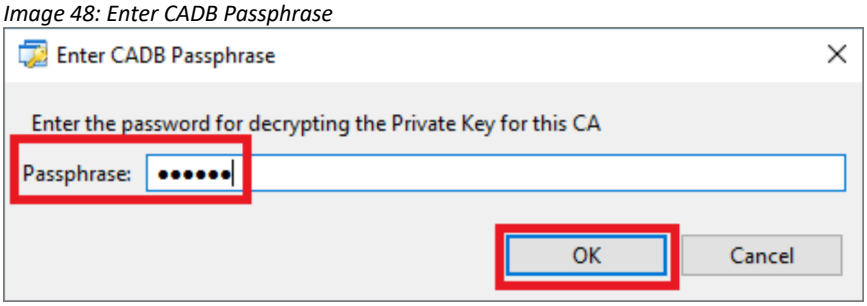
You have now created a CA and should open it in the Profile Manager (Image 47) by selecting it and clicking [**Open**].

Image 47: Sodium CA Profile Manager



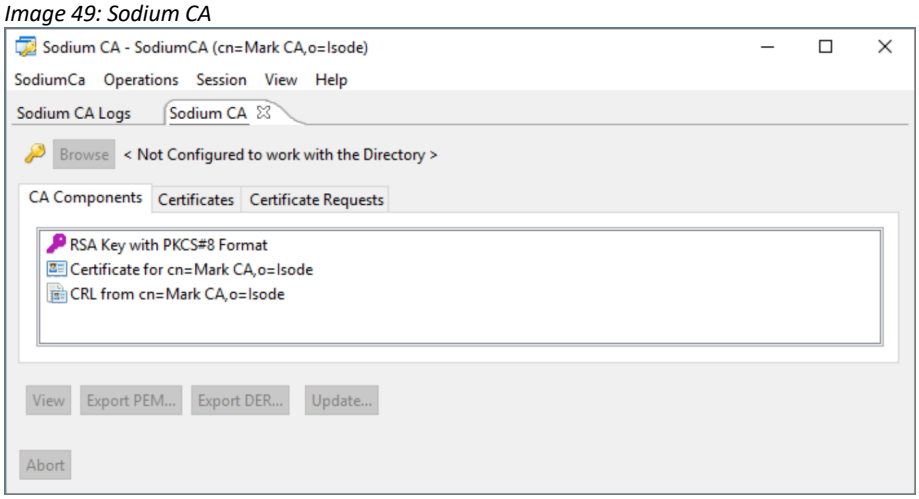
Now enter the passphrase you created earlier (Image 48) and click [**OK**].

Image 48: Enter CADB Passphrase



Your CA is now ready to receive "Certificate Signing Requests" (CSRs) from your M-Guard Appliance Image 49).

Image 49: Sodium CA



You should now return to M-Guard Console.

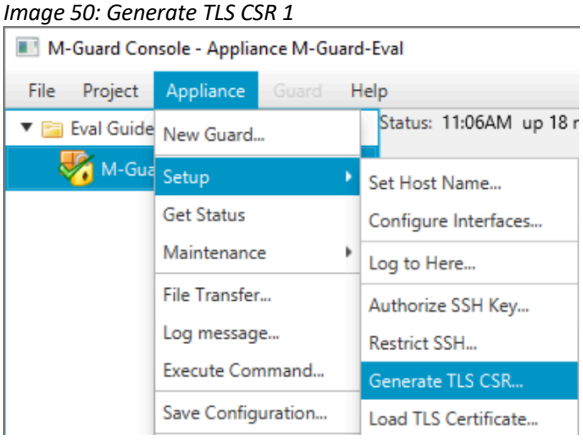
Configuring the M-Guard Appliance with M-Guard Console (Part 2)

You should now generate your Certificate Signing Request for the Appliance.

Generate Certificate Signing Request

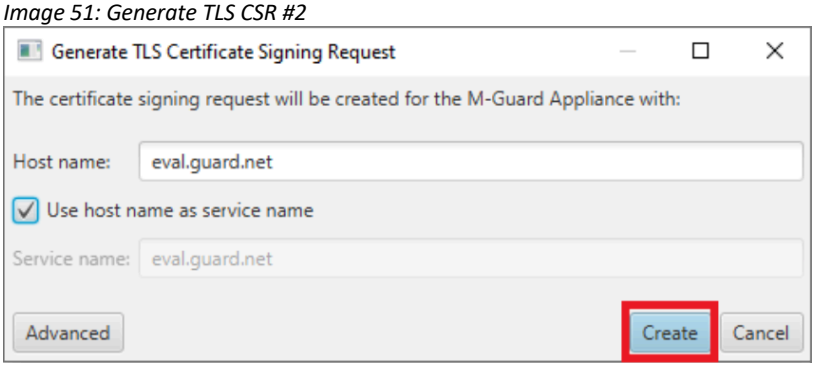
In M-Guard console right-click on the Appliance (Image 50) and select "Setup > Generate TLS CSR...".

Image 50: Generate TLS CSR 1



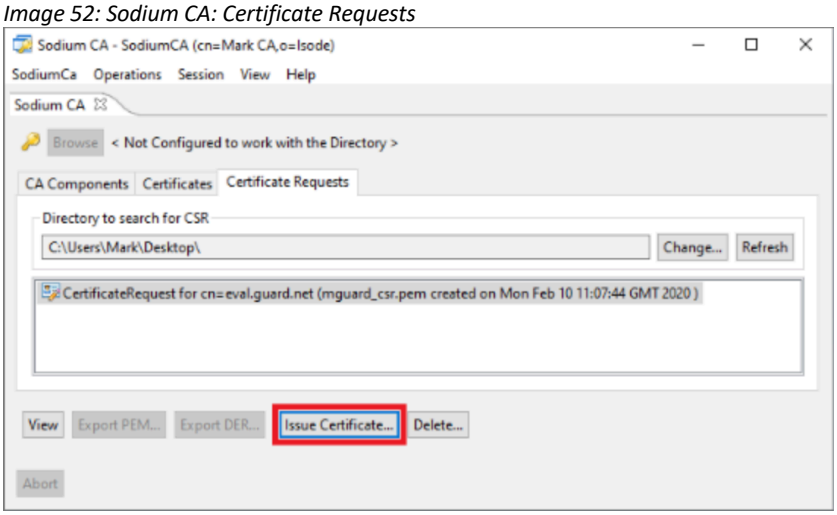
Then click on [**Create**] (Image 51) and save the file when prompted (not shown).

Image 51: Generate TLS CSR #2



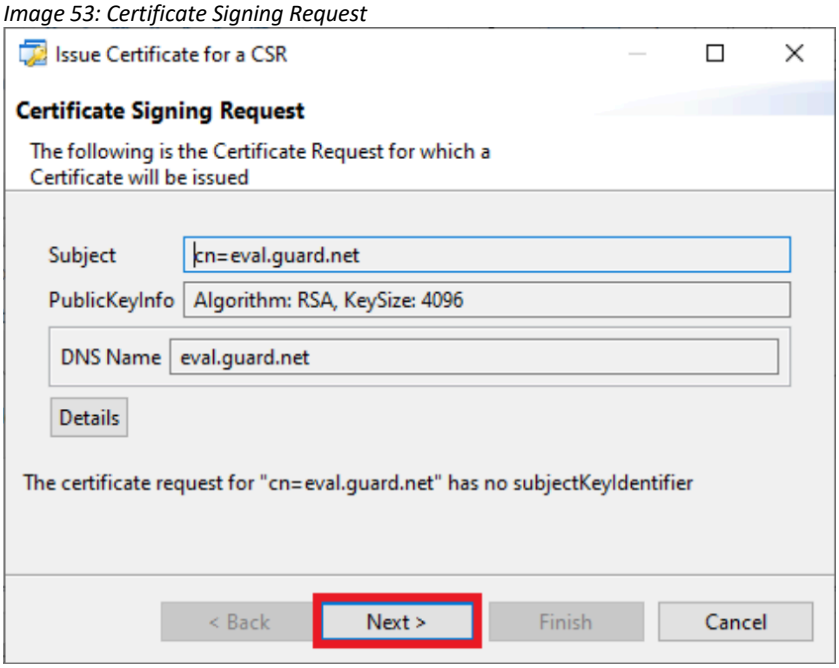
Now switch to Sodium CA and you'll see the CSR on the "Certificate Requests" tab (Image 52). Click on [**Issue Certificate...**].

Image 52: Sodium CA: Certificate Requests



Accept the defaults in the "Certificate Signing Request" screen (Image 53) and click [**Next**].

