

### M-Guard Evaluation Guide

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

### Contents

Introduction	3
Objectives	3
Using Isode Support	3
Preparation	4
Network Planning	4
Product Downloads	4
Installation on VirtualBox	6
Configure Network Settings	8
Installation on Hyper-V	10
Configuring the M-Guard Appliance with M-Guard Console (Part 1)	18
Setting up and Connecting to the Appliance	18
Configuring the Appliance	21
Setting up Sodium CA to provide the Certificates M-Guard	25
Configuring the M-Guard Appliance with M-Guard Console (Part 2) Generate Certificate Signing Request Load TLS Certificate Load TLS Trust Anchor Configure the Appliance Rule Catalogs Configure Syslog Logging	29 32 33 33 35
Testing Your Guard	37
Configuring/Running the Consumer	40
Configuring/Running the Producer	42
Testing the Guard with broken XML	44
Testing the Guard with valid XML	45
What Next?	47
Copyright	48

### 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.



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).





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 emo,emi & em2 on Virtual Box and hno, hni & hnz 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).

mag	ge 3: Host Network Manag	er
<b>3</b>	Oracle VM VirtualBox Manager	
File	Machine Help	
Þ	Preferences	Ctrl+G
n	Import Appliance	Ctrl+I
R	Export Appliance	Ctrl+E
0	Virtual Media Manager	Ctrl+D
	Host Network Manager	Ctrl+W
2	Network Operations Manager	
G	Check for Updates	
	Reset All Warnings	
$\checkmark$	Exit	Ctrl+Q

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

Image 4: Virtual	Box Manager				
Oracle VM VirtualB	ox Manager			_	
File Help					
		Virtual Media Manager 😫	Host Network Manager	Machine Tools	Global Tools
Create Remove Prop	perties				
Name	^		IPv4 Address/Mask	IPv6 Address/Mask	DHCP Server
VirtualBox Host-Only Et	hernet Adapter		10.178.0.1/16		🗹 Enable
VirtualBox Host-Only Et	hernet Adapter #2		192.168.56.1/24		Enable
Adapter DHCP Serve	er				
O Configure Adapter A	utomatically				
Configure Adapter M	lanually				
IPv4 Address:	10.178.0.1				
IPv4 Network Mask:	255.255.0.0				
IPv6 Address:	fe80::fcd3:4428:6464:ed3b				
IPv6 Prefix Length:	64				
				Apply	Reset

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).

Please choose a virtua	al appliance	file to import								×
← → ~ ↑ <mark> </mark> >	This PC $\rightarrow$	New Volume (D:) > Shar	red Data → M-G	Guard RC → VirtualBo	x v	Q	Search	VirtualBox		P
Organize 🔻 New fo	older								-	?
OneDrive	^ Nam	ne ^		Date modified	Туре	Size				
This PC	<b>9</b>	M-Guard-1.0.3-vbox-full		04/02/2020 23:08	Open Virtualizatio	115	,759 KB			
3D Objects										
Desktop										
🔮 Documents										
🕂 Downloads										
b Music										
Pictures										
Videos										
Windows (C:)										
New Volume (D:										
🛫 sales (\\mary) (K										
🛖 mt (\\mary) (L:)										
💣 Network	~									
Fil	e name: 🚺	1-Guard-1.0.3-vbox-full				~	Open	Virtualization	n Format (*.	.o ~
							(	)pen	Cance	1

#### Image 4: Select Virtual Appliance

#### Image 5: Import Virtual Appliance

ppliance to import	
D:\Shared Data\M-Guard RC\Virt.	JalBox\M-Guard-1.0.3-vbox-full.ova
ppliance settings	
Virtual System 1	,
😪 Name	M-Guard Appliance
Product	M-Guard
🥥 Vendor	Isode Limited
🥥 Vendor-URL	http://www.isode.com
Version	M-Guard 1.0.3
Description	Isode's XML Guard virtual appliance image for VirtualBox. For suppo
🗮 Guest OS Type	FreeBSD (64-bit)
CPU	2
RAM	1024 MB
🛃 Network Adapter	Intel PRO/1000 MT Desktop (82540EM)
- N. IAI.	

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 🗿 Oracle VM VirtualBox Manager × File Machine Help A 6 👼 Snapshots 🗯 🧾 Details 🞇 New Settings Discard Start Global Tool 🧕 General Preview uard Appliance owered Off () Name: M-Guard Appliance Operating System: FreeBSD (64-bit) 🚺 System Base Memory: 1024 MB **M-Guard Appliance** Processors: Boot Order: Acceleration: Optical, Hard Disk VT-x/AMD-V, Nested Paging 📃 Display Video Memory: Remote Desktop Server: Video Capture: 10 MB Disabled Disabled Storage Controller: SATA SATA Port 0: M-Guard-1.0.3-vbox-full-disk001.vmdk (Normal, 4.00 GB) Di Audio Disabled P Network Adapter 1: Intel PRO/1000 MT Desktop (Host-only Adapter, 'vboxnet0') Adapter 2: Intel PRO/1000 MT Desktop (Not attached) Adapter 3: Intel PRO/1000 MT Desktop (Not attached) Adapter 4: Intel PRO/1000 MT Desktop (Not attached) 🤌 USB 📄 Shared folders None Description Isode's XML Guard virtual appliance image for VirtualBox. For support, contact <support@isode.com>

#### **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

Ø M-Guard Appliance	e - Settings	?	×
🧾 General	Network		
🛒 System	Adapter 1 Adapter 2 Adapter 3 Adapter 4		
📃 Display	Enable Network Adapter		
5 Storage	Attached to: Host-only Adapter 🔻		_
Audio	Name: VirtualBox Host-Only Ethernet Adapter #3		•
Network			
🚫 Serial Ports			
🏈 USB			
Shared Folders			
User Interface			
	ОК	Can	icel

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.

