M-Guard Evaluation Guide

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

Contents

| Introduction |
|--|
| Objectives |
| Using Isode Support 4 |
| Preparing the Environment |
| Network Overview |
| Obtain the Isode Software and Java5 |
| Configure the Hyper-V Networks7 |
| Importing the M-Guard Appliance 12 |
| Configuring and Starting the M-Guard Appliance17 |
| Configuring and the Guard with M-Guard Console22 |
| Prepare to Add an M-Guard Instance |
| Configuring a new M-Guard Instance |
| Setup up the GCXP Producer and Consumer Certificates |
| Configure GCXP Producer and Consumer56 |
| Send messages between GCXP Producer and Consumer62 |
| What Next? |
| Whitepapers |
| Copyright |

Introduction

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

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

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

Objectives

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

The diagram below gives an overview of this setup.



System Overview

By the end of this guide, you will have:

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

Using Isode Support

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

Preparing the Environment

Network Overview

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

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

Obtain the Isode Software and Java

You will need to obtain the following from Isode Support.

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

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

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

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

Set JAVA_HOME

| Eclipse Temurin JDK with Hotspot 11.0.25+9 (x64) Setup — × Custom Setup | Eclipse Temurin JDK with Hotspot 11.0.25+9 (x64) Setup – Custom Setup Select the way you want features to be installed. |
|---|---|
| Click the icons in the tree below to change the way features will be installed. | Click the icons in the tree below to change the way features will be installed. |
| Location: C:\Program Files\Eclipse Browse Adoptum\jdk-11.0.25.9-hotspot\ | Browse |
| Reset Disk Usage Back Next Cancel | Reset Disk Usage Back Next Cancel |

Set JAVA_HOME 🔁 Eclipse Temurin JDK with Hotspot 11.0.25+9 (x64) Setup \times _ Custom Setup \square Select the way you want features to be installed. Click the icons in the tree below to change the way features will be installed. JDK with Hotspot Sets or overrides JAVA_HOME environment variable with the JDK installation directory. Modify PATH variable Associate .jar Set or override JAVA_HC 🗙 🛛 JavaSoft (Oracle) registr This feature requires 2KB on your hard drive. Browse ... Disk Usage Reset Back Next Cancel

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

Test JAVA_HOME



Configure the Hyper-V Networks

From the Hyper-V Manager.

| Hyper-V Manager | | - 🗆 X |
|---|-------------------|---|
| File Action View Help | | |
| Image: Second | | Actions M-GUARD-EVAL Quick Create New Import Virtual Machin Hyper-V Settings Virtual Switch Manage Virtual SAN Manager E dit Disk Import Disk |
| | Details | Stop Service Remove Server Refresh View Help |
| | No item selected. | |

Select "Virtual Switch Manager"

Virtual Switch Manager

| Virtual Switches | Consta victual avritati |
|---------------------------------|---|
| New virtual network switch | |
| 其 Default Switch | What type of virtual switch do you want to create? |
| Default Network | External |
| Global Network Settings | Internal Private |
| 00-15-5D-01-A3-00 to 00-15-5D-0 | |
| | Create Virtual Switch |
| | Creates a 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. |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

Select "Internal" and Click "Create Virtual Switch".

Virtual Switch Manager

| New virtual network switch Default Switch Default Network M-Guard Management Internal only | Name: M-Guard Management |
|--|---|
| C Default Switch Default Network C M-Guard Management Internal only | M-Guard Management |
| M-Guard Management Internal only | Notes |
| Internal only | Notes: |
| | Notest |
| lobal Network Settings | A |
| MAC Address Range 00-15-5D-01-A3-00 to 00-15-5D-0 | |
| | Connection type |
| | What do you want to connect this virtual switch to? |
| | External network: |
| | Microsoft Hyper-V Network Adapter #2 |
| | Allow management operating system to share this network adapter |
| | |
| | |
| | |
| | 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. |
| | |
| | Remove |

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

Host Network

| B | I Diagnose network pro | blems |
|---|---------------------------|---------------------|
| ģ | Network and Internet | settings |
| | ^ 🕥 🖫 🏷 🖢 | 17:43 08/01/2025 |

Select "Network and Internet settings".