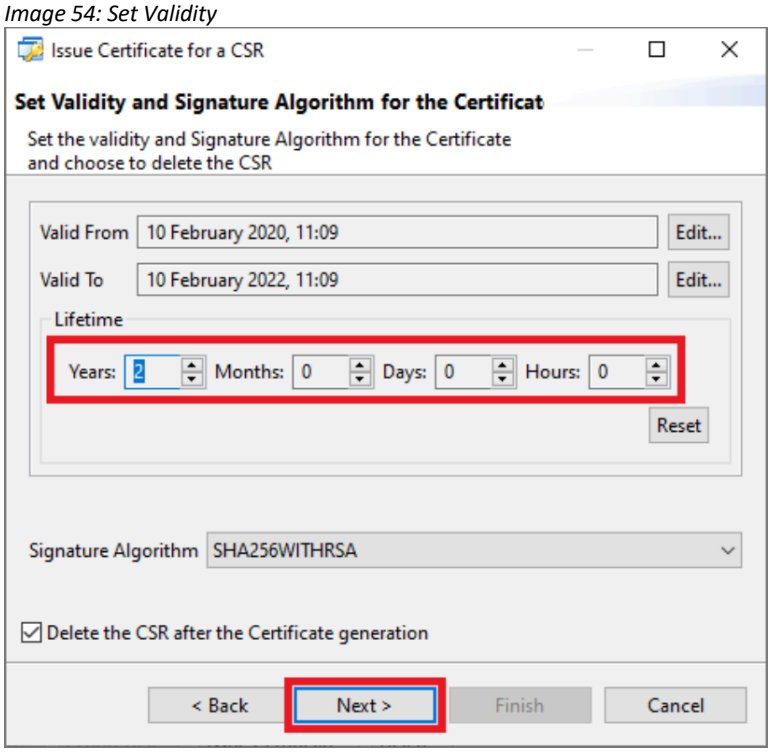
Image 53: Certificate Signing Request



Accept the defaults on the "Select and add Subject Alternative Names" screen (not shown), and on the "Select and Create X.509 Extensions" screen (not shown), clicking [**Next**] on both of them.

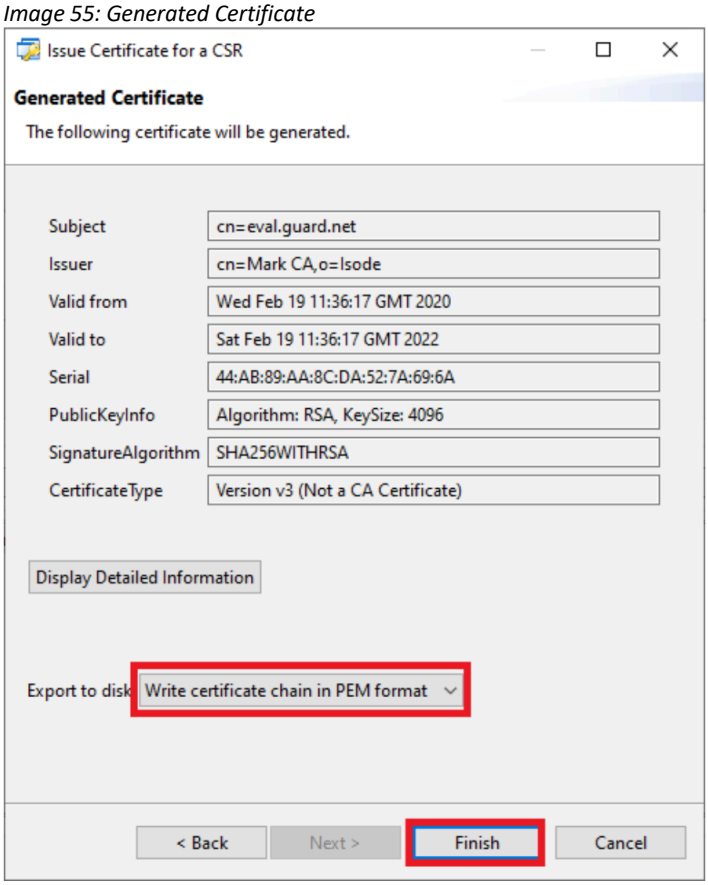
In the "Set Validity and Signature Algorithm for the Certificate" screen (Image 54), change the validity to what you want and click [**Next**].

Image 54: Set Validity



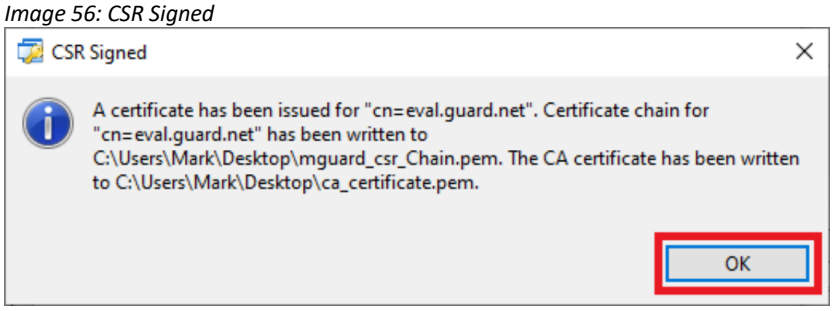
In the "Generated Certificate" screen (Image 55) select [Write certificate chain in PEM format] from the "Export to disk dropdown, then click [**Finish**].

Image 55: Generated Certificate



Click [**OK**] on the confirmation message (Image 56) and return to M-Guard console.

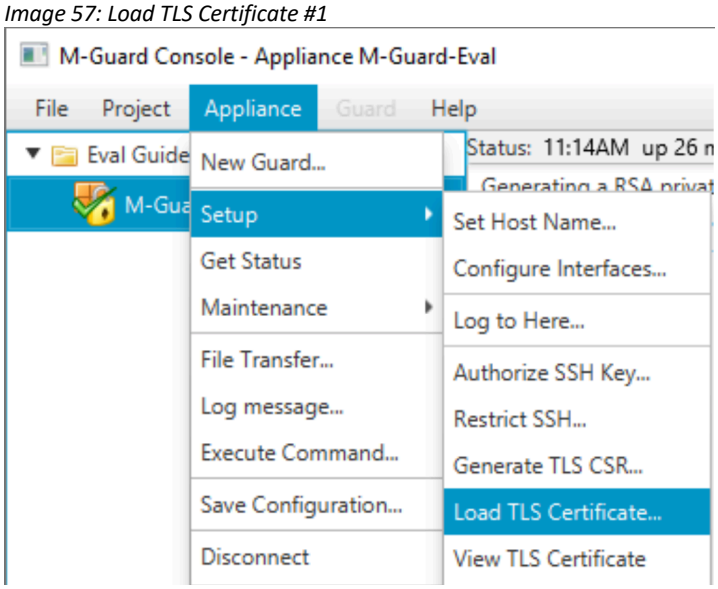
Image 56: CSR Signed



Load TLS Certificate

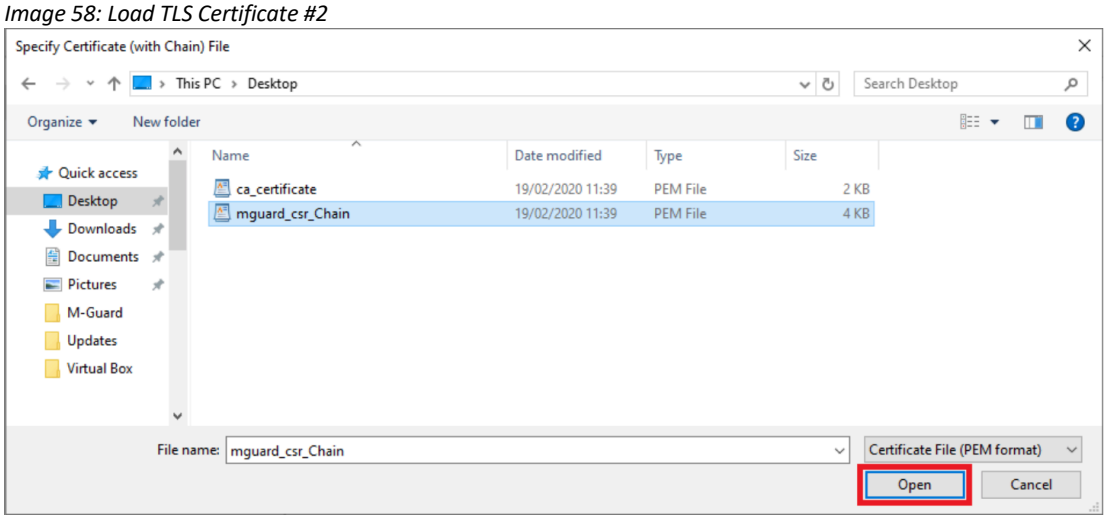
In M-Guard Console you now need to import the generated Certificate. Right-click on the Appliance (Image 57) and select “Setup > Load TLS Certificate”.

Image 57: Load TLS Certificate #1



Select the “mguard_csr_Chain.pem” file from where you earlier saved it (Image 58) and click [**Open**].