Huper-V Manager							_	×
								~
File Action View Help								
🗢 🌳 🙎 🖬 🚺 🖬								
Hyper-V Manager	Virtual Machines						Actions	
BLOODHOUND		Chata	CDUUIssas	Accienced Management	Uniting		BLOODHOUND	-
	Name	State	CPU Usage	Assigned Memory	Uptime		🖳 Quick Create	
	No virtual machines were found on this server.					New	•	
							Import Virtual Machine	
	< 2				>	Hyper-V Settings		
	Checkpoints				٢	Virtual Switch Manager		
		Marcak					Virtual SAN Manager	
			lai machine selecte	± <b>d</b> .			- Edit Dick	
							P Inspect Disk	
	D-t-1					_	Stop Service	
	Details						X Remove Server	
		N	o item selected.				8 Refresh	
							View	•
							👔 Help	
							1	

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

Virtual Switch Manager for BLOODHOUNE	) – – ×
<ul> <li>Virtual Switches         <ul> <li>New virtual network switch</li> <li>Default Switch Default Network</li> <li>Global Network Settings</li> <li>MAC Address Range 00-15-5D-01-76-00 to 00-15-5D-0</li> </ul> </li> </ul>	Create virtual switch do you want to create?  External Internal Private  Create Virtual switch that can be used only by the virtual machines that run on this physical computer, and between the virtual machines and the physical computer. An internal virtual switch does not provide connectivity to a physical network connection.
	OK Cancel Apply

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

 $\times$ 

\_

#### Image 11: Naming Virtual Switch

Virtual Switch Manager for BLOODHO	UND
Virtual Switches	T. Virtual Switch Properties
📑 New virtual network switch	
🗉 🚜 Default Switch	Name:
Default Network	Red Network
	Notes:

🗉 🚣 Default Switch	Name:
Default Network	Red Network
Internal only	Notes:
Global Network Settings	^
MAC Address Range 00-15-5D-01-76-00 to 00-15-5D-0	
	Connection type
	What do you want to connect this virtual switch to?
	O External network:
	Intel(R) Wi-Fi 6 AX200 160MHz
	Allow management operating system to share this network adapter
	Internal network
	VLAN ID  Enable virtual LAN identification for management operating system  The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.  2
	Remove
	OK Cancel Apply

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
-----------	---------	----------	----------

🕌 Virtual Switch Manager for BLOODHOUND	- 🗆 X
<ul> <li>Virtual Switches         <ul> <li>New virtual network switch</li> <li>Red Network Internal only</li> <li>M-Guard Management Internal only</li> <li>Black Network Internal only</li> <li>Default Switch Default Network</li> <li>Global Network Settings</li> <li>MAC Address Range 00-15-5D-01-76-00 to 00-15-5D-0</li> </ul> </li> </ul>	Create virtual switch What type of virtual switch do you want to create?  External Internal Private Create Virtual Switch Creates a virtual switch that binds to the physical network adapter so that virtual machines can access a physical network.
	OK Cancel Apply

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

Image 13: Windows Network Connections

P Network Connections	– 🗆 X
$\leftarrow \  ightarrow \$	✓ ♂ Search Network Connections ,
Organise 🔻	S: - II ?
Bluetooth Network Connection Not connected Bluetooth Device (Personal Area Ethernet Network Realtek PCIe GbE Family Controller Hyper-V Virtual Ethernet Adapter .	vEthernet (Default Switch) Enabled Hyper-V Virtual Ethernet Adapter
VEthernet (M-Guard Management) Unidentified network Hyper-V Virtual Ethernet Adapter Virtual Ethernet Adapter WiFi Not connected Intel(R) Wi-Fi 6 AX200 160MHz	
7 items	8== 📼

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

Hyper-V Manager								_		×
File Action View Help										
🗢 🄿 🙍 🖬 🛛 🖬										
Hyper-V Manager	Virtual Machines					1	Actions			
BLOODHOUND		<b>C</b> 1.1	CDUU		11.0	11	BLOODHOUND			-
Wirtual Machines       Virtual Machines       Actions         Name       State       CPU Usage       Assigned Memory       Uptime         No vitual machines were found on this server.       Quick Create       New         Checkpoints       Other State       Virtual Machine										
		No virtual mach	ines were found on	this server.			New			•
							🔒 Import Virtual Machine			
	<				>		Hyper-V Settings			
	Checkpoints				۲		🚰 Virtual Switch Manager			
		No virt	ual machine selecte	ed.			🛃 Virtual SAN Manager			
							🚅 Edit Disk			
							🚆 Inspect Disk			

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.

Import Virtual Machine		×
Locate Folder	,	
Before You Begin	Specify the folder containing the virtual machine to import.	
Locate Folder	Folder:	Browse
Select Virtual Machine		
Choose Import Type		
Summary		
	< Previous Next > Finish	Cancel

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

Image 16: Locate Folder		
Import Virtual Machine		×
Locate Folder		
Before You Begin	Specify the folder containing the virtual machine to import.	
Locate Folder	Folder: C:\Isode Software\M-Guard-1.0.3-hyperv-full\M-Guard Appliance\	Browse
Select Virtual Machine		
Choose Import Type		
Summary		
	< Previous Next > Finish	Cancel

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

Image 17: Select Virtual Mac	hine	
Import Virtual Machine		×
Select Virtual	Machine	
Before You Begin	Select the virtual machine to import:	
Locate Folder	Name	Date Created
Select Virtual Machine	M-Guard Appliance	26/02/2019 10:46:42
Choose Import Type		
Summary		
f		
	< Previous	Next > Finish Cancel

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	Туре
-------	-----	--------	--------	------