Configure Network

| \leftarrow Settings | - c | - × |
|--|----------------------------------|-----|
| Mark Timberlake mark.timberlake@isode.com | ··· > Advanced network setting | IS |
| Find a setting Q | vEthernet (M-Guard | |
| A Home | Hyper-V Virtual Ethernet Adapter | ^ |
| System | Media state: | |
| Bluetooth & devices | Enabled | |
| 🔷 Network & internet | Bytes sent: 0 | |
| Personalisation | Bytes received: | |
| Apps | 0 Link speed: | |
| Accounts | 10 (Gbps) Duration: | |
| 🕤 Time & language | 00:04:59 | |
| 🥶 Gaming | Rename this adapter Rename | |
| 🕇 Accessibility | | |
| Privacy & security | View additional properties | > |
| Ø Windows Update | More adaptor options Edit | |

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

Configure Network

| vEthernet (M-Guard Management) Properties | × | | |
|--|---|--|--|
| Networking Sharing | | | |
| Connect using: | | | |
| Hyper-V Virtual Ethernet Adapter #2 | | | |
| Configure This connection uses the following items: | | | |
| | | | |
| Install Uninstall Properties | | | |
| Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks. | | | |
| OK Cancel | | | |

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

Configure Network

| Internet Protocol Version 4 (TCP/IPv4) Properties | | | |
|---|---------------------|--|--|
| General | | | |
| You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings. | | | |
| Obtain an IP address automatically | | | |
| Use the following IP address: | | | |
| IP address: | 10 . 178 . 0 . 1 | | |
| Subnet mask: | 255 . 255 . 255 . 0 | | |
| Default gateway: | | | |
| Obtain DNS server address automatically | | | |
| OUse the following DNS server add | resses: | | |
| Preferred DNS server: | | | |
| Alternative DNS server: | • • • | | |
| Validate settings upon exit | Advanced | | |
| | OK Cancel | | |

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

Repeat this process for the Red Network and Black Network.

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

Hyper-V Virtual Switch Manager

| Virtual Switch Manager for M-GUARD-EVA | al – – × |
|---|---|
| Xirtual Switches | Create virtual switch What type of virtual switch do you want to create? External Internal Private |
| Black Network Internal only Global Network Settings MAC Address Range 00-15-5D-01-A3-00 to 00-15-5D-0 | 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 |

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

```
Check Network Addresses
```



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

Importing the M-Guard Appliance

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

From Hyper-V Manager.

| Hyper-V Manager | | | | | | | | | |
|-----------------------|-----------------------------|---|--------------------------|--------------|--------------|---------|----------------|----------|---|
| Hyper-V Manager | | | | | | | - | | × |
| File Action View Help | | | | | | | | | |
| 🗢 🄿 🙋 🖬 🚺 🖬 | | | | | | | | | |
| Hyper-V Manager | Virtual Machines | | | | | Act | ions | | |
| M-GUARD-EVAL | Name | Name State CDILIIsage Assigned Memory Lintime | | M-GUARD-EVAL | | • | | | |
| | | | e esuge presign | ica incinoi, | opune | 2 | Quick Create | | |
| | | No virtual machines v | vere found on this serve | er. | | | New | | ► |
| | | | | | | 6 | Import Virtua | l Machin | |
| | | | | | | | Hyper-V Setti | ings | |
| | | | | | | 52 | Virtual Switch | n Manage | • |
| | | | | | | 4 | Virtual SAN N | /anager | |
| | Checkpoints | | | | | - | Edit Disk | | |
| | No vitual machine selected. | | | - | Inspect Disk | | | | |
| | | | | | Stop Service | | | | |
| | | | | × | Remove Serve | er | | | |
| | | | | | U | Refresh | | | |
| | | | | | | View | | • | |
| | | | | | | ? | Help | | |
| | | | | | | | | | |
| | Details | | | | | | | | |
| | | No iter | n selected. | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

Select Import Virtual Machine.

| Import Virtual Mach | hine | |
|-----------------------------------|--|----------|
| Import Virtual Machine | | \times |
| 💌 Before You | Begin | |
| Before You Begin Locate Folder | This wizard helps you import a virtual machine from a set of configuration files. It guides you through resolving configuration problems to prepare the virtual machine for use on this computer. | r |
| Select Virtual Machine | | |
| Choose Import Type | | |
| Summary | | |
| | | |
| | | |
| | | |
| | | |
| | < Previous Next > Finish Cancel | |
| | | |