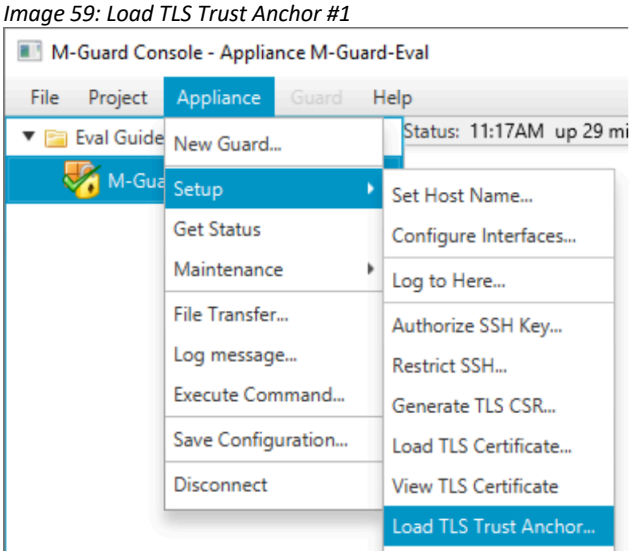
Image 58: Load TLS Certificate #2



Load TLS Trust Anchor

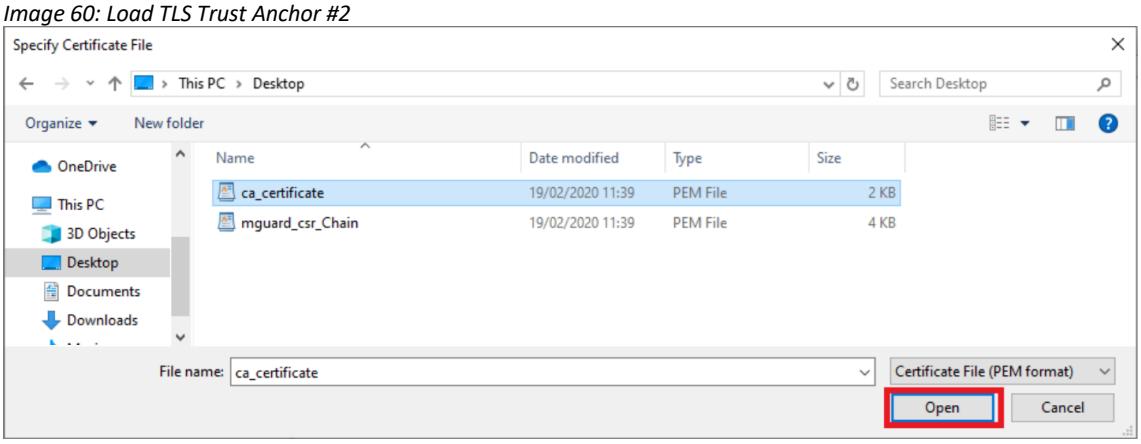
Right click on the Appliance in M-Guard Console (Image 59) and select "Setup > Load TLS Trust Anchor..."

Image 59: Load TLS Trust Anchor #1



Select the "ca_certificate.pem" file from where you earlier saved it (Image 60) and click [**Open**].

Image 60: Load TLS Trust Anchor #2

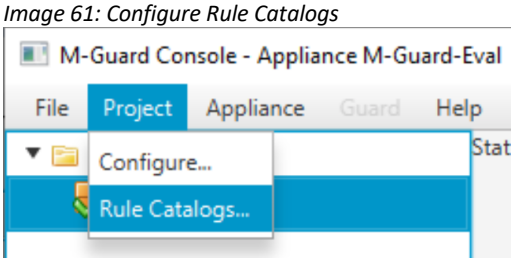


Click [**OK**] on the Confirmation Screen (not shown) and then "Save the Appliance Configuration".

Configure the Appliance Rule Catalogs

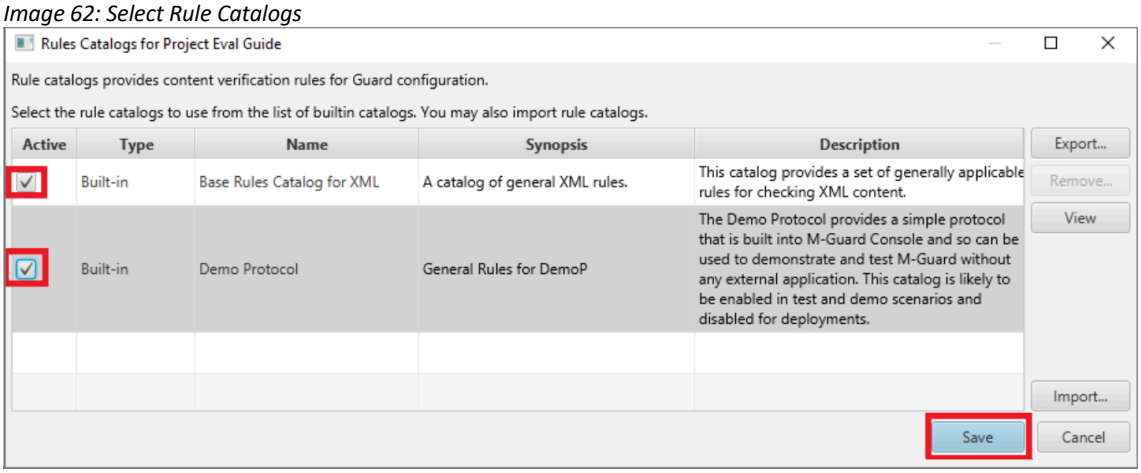
You now need to configure the Rule Catalogs. Select "Project > Rule Catalogs" (Image 61).

Image 61: Configure Rule Catalogs



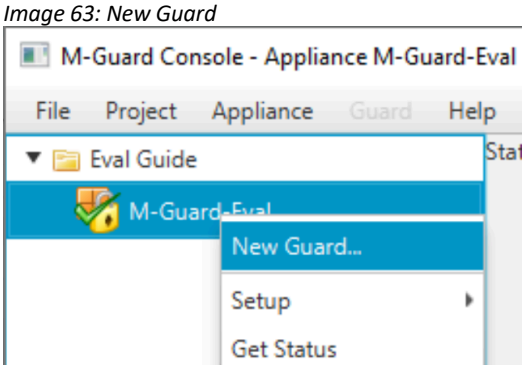
In the next screen (Image 62), tick the checkboxes for both sample catalogs and click [**Save**].

Image 62: Select Rule Catalogs



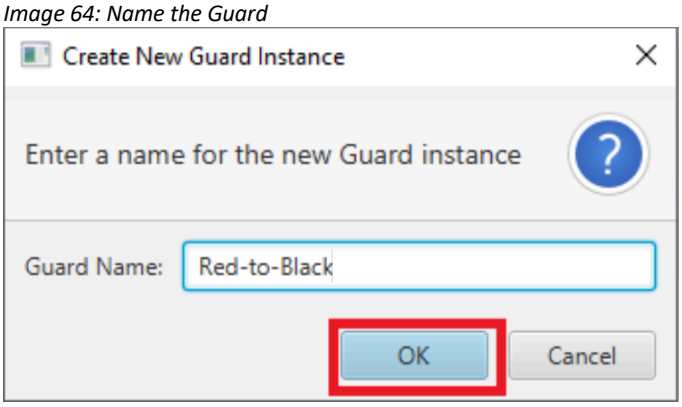
You are now ready to add a Guard Instance to your Guard Appliance. Right-click on the Appliance (Image 63) and select "New Guard".

Image 63: New Guard



Enter a name for your Guard (in Image 64, this is "Red-to-Black") and click [**OK**].

Image 64: Name the Guard

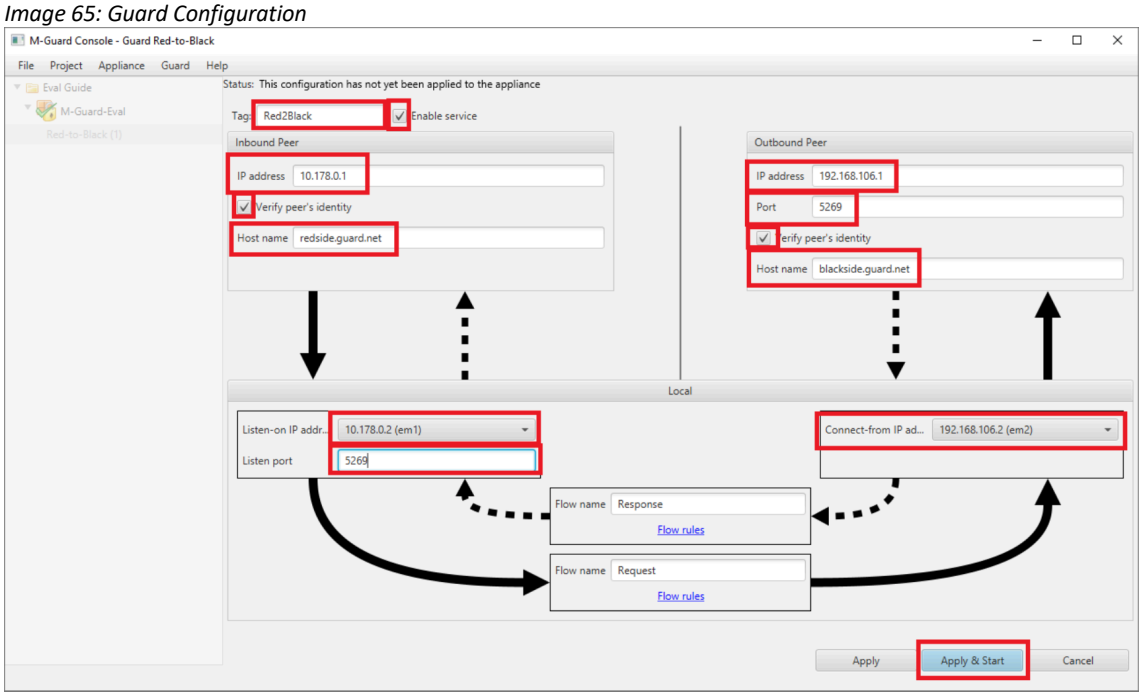


In the screen then displayed (Image 65), you'll need complete the following tasks:

- Enter a **Tag**, this can be any friendly name.
- Tick the **Enable Service** checkbox.
- The **Inbound Peer IP Address** should be the "Red Network" IP Address of the Host Machine that you connect to the appliance from, using M-Guard Console.
- On the **Inbound Peer** tick the "Verify Peer's identity" Checkbox.