Import Virtual Machine	×
🖻 Choose Imp	oort Type
Before You Begin Locate Folder Select Virtual Machine	Choose the type of import to perform:
Choose Import Type Summary	O Copy the virtual machine (create a new unique ID)
	< Previous Next > Finish Cancel

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

Import Virtual Machine		×
Completing I	mport Wizard	
Before You Begin Locate Folder	You are about to perform the following Description:	operation.
Select Virtual Machine	Virtual Machine:	M-Guard Appliance
Choose Import Type	Import file:	C: \Isode Software \M-Guard-1.0.3-hyperv-full \M-Guard Applian Copy (generate new ID)
Choose Destination	Virtual machine configuration folder:	C:\ProgramData\Microsoft\Windows\Hyper-V\
Choose Storage Folders	Checkpoint folder:	C:\ProgramData\Microsoft\Windows\Hyper-V\
Summary	Smart Paging file store:	C:\ProgramData\Microsoft\Windows\Hyper-V\
	Virtual hard disk destination folder:	C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\
	<	>
	To complete the import and close this v	vizard, dick Finish.
	[	< Previous Next > Finish Cancel

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

Hyper-V Manager						- 0	$\times$
File Action View Help							
🔶 🔿 🙇 📰 🚺							
📅 Hyper-V Manager	Minturel Marshimer					Actions	
BLOODHOUND		<b>C</b> 1.1	CDUU	A	U. C.	BLOODHOUND	· ^
	Name	State	CPU Usage	Assigned Memory	Uptime	Quick Create	
		Off				New	•
						强 Import Virtual Machine	
	<				>	Hyper-V Settings	
	Checkpoints				۲	🚰 Virtual Switch Manager	
		The selected	virtual machine has no	🔒 Virtual SAN Manager			
						🚄 Edit Disk	
						🚆 Inspect Disk	
		points  The selected vitual machine has no checkpoints.  It is selected vitual machine has no checkpoints.  It is selected vitual machine has no checkpoints.  It is selected vitual machine has no checkpoints. It is selected vitual machine has no					
	M-Guard Appliance					× Remove Server	
	C		19/02/2020 15:07/	22 Churteredt 1		🖏 Refresh	
	Con	figuration Version	: 9.0	clustered.	NO	View	•
	Gen	eration:	1			7 Help	
	Note	25:	Isode's XML Guard	virtual		M-Guard Appliance	
			Appliance for Hyper-V. For support, contact				
			<support@isode.com< td=""><td>m&gt;.5ub</td><td></td><td>Settings</td><td></td></support@isode.com<>	m>.5ub		Settings	
	Summary Memory Ne	tworking					- □ ×

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.

1-Guard Appliance	$\sim$	⊴ ♦ 0		
Hardware	^	Add Hardware		
📔 Add Hardware		-		
BIOS		You can use this setting to add devices to your virtual machine.		
Boot from IDE		Select the devices you want to add and click the Add button.		
Security		SCSI Controller		
Key Storage Drive disabled	i i	Network Adapter		
Memory		RemoteFX 3D Video Adapter		
1024 MB		Legacy Network Adapter		
Processor		Fibre Channel Adapter		
2 Virtual processors				
IDE Controller 0			Add	
🛨 🚃 Hard Drive				
M-Guard.vhdx		You can increase the storage available to a virtual machine by adding a SCSI	( controller	ł
IDE Controller 1		and attaching virtual hard disks to it. Do not attach a system disk to a SCSI of System disks must be attached to an IDE controller	controller.	
Network Adapter		System disks must be attached to an IDE controller.		
M-Guard Management				
Network Adapter				
Not connected				
Network Adapter				
Not connected				
Not connected				

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

M-Guard Appliance	~ <	▶	U					
A Hardware	^	Net	work Adapter					-
Add Hardware								
BIOS	S	pecify	the configuration of t	he network adap	ter or remove th	e network a	dapter.	
Boot from IDE	V	'irtual s	witch:					
Security		Red Ne	twork			~		
Key Storage Drive disabled		VLAN	ID					
Memory 1024 MR			nable virtual LAN iden	tification				
2 Virtual processors		The \	/LAN identifier specifie	es the virtual LAN	I that this virtual	machine wil	use for all	
IDE Controller 0		netw	ork communications tr	nrougn this netwo	ork adapter.			
🗄 🚃 Hard Drive			2					
M-Guard.vhdx								
IDE Controller 1		Bandy	vidth Management					
🗄 📮 Network Adapter			nable bandwidth man	agement				
M Cuard Management	-111	Space	fu how this potwork a	dapter utilizer p	stuark bandwidt	Roth Minir	201 102	
E 🛛 Network Adapter		Band	width and Maximum B	andwidth are me	asured in Megabi	ts per secor	nd.	
Red Network		Minim	una la marche dal blan		Athen			
Wot connected		1×1111	um banuwidun:		Mops			
+ Network Adapter		Maxir	num bandwidth:	0	Mbps			
Not connected			To logue the minimum		-	0 as the us	du e	
COM 1		U.	to leave the minimum	or maximum unr	estricted, specify	U ds trie va	siue.	
None	т	o remo	we the network adapt	ter from this virt	al machine, click	Remove		
COM 2		o reme				1101101		_
None						l	Remove	
Diskette Drive		D Us	e a legacy network ad	lapter instead of	this network ada	pter to perf	form a	
None		ne	twork-based installation	on of the guest o	perating system	or when int	egration	
Management		ser	vices are not installed	d in the guest op	erating system.			
M-Guard Appliance								
Integration Services								
Some services offered								
Julie services utrereu								