Click "Next>"

| Import Virtual Machine | | | |
|------------------------|--|--------|---|
| Import Virtual Machine | | | × |
| Locate Folder | | | |
| Before You Begin | Specify the folder containing the virtual machine to import. | | |
| Locate Folder | Folder: 1.5\Appliance\M-Guard-1.5.4-hyper-full\M-Guard Appliance\Virtual Machines\ | Browse | |
| Select Virtual Machine | | | |
| Choose Import Type | | | |
| Summary | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | < Previous Next > Finish | Cancel | |

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

Click "Next>"

Import Virtual Machine

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 | 02/09/2024 13:04:45 | | | | | |
| Choose Import Type | | | | | | | |
| Summary | | | | | | | |
| | < Previous | Next > Finish Cancel | | | | | |

Select "M-Guard Appliance".

Click "Next>"

 \times

| Import Virtual Machine | | |
|------------------------|--|---|
| Import Virtual Machine | | × |
| Choose Impo | ort Type | |
| Before You Begin | Choose the type of import to perform: | |
| Locate Folder | Register the virtual machine in-place (use the existing unique ID) | |
| Select Virtual Machine | | |
| Choose Import Type | Copy the virtual machine (create a new unique ID) | |
| Summary | | |
| | | |
| | < Previous Next > Finish Cancel |) |

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

Click "Next>"

Import Virtual Machine

| Import Virtual Machine | | × |
|---|---|-------------------|
| A Choose Fo | lders for Virtual Machine Files | |
| Before You Begin Locate Folder Select Virtual Machine Choose Import Type | You can specify new or existing folders to store the virtual machine files. Otherwise, the v imports the files to default Hyper-V folders on this computer, or to folders specified in the machine configuration. Store the virtual machine in a different location Virtual machine configuration folder: | vizard virtual |
| Choose Destination Choose Storage Folders Summary | C: \ProgramData \Microsoft \Windows \Hyper-V\ Checkpoint store: C: \ProgramData \Microsoft \Windows \Hyper-V\ Smart Paging folder: C: \ProgramData \Microsoft \Windows \Hyper-V\ | Browse Browse |
| | < Previous Next > Finish | Cancel |

Click "Next>"

Import Virtual Machine

Import Virtual Machine

| 1 |
|-----|
| × |
| / ~ |

 \times

Choose Folders to Store Virtual Hard Disks

| Before You Begin | Where do you want to store the imported virtual hard disks for this virtual machine? | |
|------------------------|--|--------|
| Locate Folder | Location: C:\ProgramData\Microsoft\Windows\Virtual Hard Disks\ | Browse |
| Select Virtual Machine | | |
| Choose Import Type | | |
| Choose Destination | | |
| Choose Storage Folders | | |
| Summary | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | < Previous Next > Finish | Cancel |
| | | |

Click "Next>"

Import Virtual Machine

Import Virtual Machine

Completing Import Wizard

| Before You Begin | You are about to perform the following | operation. |
|--|--|---|
| Locate Folder Select Virtual Machine Choose Import Type Choose Destination Choose Storage Folders Summary | Description: Virtual Machine: Import file: Import Type: Virtual machine configuration folder: Checkpoint folder: Smart Paging file store: Virtual hard disk destination folder: | M-Guard Appliance C: \[Sode Software \[M-Guard 1.5\]Appliance \[M-Guard-1.5.4-hype Copy (generate new ID) C: \[ProgramData \[Microsoft \[Windows \[Hyper-V\] C: \[ProgramData \[Microsoft \[Windows \[Hyper-V\] C: \[ProgramData \[Microsoft \[Windows \[Hyper-V\] C: \[ProgramData \[Microsoft \[Windows \[Virtual Hard Disks \] |
| | To complete the import and close this v | vizard, dick Finish. |
| | (| < Previous Next > Finish Cancel |