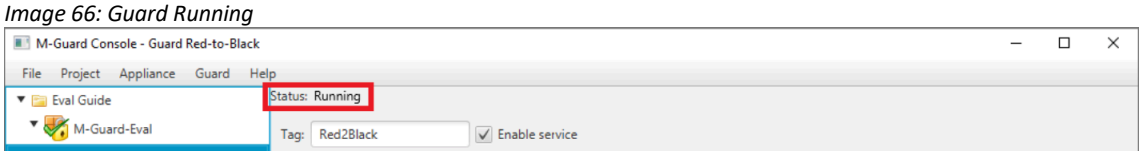
- Enter an **Inbound Peer IP Host Name** which can be any friendly hostname you like.
- The **Listen on IP Address** on **Local** should be the "Red Network" IP Address of the Guard Appliance.
- Choose a suitable **Port** for the Local "Listen Port".
- On the Outbound Peer tick the **Verify Peer's identity** checkbox.
- The **Outbound Peer IP Address** should be the "Black Network" IP Address of the Host Machine that you connect to the appliance from, using M-Guard Console.
- The **Outbound Peer IP Host Name** can be any friendly hostname you like.
- Choose a suitable **Port** for the Outbound Peer Port.
- The **Connect From IP Address** on "Local" should be the "Black Network" IP Address of the Guard Appliance.

Image 65: Guard Configuration



Click on [Apply & Start] and you should now see the Guard status as "Running" (Image 66).

Image 66: Guard Running

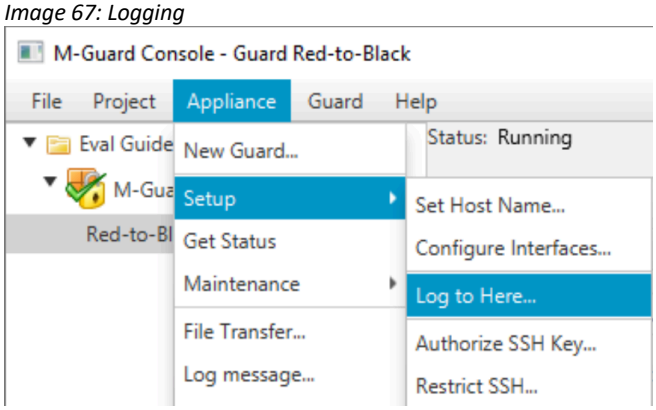


Configure Syslog Logging

You'll now need to configure the "Syslog" logging. You should have installed and started the Visual Syslog Server on the Host Machine before starting this step.

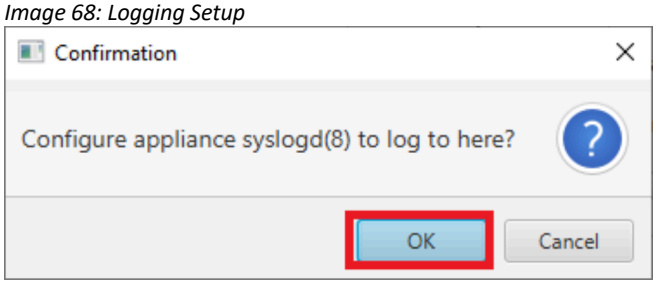
Select "Appliance > Setup > Log to Here..." (Image 67).

Image 67: Logging



Click [**OK**] on the confirmation screen (Image 68) and then Save the Appliance configuration.

Image 68: Logging Setup



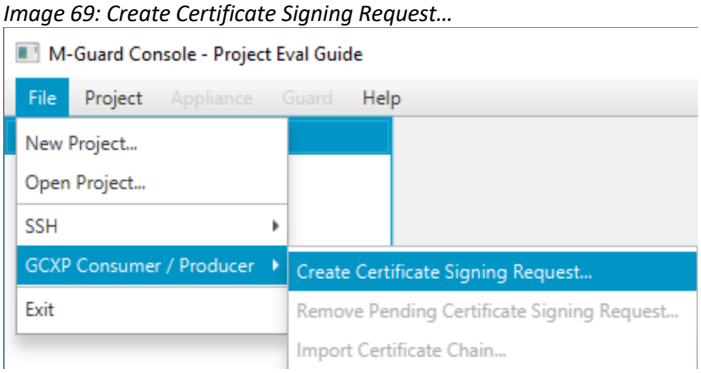
Your Guard is now ready to test.

Testing Your Guard

To test the Guard we run two custom instances of M-Guard Console that have additional command line options, but before we do that we must configure the TLS Certificates for them.

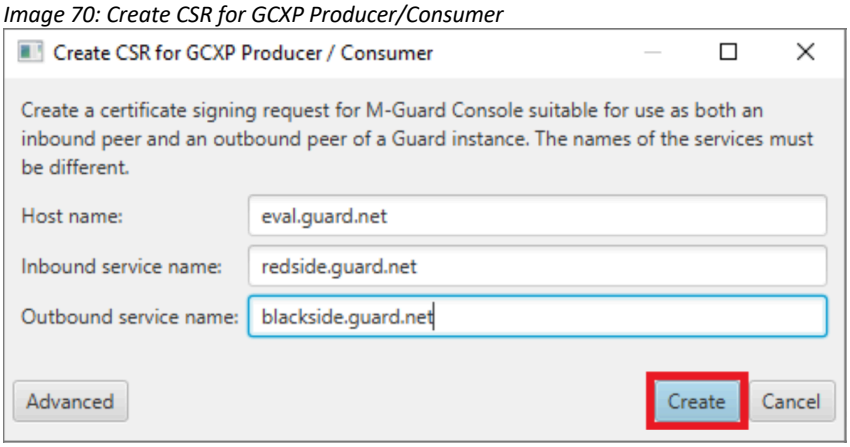
From the M-Guard Console Menu (Image 69) select "File > GCXP Consumer/Producer > Create Certificate Signing Request…."

Image 69: Create Certificate Signing Request…



In the next screen (Image 70), enter the values you've just entered on your Guard instance and then click [**Create**].

Image 70: Create CSR for GCXP Producer/Consumer



Select a folder for the CSR (Image 71) and then click [**OK**] on the confirmation screen (Image 72).

Image 71: Select Folder

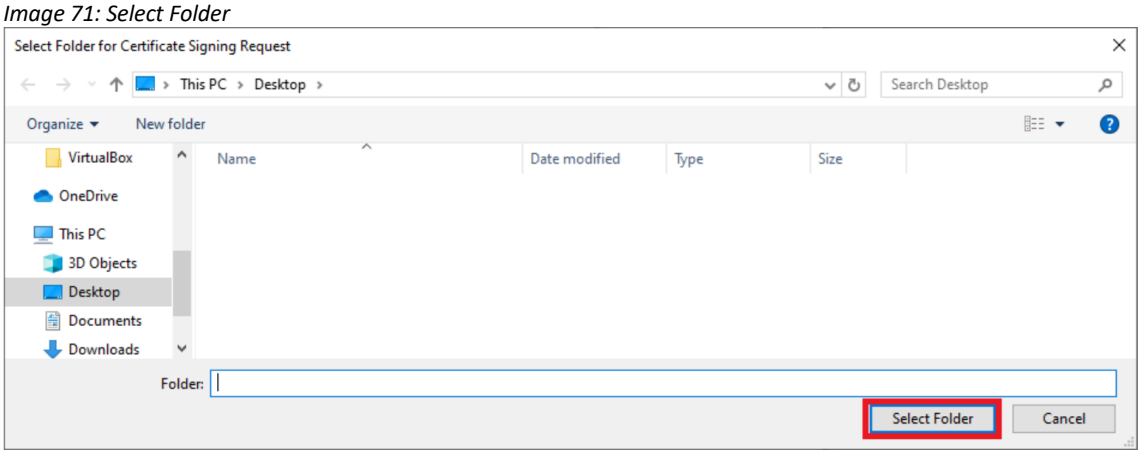
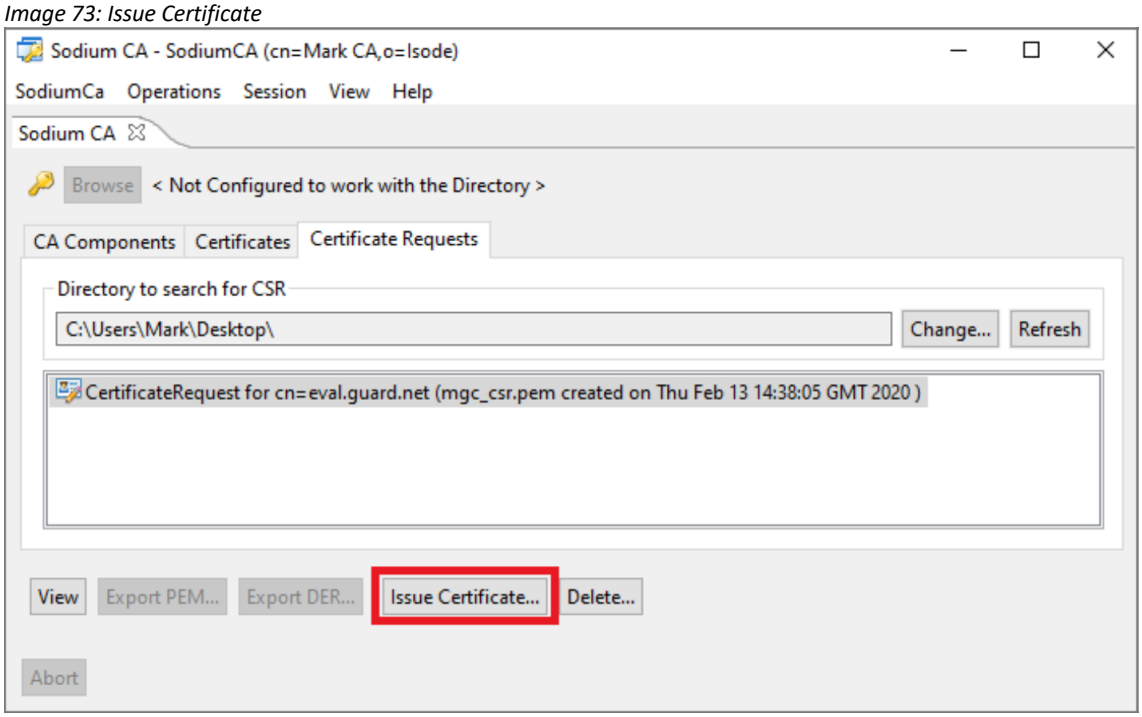