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

Hyper-V Manager								-		×
File Action View Help										
🗢 🔿 🙍 📰 🚺										
Hyper-V Manager	Virtual Machines						Actions		_	
BLOODHOUND	Name	State	CPU Usage	Assigned Memory	Untime		BLOODHOUND			<b>^</b>
	M-Guard Appliance	Off	er o osage	, asigned memory	optime		Quick Create			
							New			•
							Import Virtual Machine			
	<					>	Hyper-V Settings			
	Checkpoints					۲	🕌 Virtual Switch Manager			
The selected virtual machine has no checkpoints. 🤬 Virtual SAN Manager						🔒 Virtual SAN Manager				
	🚅 Edit Disk						🛃 Edit Disk			
							🚆 Inspect Disk			
							Stop Service			
	M-Guard Appliance						X Remove Server			
	Crea	ted:	19/02/2020 15:07:2	2 Clustered: N	lo		🖸 Refresh			
	Confi	guration Version:	9.0				View			•
	Gene	ration:	1				Help			
	Note	s:	Isode's XML Guard v appliance for Hyper-	rirtual V.			M-Guard Appliance			
			For support, contact	as Sub			- Connect			
			adpporterioude.com				Settings		_	_
	Summary Memory Net	working					( Start			~
	1									

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)		
M-Guard Appliance on BLOODHOUND - Virtual Machine Connection	_	$\times$
File Action Media Clipboard View Help		
E   ◎ ● ● ●   II I   F   E 5   🗮 🚮		
<pre>SSH host fingerprints: SHA256:yo+0+xHscCp/NxAgIDTOtDpaCiEqSwGp1i1kaZY73vk (ECDSA) MD5:13:71:5d:43:ed:09:1e:b5:51:83:ec:bb:58:ec:4e:82 (ECDSA) SHA256:Pdggs1AD5G54EVrNuuExCE1XB0Gw3A+vr6gdYLt2UWQ (ED25519 MD5:75:d8:ad:73:9a:4d:0c:ae:ea:21:e2:a9:ad:09:c3:4f (ED2551' SHA256:v1F5vYhJrcVyrjf+tuWFLNxwBF1H3Gd0dDKCEUMB1pw (RSA) MD5:06:b0:3f:26:5b:be:d6:17:ca:e5:7d:01:2b:30:5c:d0 (RSA) IPv4 link-local address: 169.254.249.192/16 (hn0) IPv6 link-local address: fe80::215:5dff:fe01:7605Amnesiacn0/64 Admin (root) password set to: n/T1QkegKnKKPD</pre>	) 9)	
M-Guard Appliance/m-guard (Amnesiac) (ttyv1)		
login:		
Status: Running		 0 🔒

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

		Hel	р	
			Status:	Message
Þ				
Þ				
	1			
	•	Guard	Guard Hel	Guard Help Status:

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

Image 26: Save Project Configuration							
Project Configuration: null (mge	ttxml) – 🗆 X						
🔻 🚘 Eval Guide	Name	Eval Guide					
	Folder	C:\MGC-Eval-Guide					
		You can now add appliance configurations to this project Add Appliance Save Project Configuration Cance	1				

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

#### Image 27: Generate SSH Keys #1

M-Guard Console - Project Eval Guide								
File	Project	Appliance	(	Guard	Help	0		
New	Project							
Open	n Project							
SSH			۲	Select	SSH I	(eys		
GCXF	Consume	/ Producer	۲	Gener	ate SS	H Keys		
Exit								

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

💽 Generate SSH Keys — 🗆							
This will generate a new SSH key pair for use by M-Guard Console and save them in the specified folder							
Directory	C:\MGC-Eval-Guide		Sele	ct			
Key Length	4096 👻	Key	Type rsa	*			
Comment	your.name@yourdomain.com						
Passphrase	•••••						
Confirm Passphrase	•••••						
		Generate	Cance	ł			

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

M-Guard Console - Project Eval Guide						
File Pro	<b>ject</b> Appliance	Guard	Help			
📄 Eval	Guide					
	Configure					
	Rule Catalogs					
		1				

#### Image 30: Add Appliance

Project Configuration: Eval Guid	e (mgc	-project.xml) —		×
🔻 🚞 Eval Guide	Name	Eval Guide		
	Folder	C:\MGC-Eval-Guide		
		You can now add appliance configurations to this Add Appliance	project ion	Cancel

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 App	liance	
Project Configuration: Eval	Guide (mgc-j	project.xml) — 🗆 X
🔻 🚞 Eval Guide	Name	M-Guard-Eval
授 No name set	User	root
	Address	fe80::a00:27ff:fe3b:7ceb
	Folder	
		✓ Automatically connect
	Status	Unable to create session
		Delete appliance
		Save Project Configuration Cancel

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

Confirmation	×
Confirmation	?
The authenticity of host 'fe80::a00:27ff;fe established. RSA key fingerprint is 7b:a6:a3:24:65:05:58:24:de:ab:1d:e9:db:91: Are you sure you want to continue conn	e3b:7ceb' can't be ce:4d. hecting? OK Cancel

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

root@fe80::a00:27ff:fe3b:7ceb -					
Password for root@:					
	ОК	Cancel			

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 Inter	rfaces		
M-Guard Console - A	ppliance M-Guard-E	/al	
File Project Appliar	nce Guard Help	)	
🔻 🚞 Eval Guide	c c	Status	: 10:29AM up 1:17, 0 user
M-Guard-Eval	New Guard	File /	etc/host.conf added to /cfg etc/hostid added to /cfg. etc/master.passwd.added.t
	Setup	•	Set Host Name
	Get Status		Configure Interfaces
	Maintenance	•	Log to Here
	File Transfer		Authorize SSH Key

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

Image 35: Interface Configuration Screen

Interface Configuration	— 🗆 X
Interface em0 -	
IP Address IP Aliases Name	
✓ Enable	
IPv4	
Address 192.168.56.2	Prefix Length 24
IPv6	
Address	Prefix Length 64
	OK Revert Cancel