Click "Finish"

| Import Virtual Machine | | | | | | | |
|------------------------|-------------------|-------------------------------|---------------------|-----------------|--------|--------------------------------|--------|
| Hyper-V Manager | | | | | | — C | |
| File Action View Help | | | | | | | |
| 🔶 🄿 🙎 📰 🚺 🖬 | | | | | | | |
| Hyper-V Manager | Virtual Machiner | | | | | Actions | |
| M-GUARD-EVAL | Name | Ctata | CDUUrage | Assigned Memory | Untime | M-GUARD-EVAL | • |
| | M-Guard Appliance | Off | CF0 0sage | Assigned Memory | optime | Quick Create | |
| | | | | | | New | + |
| | | | | | | 🔒 Import Virtual M | lachin |
| | | | | | | Hyper-V Setting | 5 |
| | | | | | | 📲 Virtual Switch M | lanage |
| | | | | | | 🔜 🔬 Virtual SAN Mar | nager |
| | Checkpoints | | | | (| 🔺 🛃 Edit Disk | |
| | | No vi | tual machine select | ed | | Inspect Disk | |
| | | ivo virtual machine selected. | | | | | |
| | | | | | | × Remove Server | |
| | | | | | | 🖸 Refresh | |
| | | | | | | View | • |
| | | | | | | <table-cell> Help</table-cell> | |
| | | | | | | = | |
| | Details | | | | | | |
| | | | No item selected. | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | _ | |
| |] | | | | | | |

You have now successfully imported the M-Guard Appliance.

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

Configuring and Starting the M-Guard Appliance

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



Select the M-Guard Appliance and Click Settings.

Configure Network Interfaces on M-Guard



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

You should have something like the following.

Configure Network Interfaces on M-Guard



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



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

| M-Guard 1 st Start | |
|--|---|
| 🕎 M-Guard Appliance on M-GUARD-EVAL - Virtual Machine Connection | - |
| File Action Media Clipboard View Help | |
| ⊞ 🖲 💿 💿 🔢 🕨 🔂 ⊅ 🖳 👪 | |
| | |
| | |
| | |
| | |
| ++ | |
| | |
| + | |
| | |
| | |
| | |
| | |
| | |
| + | |
| + | |
| | |
| +. | |
| ++ | |
| *************************************** | |
| | |
| | |
| | |
| | |
| | |
| | |
| OK Cancel Apply | |

When this has finished you will see the screen below.

| M-Guard Boot complete |
|--|
| Thu Jan 9 11:38:00 UTC 2025 2025-01-09T11:38:00.838211+00:00 - init[1] kernel security level changed from 0 to 1 |
| <pre>SSH host fingerprints: SHA256:Shj9a4SCLvvCyVp01EL0Ue483ylZfjkvY6th1ns9ZU8 (ECDSA) MD5:2c:b4:1d:c2:8c:31:2c:f6:dc:53:fa:52:96:3a:99:ec (ECDSA) SHA256:uY0JVS5asCcJ/TDHIq/6k1v0+p+1rBS9oRc5ydkNFRE (ED25519) MD5:33:a1:00:fe:61:b9:d4:14:59:f5:8b:ba:30:00:62:19 (ED25519) SHA256:ukzHtVtHIXKG+fSVNJ4EHqnTHt7d673euWXBnwxXKJ8 (RSA) MD5:1b:80:98:e5:60:c2:5f:e6:6f:27:63:c6:99:ed:c6:87 (RSA) IPv4 link-local address: 169.254.60.116/16 (hn0) IPv6 link-local address: fe80::215:5dff:fe01:a303%hn0/64 Admin (root) password set to: nTPlf23bJAEum</pre> |
| M-Guard Appliance/m-guard (Amnesiac) (ttyv0) |
| login: |

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

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

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

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

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

Configuring and the Guard with M-Guard Console

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

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

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

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



You will then be presented with this screen.



| H-Guard Co File Project S | onsole | - | \times | |
|-----------------------------------|--------------|-----------------------------|----------|--|
| | File Project | Appliance Guard Help | | |
| | | Status: Message | | |
| | | Alert | | |

Select File--> New Project

M-Guard Console Project configuration

| ■ M- | Guard Co | nso | le | | |
|------|----------|-----|------------|----|------|
| File | Project | | | | Help |
| New | Project | | ıs: Messag | je | |
| Open | Project | | | | |
| SSH | | ۲ | | | |
| Exit | | | | | |

M-Guard Console Project configuration

| Select New Folder for M-Guar | d Console Project | | | × |
|---|--|-----------------------|---------------------|--------|
| \leftrightarrow \rightarrow \checkmark \uparrow | « Local Disk (C:) > M-Guard > M-Guard Eval | ~ C | Search M-Guard Eval | Q |
| Organise 👻 New folder | | | | ≣ • 😗 |
| 🔛 Documents 🖈 | Name | Date modified | Туре | Size |
| 🔀 Pictures 🛛 🖈 | No iter | ns match your search. | | |
| 🕖 Music 🔹 🖈 | | | | |
| 🛂 Videos 🔹 🖈 | | | | |
| System32 | | | | |
| > 💻 This PC | | | | |
| > 📫 DVD Drive (D:) C | | | | |
| > 💁 Network | | | | |
| Folder: | M-Guard Eval | | | |
| | | | Select Folder | Cancel |