Image 72: CSR Created

Now return to Sodium CA [**Refresh**] the Certificate Requests tab, select the certificate and click [**Issue Certificate…**] (Image 73).

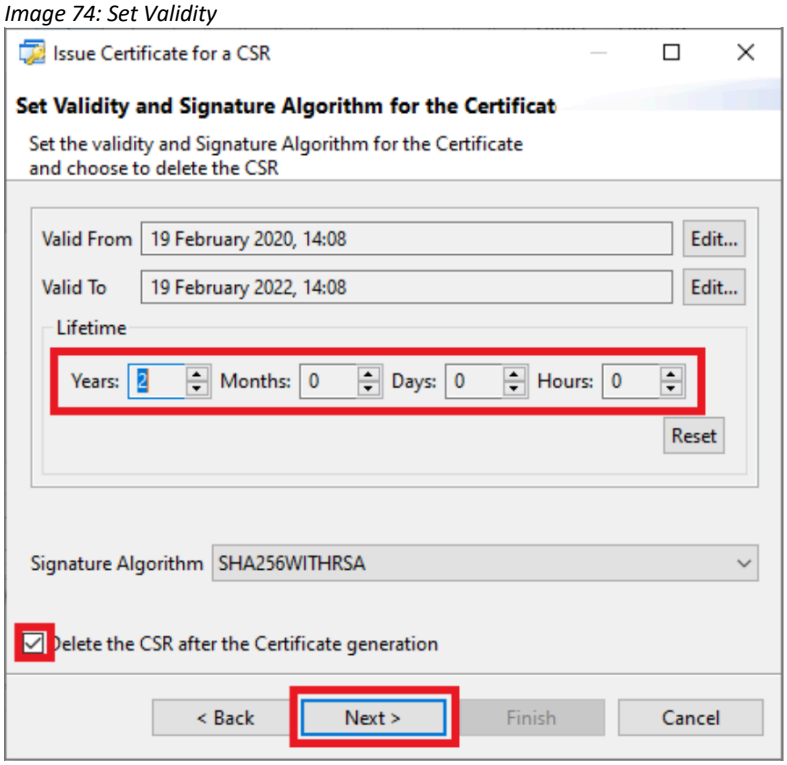
Image 73: Issue Certificate



On the three screens that follow; "Certificate Signing Request", "Select and Add Subject Alternative Names" and "Select and Create X.509 Extensions", accept the default settings and click [**Next**] on each screen.

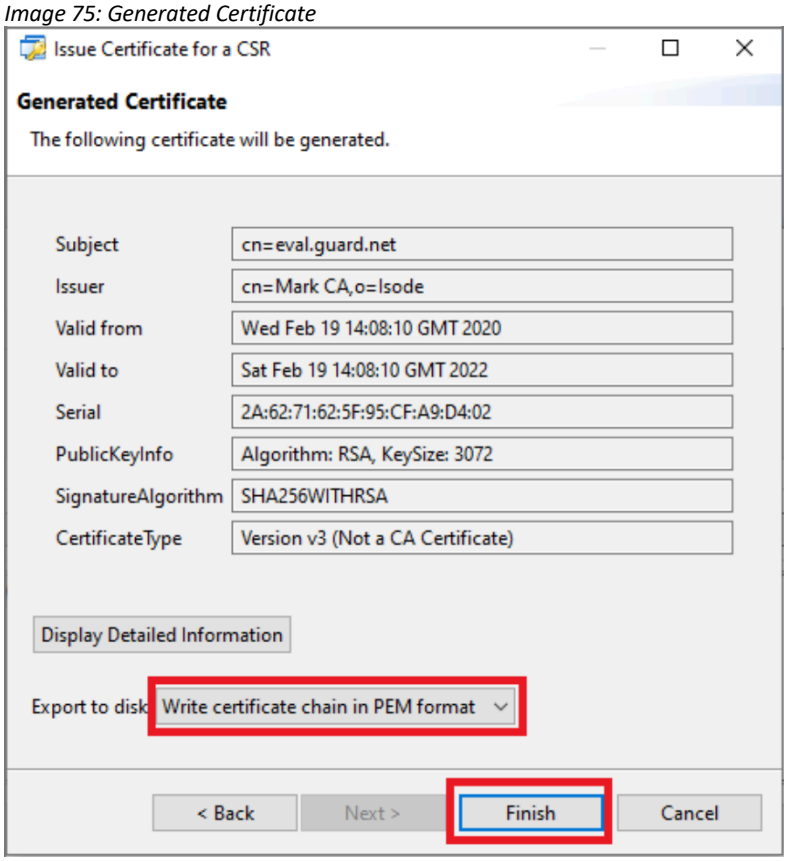
On the "Set Validity" screen (Image 74) set the "Lifetime" and tick the "Delete the CSR after the Certificate generation" checkbox and click [**Next**].

Image 74: Set Validity



In the "Generated Certificate" screen (Image 75) select the) select [Write certificate chain in PEM format] from the "Export to disk" dropdown, then click [**Finish**].

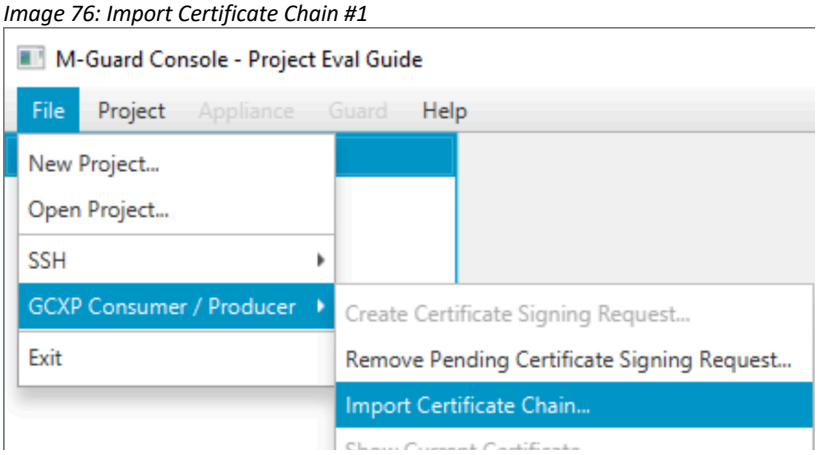
Image 75: Generated Certificate



Click [**OK**] on the confirmation screen (not shown) and return to M-Guard Console.

From the M-Guard Console menu (Image 76) select “File > GXCP Consumer/Producer > Import Certificate Chain...”.

Image 76: Import Certificate Chain #1



Select the “mgc_gsr_chain.pem” file (Image 77), click [**Open**] and then click [**OK**] on the confirmation message (Image 78).

Image 77: Import Certificate Chain #2

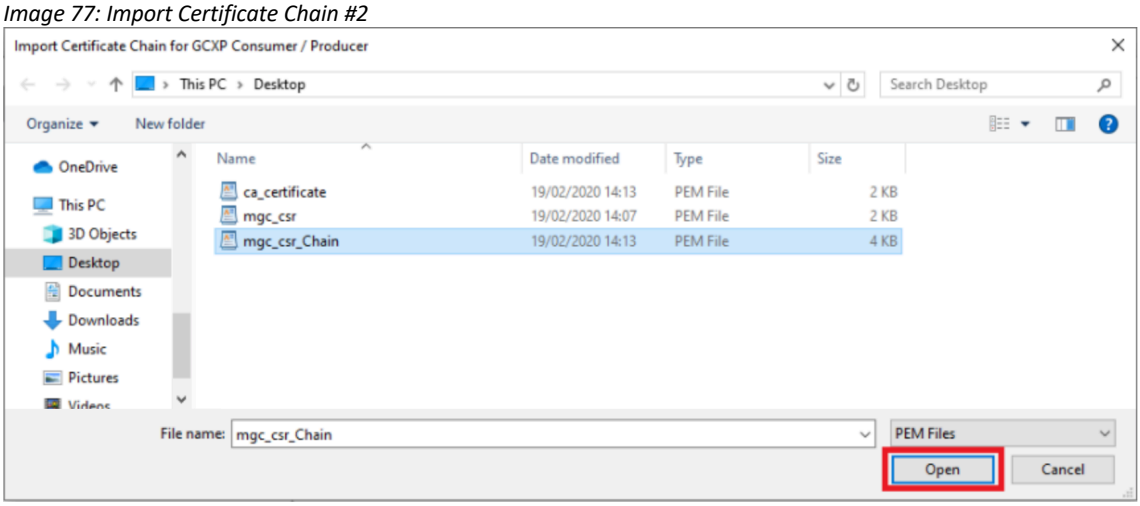
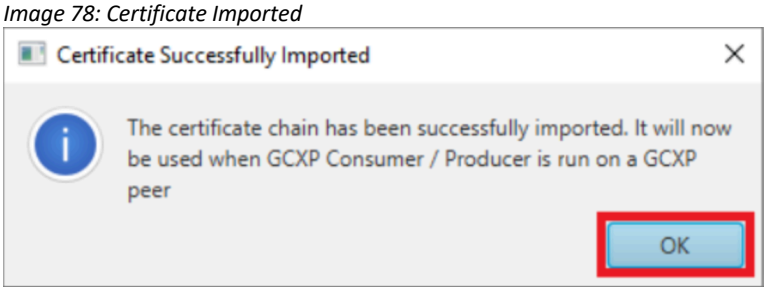


Image 78: Certificate Imported



“Save the Appliance Configuration”.