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

5	
M-Guard Console - Appliance M-Guard-	Eval
File Project Appliance Guard Hel	lp
🔻 🚞 Eval Guide	Status: Connection failed: java.net.ConnectException: Connection timed out: connect
M-Guard-Eval	Error Performing Task —      X     X     There was an error performing the task     OK

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

Project Configuration: Eval Guid	le (mgc-p	project.xml) — 🗆 X
🔻 🚞 Eval Guide	Name	M-Guard-Eval
M-Guard-Eval	User	root
-	Address	192.168.56.2
	Folder	
		✓ Automatically connect
	Status	Not connected
		Delete appliance
		Save Project Configuration Cancel

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

M-Guard Console - Appliance M-Guard-Eval						
File Project Applian	ce Guard Help					
🔻 🚞 Eval Guide	▼ 📴 Eval Guide Status: 11:01AM up 13 mins, 1 us					
M-Guard-Eval		ether 08:00:27:95:23:ba				
	New Guard	tatus: active				
	Setup	Set Host Name				
	Get Status	Configure Interfaces				
	Maintenance	Log to Here				
	File Transfer	Authorize SSH Key				
	Log message	Destrict COU				

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

Image 39: Set Host Name #2			
Set Host Name			×
	Host name eval.guard.net		
		OK	Cancel

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						
M-Guard Console - Appliance M-Guard-Eval						
File	Project	Appliance		Н	elp	
<b>T</b>	Eval Guide	New Guard.			Status: 11:03AM up 15 r	
	🔏 M-Gua	Setup		۲	Set Host Name	
		Get Status			Configure Interfaces	
		Maintenanc	e	Þ	Log to Here	
		File Transfer	·		Authorize SSH Key	
		Log messag	e		Restrict SSH	

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

mage 41: Confirmation	
Confirmation	×
Authorize this public key to manage the appliance?	?
D:\M-Guard\id_guard.pub	Cancel

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

🐼 Sodium CA	_	$\times$
SodiumCa Operations Session View Help		
Sodium CA Logs 🕴		
WARNING: Attempting to create directory C:\Users\Mark\AppData\Roaming\Isode		^
🧔 Sodium CA Profile Manager	×	
Configured CAs		
	New Modify	

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

🔁 New CA		—		Х
Set Properties of the	Certificate Authority			
Use this page to set the d directory for the CA	isplay name, key passphrase and CADB			
Sodium CA Profile Name CADB Directory	SodiumCA			
C:\lsode\cadb-Sodium	CA	Chan	ge Cr	eate
Passphrase (Optional) :	•••••		_ SH	low
et the CA to work with	n the Directory			

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 🧊 New CA $\times$ Set Key type, Subject and Subject Alternative Names Use this page to set Key type, Subject and Subject Alternative Names for the CA Subject DN cn=Mark CA,o=Isode Algorithm for the Key ● RSA ○ DSA ○ ECDSA Key Size Key Size 3072 🗸 Add Subject Alternative Names for the CA Add... Edit... Remove < Back Next > Cancel

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				
🧔 New CA			_		$\times$
Set Basic Constrain	its and KeyUsagi	e Extension			
Use this page to set the CA	Basic Constraints and	KeyUsage extensior	ns for		
Key Usage Digital Signature Data Encipherment CRL Sign	Non Repudiation Key Agreement Encipher Only	Key Encipherm	ent		
Basic Constraints	yth		Path Length 1		<u>•</u>
	< Back	Next >	Finish	Cancel	

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

🐼 New CA			×
Generate Self Signed Certificate or CSR			
Use this page to either generate a Self Signed Root Certificate or CSR to be signed by another CA			
C Generate a Self Signed Root Certificate			
O Generate a CSR to be signed by another CA			
Signature Algorithm SHA256WITHRSA ~			
Valid From 13 February 2020, 11:41		Edi	t
Valid To 13 February 2030, 11:41		Edi	t
Lifetime			
Years: 10 🗘 Months: 0 🎝 Days: 0 🗘 Hours	: 0	•	
		Reset	
< Back Next > Finish		Cance	I

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

🧔 Sodium CA Profile Manager	$\times$
Configured CAs SodiumCA Modify Delete Encrypt	
Open Close	

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

Image 48: Enter CADB Passphrase		
💯 Enter CADB Passphrase		×
Enter the password for decrypting the Privat Passphrase:	e Key for this CA	
	ок	Cancel

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

Image 49: Sodium CA		
🧔 Sodium CA - SodiumCA (cn=Mark CA,o=Isode)	-	×
SodiumCa Operations Session View Help		
Sodium CA Logs Sodium CA 🕅		
Browse < Not Configured to work with the Directory >		
CA Components Certificates Certificate Requests		
RSA Key with PKCS#8 Format     Image: Credition of the second secon		
View Export PEM Export DER Update		
Abort		

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...".



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

Image 51: Gei	nerate TLS CSR #2				
Generate TLS Certificate Signing Request					
The certificate	signing request will be created for the M-Guard Applianc	e with:			
Host name:	eval.guard.net				
🗸 Use host n	ame as service name				
Service name:	eval.guard.net				
Advanced		Creat	te	Cancel	

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

#### Evaluation Guide: M-Guard

#### Image 52: Sodium CA: Certificate Requests

🥨 Sodium CA - SodiumCA (cn=Mark CA,o=Isode)	_		$\times$
SodiumCa Operations Session View Help			
Sodium CA 😫			
Browse < Not Configured to work with the Directory >			
CA Components Certificates Certificate Requests			
Directory to search for CSR			
C:\Users\Mark\Desktop\	Change	Refresh	
C:\Users\Mark\Desktop\	Change	Refresh	