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

| Verify Name M-Guard Eval Folder C:\M-Guard\M-Guard Eval You can now add appliance configurations to this project Add Appliance | Project Configuration: <unname< p=""></unname<> | d> (mg | jc-project.xml) – 🗆 X |
|--|---|--------|---|
| Folder C:\M-Guard\M-Guard Eval You can now add appliance configurations to this project Add Appliance | 🔻 🚞 M-Guard Eval | Name | M-Guard Eval |
| You can now add appliance configurations to this project Add Appliance | | Folder | C:\M-Guard\M-Guard Eval |
| | | | You can now add appliance configurations to this project Add Appliance |

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

M-Guard Console Project configuration

| M-Guard Console - Project M-Guard Eval | | | | | | |
|--|----------------------|--|--|--|--|--|
| File Project | Appliance Guard Help | | | | | |
| New Project | | | | | | |
| Open Project | | | | | | |
| SSH | Select SSH Keys | | | | | |
| Exit | Generate SSH Keys | | | | | |
| | | | | | | |

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

M-Guard Console Project configuration

| M-Guard Console Proje | ct configuration | | | | | |
|--|--|------------|-----------|--------|--------|----------|
| 📧 Generate SSH Keys | | _ | | × | | |
| This will generate a new S specified folder | SH key pair for use by M-Guard Console and | d save the | em in the | | | |
| Directory | | | Sel | ect | | |
| Key Length 40 | 096 👻 | Key | Type rs | a 🔻 | | |
| Comment | | | | | | |
| Passphrase | | | | | | |
| Confirm Passphrase | | | | | | |
| | Gen | erate | Canc | el | | |
| M-Guard Console Proje | ect configuration | | | | | |
| 🔳 Generate SSH K | eys | | | | | \times |
| This will generate a n specified folder | ew SSH key pair for use by M-Guard | l Conso | le and s | ave th | nem in | the |
| Directory | C:\M-Guard\M-Guard Eval | | | | | Select |
| Key Length | 4096 - | | | Key | Туре | rsa 🔻 |
| Comment | isode.support@isode.com | | | | | |
| Passphrase | ••••• | | | | | |
| Confirm Passphrase | ••••• | | | | | |
| | | | Genera | ate | Ca | ancel |

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

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

Click "Generate".

M-Guard Console Project configuration

| ■ M- | M-Guard Console - Project M-Guard Eval | | | | | | | | |
|----------------------|--|-----------------------------|--|--|--|--|--|--|--|
| File | Project | Appliance Guard Help | | | | | | | |
| | M-Guard E | val | | | | | | | |
| Configure | | | | | | | | | |
| Application Profiles | | | | | | | | | |
| | Rule Catalogs | | | | | | | | |
| | | Content Catalogs | | | | | | | |
| | | Certificate Authority | | | | | | | |

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

| A-Guard Console Project configuration | | | | | | | | |
|---------------------------------------|--|--|--|--|--|--|--|--|
| M-Guard Cor | M-Guard Console - Project M-Guard Eval | | | | | | | |
| File Project | Appliance Guard Help | | | | | | | |
| 🚞 M-Guard E | 🚘 M-Guard Eval | | | | | | | |
| | Configure | | | | | | | |
| | Application Profiles | | | | | | | |
| | Rule Catalogs | | | | | | | |
| | Content Catalogs | | | | | | | |
| | Certificate Authority | | | | | | | |
| | | | | | | | | |

M-Guard Console Project configuration

| Project Configuration: M-Guard | Eval (m | gc-project.xml) — 🗆 🗙 |
|--------------------------------|---------|---|
| 🔻 🚞 M-Guard Eval | Name | M-Guard Eval |
| | Folder | C:\M-Guard\M-Guard Eval |
| | | You can now add appliance configurations to this project Add Appliance |

Click "Add Appliance".