Configuring/Running the Consumer

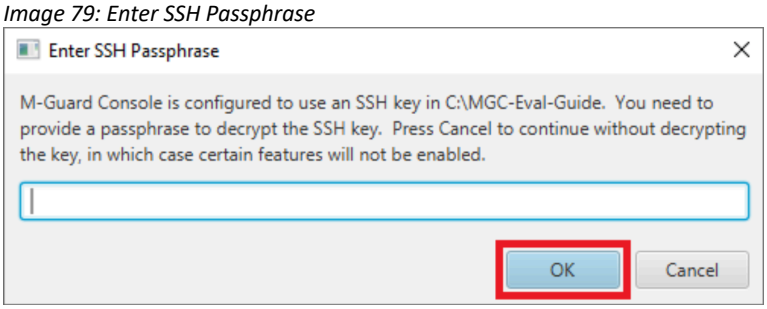
From a new Command Prompt navigate to the same folder that you are running M-Guard Console from and type the following command:

```
"C:\Program Files\OpenJDK for Isode\openjdk\jdk-
```

```
11.0.2\bin\java.exe" -jar M-Guard-Console-1.0.2.jar --gcxp-
consumer
```

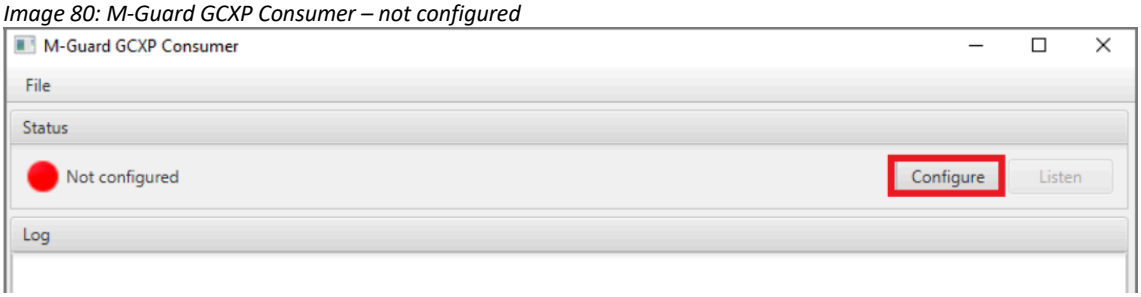
When prompted (Image 79) enter the passphrase you use for M-Guard Console and click [**OK**].

Image 79: Enter SSH Passphrase



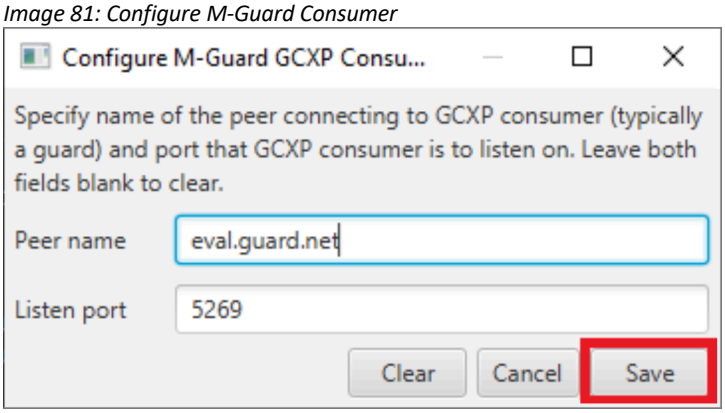
In the M-Guard GCXP Consumer screen (Image 80) click on [**Configure**].

Image 80: M-Guard GCXP Consumer – not configured



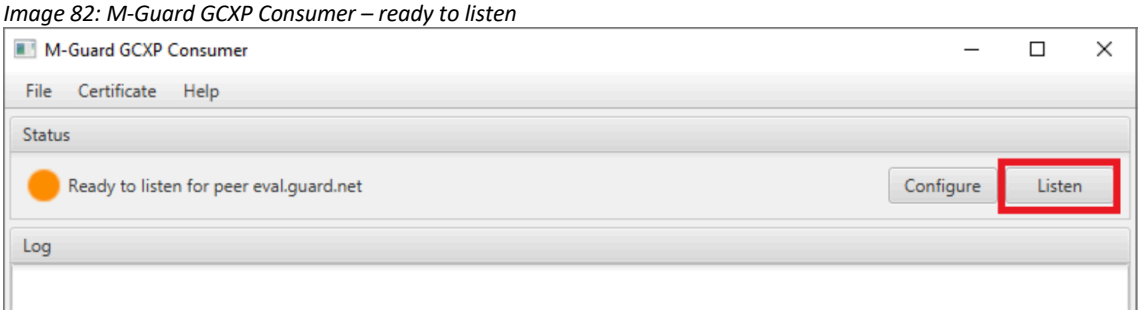
Next, enter the Hostname of your Appliance as the "Peer name" and the Port you configured in the Outbound Peer of your Guard (Image 81). Click [**Save**].

Image 81: Configure M-Guard Consumer



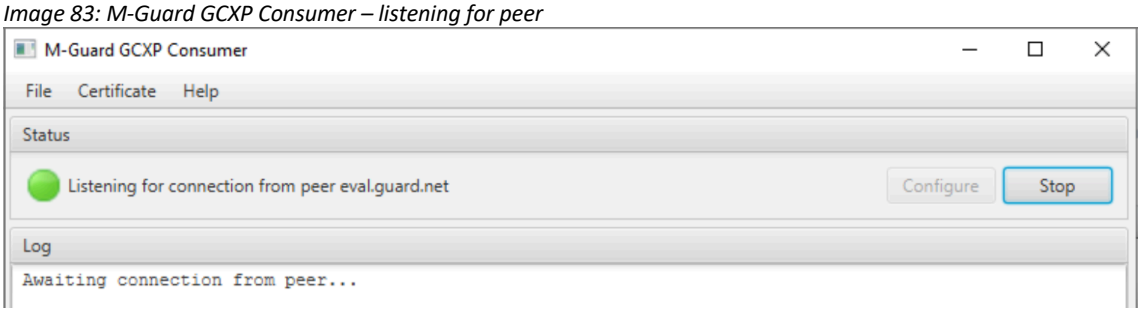
The M-Guard GCXP Consumer screen (Image 82) will indicate that it is ready to listen for the peer, so click on [**Listen**].

Image 82: M-Guard GCXP Consumer – ready to listen



You will see that the status has now changed (Image 83). You are now ready to run the "Producer".

Image 83: M-Guard GCXP Consumer – listening for peer



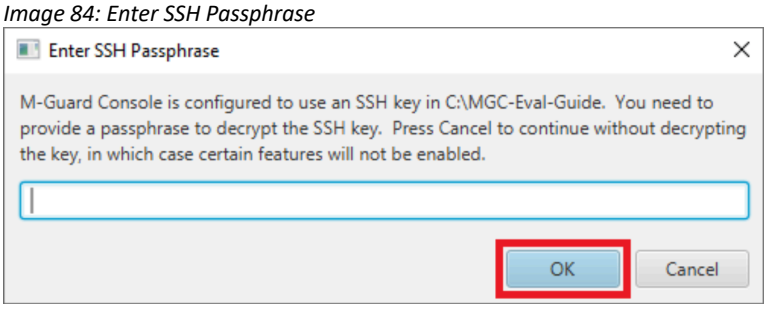
Configuring/Running the Producer

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

```
"C:\Program Files\OpenJDK for Isode\openjdk\jdk-
11.0.2\bin\java.exe" -jar M-Guard-Console-1.0.2.jar --gcxp-
producer
```

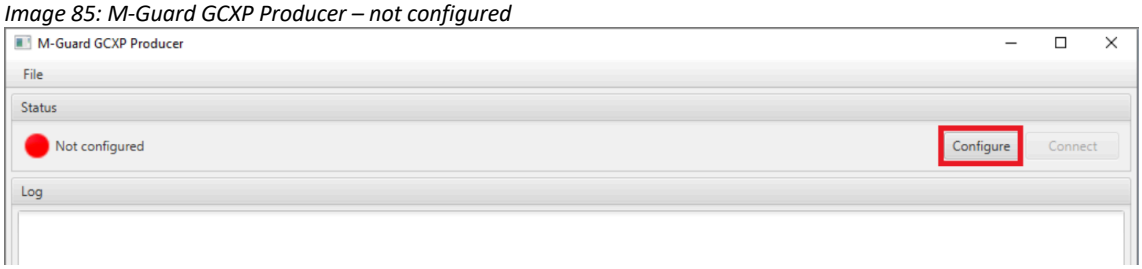
When prompted (Image 84) enter the passphrase you use for M-Guard Console and click [**OK**].