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

Image 53: Certifica	ate Signing Re	equest				
😺 Issue Certifica	te for a CSR					×
Certificate Signi	ing Request					
The following is t Certificate will be	the Certificate e issued	Request for which	a			
						_
Subject	cn=eval.gua	rd.net				
PublicKeyInfo	Algorithm: R	SA, KeySize: 4096				
DNS Name	eval.guard.net	t				
Details						
The certificate rec	uest for "cn=	eval.guard.net" has	no subjectKeyl	dentifie	r	
	< Back	Next >	Finish		Cance	I

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		
🧔 Issue Certificate for a CSR		×
Set Validity and Signature Algorithm for the Certificat		
Set the validity and Signature Algorithm for the Certificate and choose to delete the CSR		
Valid From 10 February 2020, 11:09	Edi	t
Valid To 10 February 2022, 11:09	Edi	t
Lifetime		
Years: 2 A Months: 0 Days: 0 Hours: 0	÷ Reset	
Signature Algorithm SHA256WITHRSA		~
Delete the CSR after the Certificate generation		
< Back Next > Finish	Cance	I

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

mage 55: Generated	Certificate						
🧔 Issue Certificate for a	CSR	_		$\times$			
Generated Certificate							
The following certificate	will be generated.						
Subject	cn=eval.guard.net						
lssuer	cn=Mark CA,o=Isode						
Valid from	Wed Feb 19 11:36:17 GMT 2020						
Valid to	Sat Feb 19 11:36:17 GMT 2022						
Serial	44:AB:89:AA:8C:DA:52:7A:69:6A						
PublicKeyInfo	Algorithm: RSA, KeySize: 4096						
SignatureAlgorithm	SHA256WITHRSA						
CertificateType	Version v3 (Not a CA Certificate)						
Display Detailed Information Export to disk Write certificate chain in PEM format V							
< Ba	ick Next > Fini	ish	Cance	21			

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

Image 5	i6: CSR Signed	
🧔 CSF	R Signed X	<
1	A certificate has been issued for "cn=eval.guard.net". Certificate chain for "cn=eval.guard.net" has been written to C:\Users\Mark\Desktop\mguard_csr_Chain.pem. The CA certificate has been written to C:\Users\Mark\Desktop\ca_certificate.pem.	
	ОК	

#### 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

Specify Certificate (with	Chain) F	File					×
🗲 🔶 👻 🕇 🛄 🤅	This P	C > Desktop			✓ <sup>™</sup> S	earch Desktop	Ą
Organize 🔻 New	folder						. ?
1 Ouiskaanse	^	Name	Date modified	Туре	Size		
		🔼 ca_certificate	19/02/2020 11:39	PEM File	2 KB		
Desktop *		🖉 mguard_csr_Chain	19/02/2020 11:39	PEM File	4 KB		
Documents     Documents     M     Documents     M     Documents     M     M-Guard     Undates							
Virtual Box	~						
F	ile name	e: mguard_csr_Chain			~	Certificate File (PEM forma Open Can	t) ~

### 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

Specify Certificate File								×
← → • ↑ 🗖	> This PC	C → Desktop			~ Ō	Se	arch Desktop	Ą
Organize 🔻 Ne	w folder							
OneDrive	^ N	Name	Date modified	Туре	Size			
This PC	L	🔄 ca_certificate	19/02/2020 11:39	PEM File		2 KB		
3D Objects	l	Mguard_csr_Chain	19/02/2020 11:39	PEM File		4 KB		
Desktop								
Documents								
Downloads	~							
	File name	ca_certificate				~ C	ertificate File (PEM form	at) 🗸
							Open Ca	ncel

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).



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

Image	62: Select F	Rule Catalogs				
🔳 Rule	Catalogs for Pr	oject Eval Guide		—		×
Rule cata	ogs provides co	ntent verification rules for Guard	configuration.			
Select the	rule catalogs to	use from the list of builtin catalo	gs. You may also import rule catalogs.			
Active	Туре	Name	Synopsis	Description	Expo	ort
$\checkmark$	Built-in	Base Rules Catalog for XML	A catalog of general XML rules.	This catalog provides a set of generally applicable rules for checking XML content.	Remo	ove
	Built-in	Demo Protocol	General Rules for DemoP	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. This catalog is likely to be enabled in test and demo scenarios and disabled for deployments.	Vie	:w
					Impo	ort
				Save	Car	ncel

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

Create New	Guard Instance	×
Enter a name	for the new Guard instance	?
Guard Name:	Red-to-Black	
	ОК	Cancel

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.

M-Guard Console - Guard Red-to-Bla	ik	-		×
File Project Appliance Guard	Help			
🔻 🚞 Eval Guide V 😽 M-Guard-Eval	Status: This configuration has not yet been applied to the appliance Tag: Red2Black Finable service			
Red-to-Black (1)	Inbound Peer Outbound Peer UP address 10.178.0.1 Verify peer's identity Host name redside.guard.net UP address 192.168.106.1 Verify peer's identity Host name blackside.guard.net			
		1		
	Listen port 5269	12)		•
	Flow name Response Flow rules	Ĵ		
	Flow name Request Flow rules			
	Apply & Start		Cancel	

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

mage 66: Guard Running						
📧 M-Guard Console - Guard Red-to-Black - 🗆 🗙						
File Project Appliance Guard He	lp			_		
🔻 🚞 Eval Guide	Status: Running					
🕈 🌄 M-Guard-Eval	Tag: Red2Black 🖌 Table service					

#### **Configure Syslog Logging**

Image 65: Guard Configuration

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							
M-Guard Console - Guard Red-to-Black							
File Proj	ect	Appliance	Guard	Н	elp		
▼ 📄 Eval (	Guide	New Guard			Status: Running		
- <b>* 🎸</b> M	l-Gua	Setup		۲	Set Host Name		
Red-	to-Bl	Get Status			Configure Interfaces		
		Maintenance	2	۲	Log to Here		
		File Transfer			Authorize SSH Key		
		Log message	e		Restrict SSH		

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

Image 68: Logging Setup

Confirmation	$\times$
Configure appliance syslogd(8) to log to here?	?
ОК	Cancel

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...