M-Guard Console Project configuration

| Project Configuration: M-Guard | Eval (mg | jc-project.xml) | | | × |
|--------------------------------|----------|---|-----------|------|--------|
| 🔻 🚞 M-Guard Eval | Name | | | | |
| 🙀 No name set | User | root | | | |
| | Address | | | | |
| | Folder | | | | |
| | _ | Automatically connect | | | |
| | Status | Unable to create session | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | Delete appliance | | | |
| | | Delete appliance | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | Save Project Co | nfigurati | on (| Cancel |
| | | | | on | cancel |

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

| Project Configuration: M-0 | Guard Eval (mg | gc-project.xml) — C | ı × |
|----------------------------|----------------|----------------------------|-------|
| 🔻 🚞 M-Guard Eval | Name | M-Guard Eval | |
| 🌈 No name set | User | root | |
| - | Address | fe80::215:5dff:fe01:a303 | |
| | Folder | | |
| | | Automatically connect | |
| | | Delete appliance | |
| | | Save Project Configuration | Cance |

Click "Save Project Configuration".

Right Click on the Appliance and Click Connect.

| M-Guard Console - Appliance M-Guard Eval | - | \times |
|--|---|----------|
| File Project Appliance Guard Help | | |
| M-Guard Eval Status: status available (unsaved configuration changes may be present) File Transfer Connect | | |

You will the following dialogue box.

| M-Guard Console Project configuration | |
|--|----------|
| Confirmation | \times |
| Confirmation | ? |
| The authenticity of host 'fe80::215:5dff:fe01:a303' can't b established. RSA key fingerprint is 1b:80:98:e5:60:c2:5f:e6:6f:27:63:c6:99:ed:c6:87. Are you sure you want to continue connecting? | e |
| ОК Са | ncel |

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

M-Guard Console Project configuration

| SSH Authentication | × |
|--|---|
| Provide the input as prompted below to connect to root@fe80::215:5dff:fe01:a303. | |
| Password for root: | |

Enter the root password noted earlier. Click "OK".

| M-Guard Conso | le Project configuration | | |
|---------------------|--|-----|---|
| M-Guard Console - A | ppliance M-Guard Eval | - | × |
| File Project Applia | nce Guard Help | | |
| ▼ 🚞 M-Guard Eval | Status: 12:26PM up 50 mins, 0 users, load averages: 0.40, 0.29, 0.22 (unsaved configuration changes may be prese | nt) | |
| M-Guard Eval | | | |
| _ | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

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

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





| Confirmation | × |
|---|---------|
| Confirmation | ? |
| Are you sure you want to save the appliance configu | ration? |
| ОК | Cancel |

Click OK

M-Guard Console Save configuration

| 🔳 Save | configuration changes for M-Guard Eval | 1 | Х |
|--------------|--|---|-------|
| A | The appliance returned the following: | | |
| \mathbf{U} | File /etc/hostid added to /cfg. | | â |
| | File /etc/machine-id added to /cfg. | | |
| | File /etc/master.passwd added to /cfg. | | |
| | File /etc/opiekeys added to /cfg. | | |
| | File /etc/pwd.db added to /cfg. | | |
| | /cfg/rc.conf.d | | |
| | /cfg/rc.conf.d/sshd | | |
| | File /etc/rc.conf.d/sshd/manage added to /cfg. | | |
| | File /etc/spwd.db added to /cfg. | | |
| | /cfg/ssh | | |
| | File /etc/ssh/ssh_host_ecdsa_key.pub added to /cfg. | | |
| | File /etc/ssh/ssh_host_rsa_key added to /cfg. | | |
| | File /etc/ssh/ssh_host_ed25519_key.pub added to /cfg. | | |
| | File /etc/ssh/ssh_host_ecdsa_key added to /cfg. | | |
| | File /etc/ssh/ssh_host_ed25519_key added to /cfg. | | |
| | File /etc/ssh/ssh_host_rsa_key.pub added to /cfg. | | |
| | /cfg/tls | | |
| | File /etc/tls/dhparam.pem added to /cfg. | | |
| | /etc/hostid -> /cfg/hostid | | U |
| | /etc/machine-id -> /cfg/machine-id | | |
| | /etc/master.passwd -> /cfg/master.passwd | | |
| | /etc/pwd.db -> /cfg/pwd.db | | |
| | /etc/rc.conf.d/sshd/manage -> /cfg/rc.conf.d/sshd/manage | | |
| | /etc/spwd.db -> /cfg/spwd.db | | |
| | /etc/ssh/ssh_host_ecdsa_key.pub -> /cfg/ssh/ssh_host_ecdsa_key.pub | | ~ |
| | | | Close |

Click Close.