Image 84: Enter SSH Passphrase



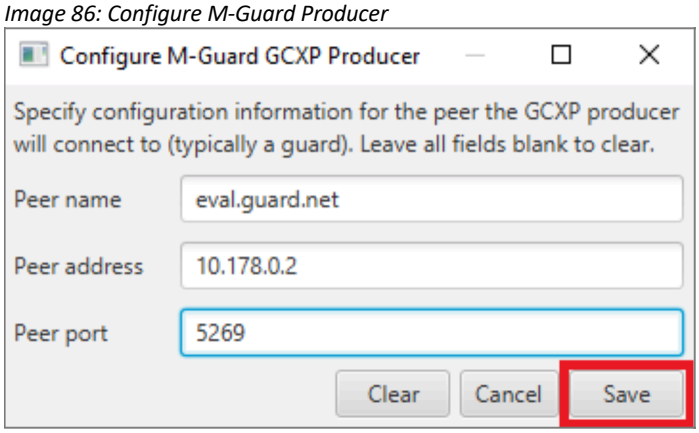
In the M-Guard GCXP Producer screen (Image 85) click on [**Configure**].

Image 85: M-Guard GCXP Producer – not configured



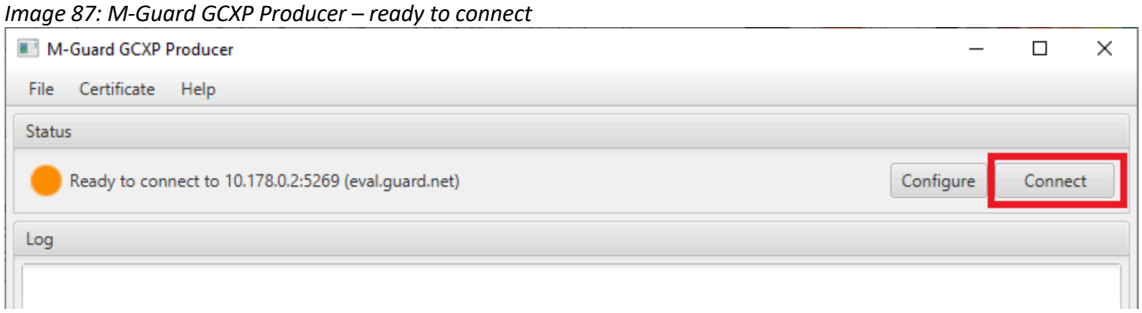
Next enter the Hostname of the Appliance, the IP Address and Port the Inbound Peer is listening on (Image 86) and click [**Save**].

Image 86: Configure M-Guard Producer



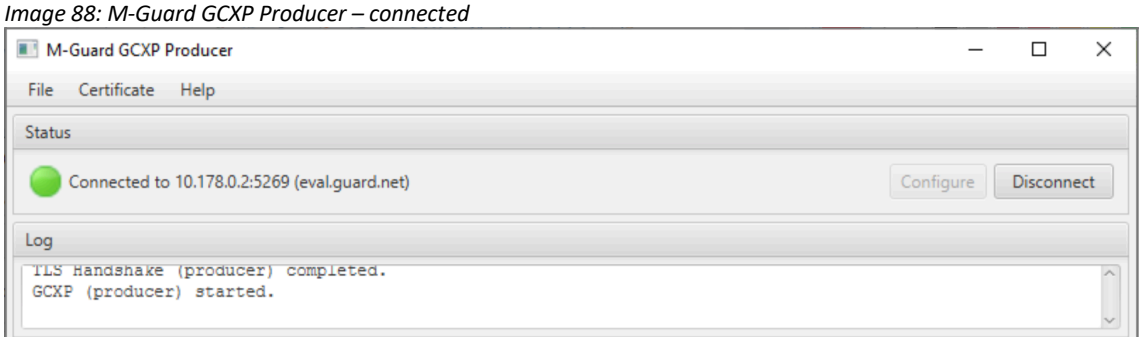
The Producer screen (Image 87) will indicate that it is ready to connect, so click on [**Connect**].

Image 87: M-Guard GCXP Producer – ready to connect



You will see that the status has now changed (Image 88). You are now ready to test the Guard by trying to pass some "broken" XML.

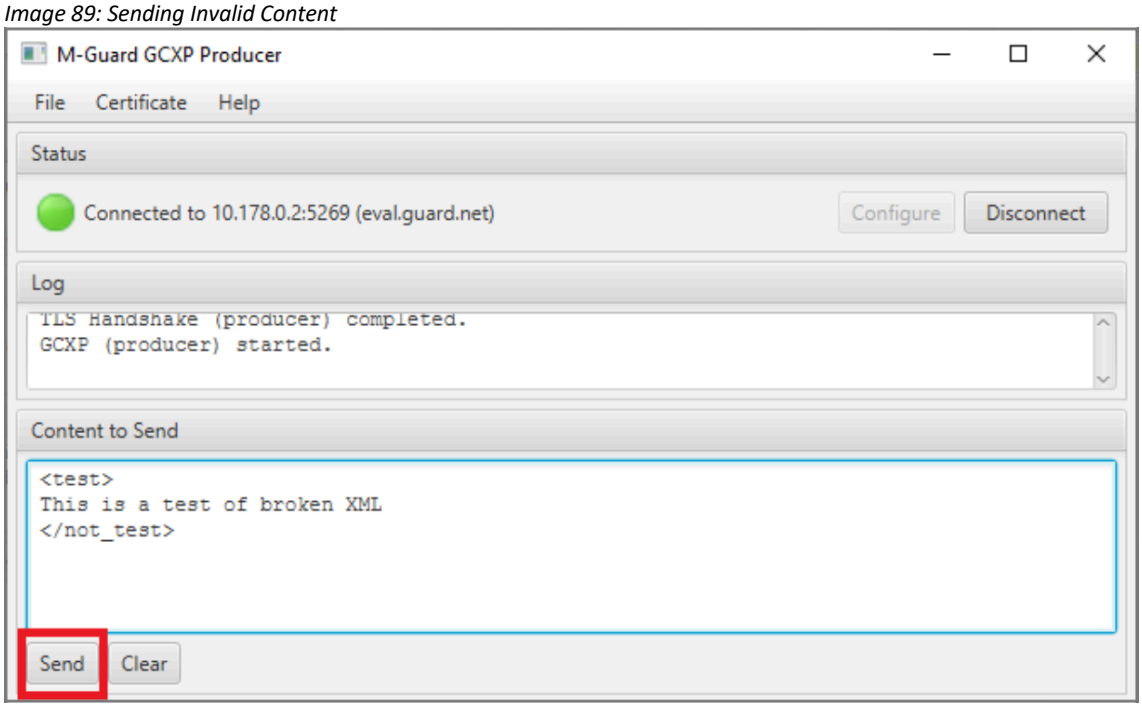
Image 88: M-Guard GCXP Producer – connected



Testing the Guard with broken XML

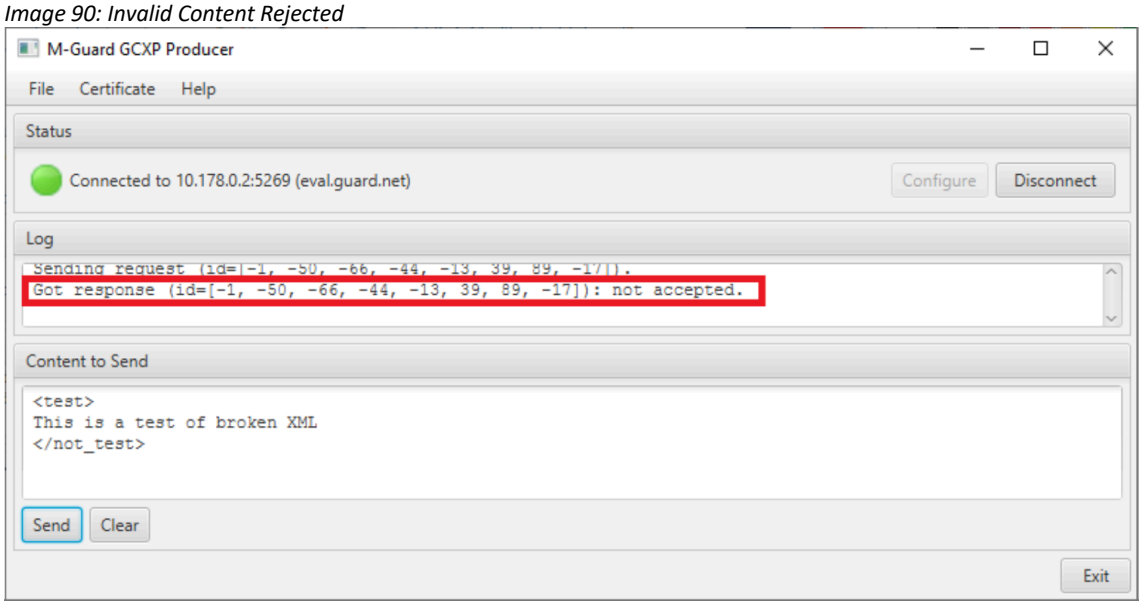
In the Producer screen enter some “broken” XML in the Content to Send area (Image 89) and then click [**Send**].