M-Guard Console - Project Eval Guide						
File Project Appliance O	Suard Help					
New Project						
Open Project						
SSH 🕨						
GCXP Consumer / Producer 🔸	Create Certificate Signing Request					
Exit	Remove Pending Certificate Signing Request					
	Import Certificate Chain					

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

Create CSR for GCXP Producer / Consumer					
Create a certificate signing request for M-Guard Console suitable for use as both an inbound peer and an outbound peer of a Guard instance. The names of the services must be different.					
Host name:	eval.guard.net				
Inbound service name:	redside.guard.net				
Outbound service name:	blackside.guard.net				
Advanced		Crea	ate	ancel	

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

Select Folder for Certificate Signing Request						×
$\leftarrow \rightarrow$ $\vee$ $\uparrow$ $\square$ > This PC > Desktop >			✓ <sup>™</sup> Si	earch Desktop		,c
Organize 👻 New folder						?
VirtualBox ^ Name	Date modified	Туре	Size			
<ul> <li>OneDrive</li> </ul>						
💻 This PC						
3D Objects						
E Desktop						
🖹 Documents						
👆 Downloads 🛛 🗸						
Folder:						
			S	elect Folder	Cance	el

#### 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			
😨 Sodium CA - SodiumCA (cn=Mark CA,o=Isode)	_		×
SodiumCa Operations Session View Help			
Sodium CA 🕱			
Browse < Not Configured to work with the Directory >			
CA Components Certificates Certificate Requests			
Directory to search for CSR			
C:\Users\Mark\Desktop\	Change	Refresh	
CertificateRequest for cn=eval.guard.net (mgc_csr.pem created on Thu Feb 13 14:38:05 GMT 202	20)		
View     Export PEM     Export DER     Delete       Abort			

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					
🧊 Issue Certificate for a CSR —					
Set Validity and Signature Algorithm for the Certificat					
Set the validity and Signature Algorithm for the Certificate and choose to delete the CSR					
Valid From 19 February 2020, 14:08	Edit				
Valid To 19 February 2022, 14:08	Edit				
Lifetime					
Years: 2 🗘 Months: 0 🗘 Days: 0 🗘 Hours: 0	-				
	Reset				
Signature Algorithm SHA256WITHRSA	~				
Delete the CSR after the Certificate generation					
< Back Next > Finish	Cancel				

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 Co	ertificate						
👿 Issue Certificate for a CSR			_		×		
Generated Certificate							
The following certificate	The following certificate will be generated.						
Subject	cn=eval.guard.net						
lssuer	cn=Mark CA,o=Isode						
Valid from	Wed Feb 19 14:08:10 GMT	2020					
Valid to	Sat Feb 19 14:08:10 GMT 2	2022					
Serial	2A:62:71:62:5F:95:CF:A9:D	4:02					
PublicKeyInfo	Algorithm: RSA, KeySize: 3072						
SignatureAlgorithm	SHA256WITHRSA						
CertificateType	Version v3 (Not a CA Certificate)						
Display Detailed Inform	nation						
Export to disk Write certificate chain in PEM format 🗸							
		-	-				
< Back Next > Finish Cancel							

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

M-Guard Console - Project Eval Guide						
File Project Appliance Guard Help						
New Project						
Open Project						
SSH 🕨						
GCXP Consumer / Producer 🔸	Create Certificate Signing Request					
Exit	Remove Pending Certificate Signing Request					
	Import Certificate Chain					

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

Import Certificate Chain for GCXP Consumer / Producer X						$\times$	
	> This	PC > Desktop			✓ Ö Search Des	ktop	P
Organize 👻 Nev	v folder					8== 👻 🔲	8
OneDrive	^	Name	Date modified	Туре	Size		
		📇 ca_certificate	19/02/2020 14:13	PEM File	2 KB		
This PC		mgc_csr	19/02/2020 14:07	PEM File	2 KB		
3D Objects		Mgc_csr_Chain	19/02/2020 14:13	PEM File	4 KB		
Desktop							
Documents							
👆 Downloads							
Music							
Pictures							
Videos	$\sim$						
	File nar	me: mgc_csr_Chain			✓ PEM Files		~
					Open	Cancel	



Certifi	icate Successfully Imported	×
i	The certificate chain has been successfully imported. It will no be used when GCXP Consumer / Producer is run on a GCXP peer	w
	ОК	

"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

Enter SSH Passphrase	×
M-Guard Console is configured to use an SSH key in C:\MG provide a passphrase to decrypt the SSH key. Press Cancel the key, in which case certain features will not be enabled.	iC-Eval-Guide. You need to to continue without decrypting
	OK Cancel

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

#### Image 80: M-Guard GCXP Consumer - not configured

M-Guard GCXP Consumer	-		$\times$
File			
Status			
Not configured	Configure	Listen	
Log			

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].

Configure	M-Guard GCX	P Consu	_		×
Specify name o a guard) and po fields blank to o	f the peer com ort that GCXP o clear.	necting to G consumer is	CXP con to listen	sumer on. Lei	(typically ave both
Peer name	eval.guard.ne	et			
Listen port	5269				
		Clear	Can	cel	Save

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

M-Guard GCXP Consumer	_		×
File Certificate Help			
Status			
Ready to listen for peer eval.guard.net	Configure	Liste	n
Log			

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

M-Guard GCXP Consumer	- 🗆 ×
File Certificate Help	
Status	
Listening for connection from peer eval.guard.net	Configure Stop
Log	
Awaiting connection from 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

Enter SSH Passphrase X
M-Guard Console is configured to use an SSH key in C:\MGC-Eval-Guide. You need to provide a passphrase to decrypt the SSH key. Press Cancel to continue without decrypting the key, in which case certain features will not be enabled.
1
OK Cancel

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

Image 85: M-Guard GCXP Producer – not configured

File Status Not configured Configure Connect	
Status           Not configured         Configure         Connect	
Not configured Configure	
Log	

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

Configure N	A-Guard GCXP Producer $\Box$ X
Specify configur will connect to (	ation information for the peer the GCXP producer typically a guard). Leave all fields blank to clear.
Peer name	eval.guard.net
Peer address	10.178.0.2
Peer port	5269
	Clear Cancel Save

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

M-Guard GCXP Producer	_	
File Certificate Help		
Status		
Ready to connect to 10.178.0.2:5269 (eval.guard.net)	Configure	Connect
Log		

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

M-Guard GCXP Producer	_		×
File Certificate Help			
Status			
Connected to 10.178.0.2:5269 (eval.guard.net)	Configure	Disconn	ect
Log			
TLS Handshake (producer) completed. GCXP (producer) started.			< >

#### 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].

mage 89: Sending Invalid Content	
File Certificate Help	
Status	
Connected to 10.178.0.2:5269 (eval.guard.net)	Configure <b>Disconnect</b>
Log	
TLS Handshake (producer) completed. GCXP (producer) started.	^ ~
Content to Send	
<test> This is a test of broken XML </test>	
Send Clear	

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

M-Guard GCXP	Producer						—		×
File Certificate	Help								
Status									
Connected t	to 10.178.0.2:5269 (e	val.guard.net)				Configu	re	Disconne	ect
Log									
log Sending reque Got response	est (1d= -1, -5 (id=[-1, -50,	), -66, -44, - -66, -44, -13,	13, 39, 89, 39, 89, -17	-17]). ]): not accep	pted.				
log Sending reque Got response	est (1d= -1, -5 (id=[-1, -50,	), -66, -44, - -66, -44, -13,	13, 39, 89, 39, 89, -17	-17]). ]): not acce	pted.				
Log <u>Sending reque</u> Got response Content to Send	est (1d= -1, -5 (id=[-1, -50,	), -66, -44, - 66, -44, -13,	<del>13, 39, 89,</del> 39, 89, -17	-17[]. ]): not accep	pted.				
Log Sending reque Got response Content to Send <test></test>	est (1d= -1, -5 (id=[-1, -50,	), -66, -44, - 66, -44, -13,	13, 39, 89, 39, 89, -17	-17[]. ]): not accep	pted.				
og Sending reque Got response Content to Send <test> This is a tes </test>	est (1d= -1, -5 (id=[-1, -50, st of broken XM	), -66, -44, - 66, -44, -13,	13, 39, 89, 39, 89, -17	-1/ ). ]): not accep	pted.				
og Sending reque Got response Content to Send <test> This is a tes </test>	est (1d= -1, -5 (id=[-1, -50, st of broken XM	2, -66, -44, - 66, -44, -13,	13, 39, 89, 39, 89, -17	-17]). ]): not accep	pted.				
og Sending reque Got response Content to Send <test> This is a tes </test>	est (1d= -1, -5 (1d=[-1, -50, st of broken XM	), -66, -44, - -66, -44, -13,	13, 39, 89, 39, 89, -17	-17/)). ]): not acce;	pted.				,

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

Imag	e 91: Sys	log													
📰 Vis	ual Syslog Ser	ver 1.6.4											-		$\times$
Set		Processing	Highlighti	ng G	ioto new	More View	w prev V	iew next	View file	olear	About	Terminate			
Dispid	v View file	syslog				$\sim$									
Me	ssage filtering	Prio	rity = alert												
Display	ying 1 message	s of 3													
Time		IP	Host	Facility	Priority	Tag	Message								
Feb 1	3 14:58:52	192.168.56.2		daemon	alert	Red2Black[811]	redside.gu	iard.net Cor	ntent Alert - re	ject (Error)	: message id=	ffcebed4:f32759e	f type=Reques	t: could no	otp
UDP 192	2.168.56.1:514	1	TCP 192.16	8.56.1:514	01										

### Testing the Guard with valid XML

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

#### Image 92: Sending Valid Content

M-Guard GCXP Producer	-		$\times$
File Certificate Help			
Status			
Connected to 10.178.0.2:5269 (eval.guard.net)	Configure	Disconn	ect
Log			
Sending request (id=[-1, -50, -66, -44, -13, 39, 89, -17]). Got response (id=[-1, -50, -66, -44, -13, 39, 89, -17]): not accepted.			< >
Content to Send			
<test> This is a test of good XML </test>			
Send Clear			
			Exit

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

M-Guard GCXP Producer	-		×
File Certificate Help			
Status			
Connected to 10.178.0.2:5269 (eval.guard.net)	Configure	Disconne	ect
Log			
Sending request (1d= -5, 6, -93, -39, 78, 117, 66, 17 ). Got response (id=[-5, 6, -93, -39, 78, 117, 66, 17]): accepted.			~
Content to Send			
<test> This is a test of good XML </test>			
Send Clear			
			Exit

#### 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

M-Guard GCXP Consumer	_		$\times$
File Certificate Help			
Status			
Awaiting GCXP messages from peer eval.guard.net	Configure	Stop	
Log			
Accepted connection from peer. TLS Handshake (consumer) completed. GCXP (consumer) started. Accepting forwarded message (id=[-5, 6, -93, -39, 78, 117, 66, 17]) from peer.			<u> </u>
Received Content			
start of data <test> This is a test of good XML </test> end of data			
		Clear	
			Exit

### 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

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 2002-2020. 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 2020.