Image 89: Sending Invalid Content



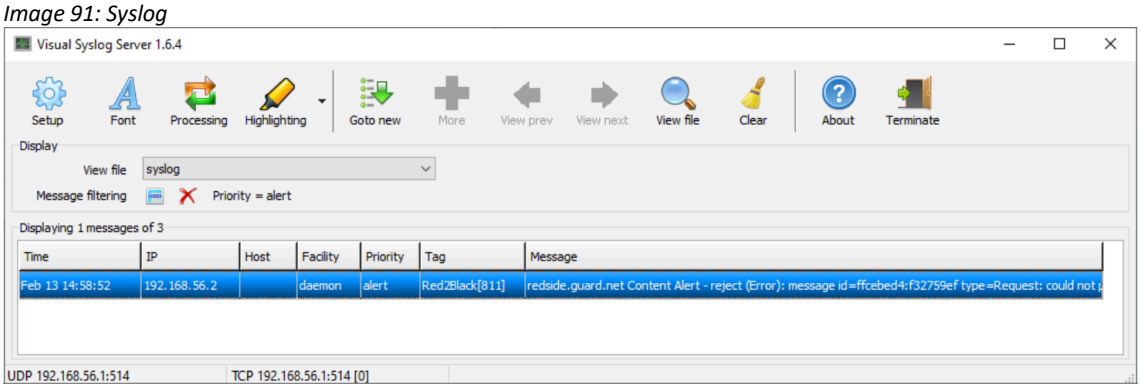
You will see that in the Log Frame (Image 90), the content has been rejected.

Image 90: Invalid Content Rejected



You will also see an error message in the Syslog server (Image 91).

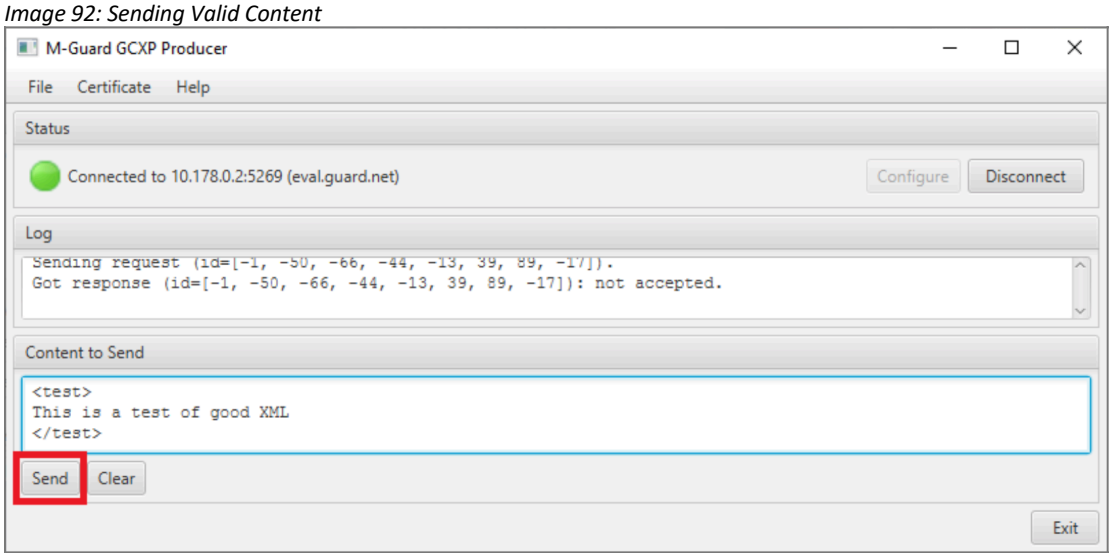
Image 91: Syslog



Testing the Guard with valid XML

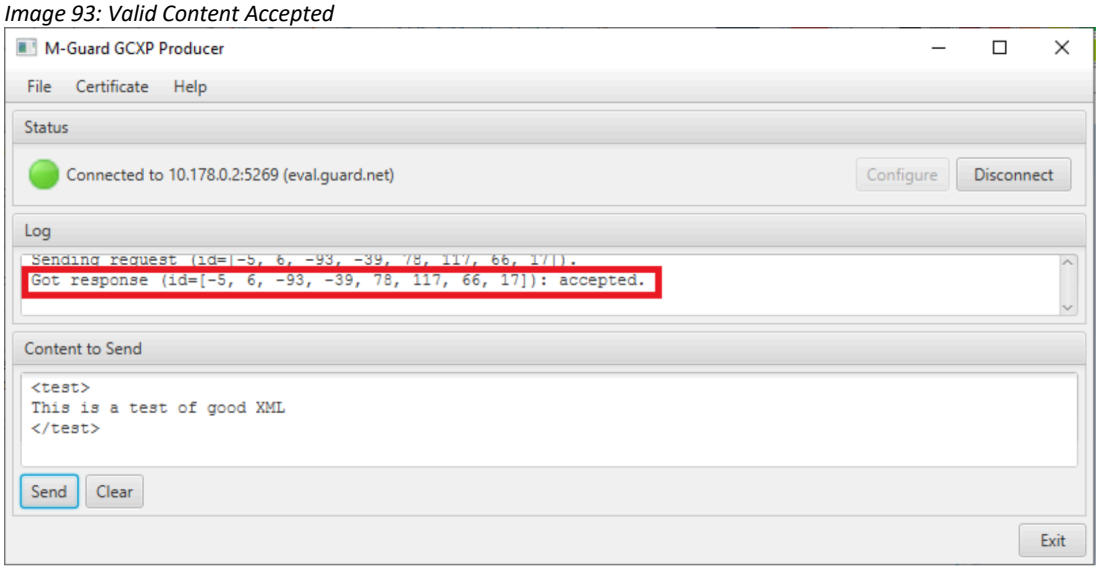
In the Producer screen enter some valid XML (Image 92) and click [**Send**].

Image 92: Sending Valid Content



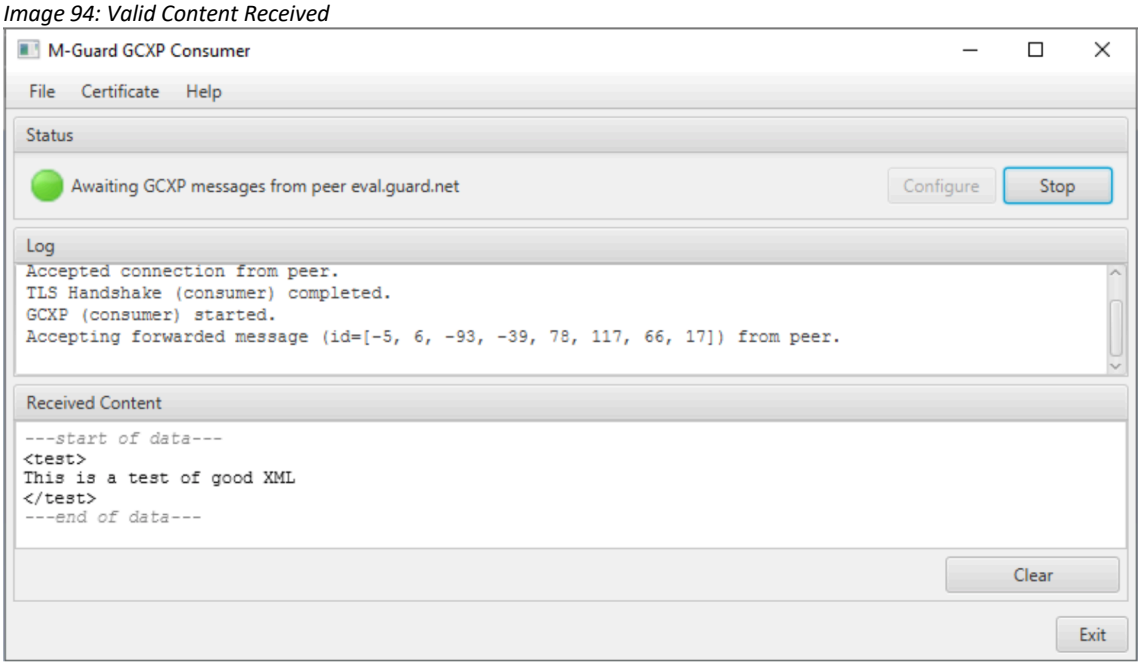
You will see that in the Log Frame (Image 93), the content has been accepted.

Image 93: Valid Content Accepted



Switching to the Consumer, you'll see that the valid content has been received by the Consumer (Image 94) showing that the Guard is working.

Image 94: Valid Content Received



What Next?

More information on M-Guard can be found on the Isode website at *https://www.isode.com/products/m-guard.html*.

Detailed configuration and operational information Icon-5066 can be found in the Icon-5066 Administration Guide available from the Isode website at www.isode.com/support/help.html.

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