Right Click on the Appliance Maintenance-->Set Password

M-Guard Console Appliance configuration

| M-Guard Eval Status | 12:31PM up 55 mins, 0 user | s, load averages: 0.40, 0.28, 0 | .23 | | |
|---------------------|----------------------------|---------------------------------|-----|--|--|
| M-Guard Eval | | | | | |
| New Guard | | | | | |
| Setup | • | | | | |
| Get Status | | | | | |
| Maintenance | Backup | | | | |
| File Transfer | Restore | | | | |
| Log message | Reboot | | | | |
| Execute Command | Shutdown | | | | |
| Save Configuration | Update System | | | | |
| Disconnect | Check System Integrity | | | | |
| | Set Password | | | | |
| | | | | | |

The following Dialogue will appear.

M-Guard Console Appliance configuration

| Set Appliance Password | — | | × |
|------------------------|---|-----|------|
| Enter the new password | | | |
| ••••• | | | |
| ••••• | | | |
| 0 | K | Car | icel |

Enter your New Password and Click "OK".

| M-Guard Console Appliance configuration | |
|--|-------------------|
| Confirmation | × |
| Are you sure you want to set the appliance password? | ? |
| The current settings including the new password will immediately b | e saved. ancel |

Click "OK".

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

| M-Guard C | Console Appliance d | configuration | | | |
|-------------|---------------------------------------|--|--------------------------|---|----------|
| I M-Guard | Console - Appliance M-Gu | ard Eval | | - | \times |
| File Projec | t Appliance Guard | Help | | | |
| 🔻 🚞 M-Guai | rd Eval Status: 12:34 | 4PM up 58 mins, 0 users, load av | erages: 0.20, 0.25, 0.23 | | |
| 🌄 М-С | Guard Eval /etc/master /otc/courd. | r.passwd -> /cfg/master.passwd 4b -> /cfg/spwd.db | | | |
| | Setup 🔸 | Set Hostname | | | |
| | Get Status | Configure Firewall | | | |
| | Maintenance 🕨 | Configure Interfaces | | | |
| | File Transfer | Configure Clock Sync | | | |
| | Log message | Remote Logging | | | |
| | Execute Command | Appliance Logging | | | |
| | Save Configuration | Log Cleanup Configuration | | | |
| | Disconnect | Authorize SSH Key | | | |
| | | Restrict SSH | | | |
| | | Generate TLS CSR | | | |
| | | Load TLS Certificate | | | |
| | 10 | View TLS Certificate | Task result: 0 | | |
| | | Load TLS Trust Anchor | | | |
| | | View TLS Trust Anchors | | | |
| | | Verify Trust | | | |

M-Guard Console Appliance configuration

| 💽 Interface Co | nfiguration | | | | × |
|--------------------|-------------------------------|----|-------------|--------|-----|
| Interface hn0 | - | | | | |
| IP Address * II | P Aliases Settings | | | | |
| hn0 is currently e | nabled | | | | |
| IPv4 | | | | | |
| Address | 10.178.0.2 | | Prefix Leng | gth 24 | |
| IPv6 | | | | | |
| Address | | | Prefix Leng | gth 64 | |
| * Configuration | on this tab has been modified | | | | |
| | | OK | Revert | Can | cel |
| | | OK | Revent | Can | cer |

Start with "hno", the Management Interface and set the IPv4 Address to 10.178.0.2.

Then Settings Tab

| M-Guard Console Appliance configuration | | | | |
|--|----|--------|----|----------|
| Interface Configuration | | | | \times |
| Interface hn0 - | | | | |
| IP Address * IP Aliases Settings * | | | | |
| Name hn0 | | | | |
| Allow management services Allow GCXP Allow time services | | | | |
| * Configuration on this tab has been modified | ОК | Revert | Ca | ncel |
| | | | | |

Check "Allow management services" . Click "OK".

M-Guard Console Appliance configuration

| I M-Guard Console - Ap | I M-Guard Console - Appliance M-Guard Eval | | | |
|------------------------|--|--|--|---|
| File Project Applian | ce Guard Help | | | |
| ▼ 📄 M-Guard Eval | Status: 12:41PM up 1:04, 0 users, load averages: 0.16, 0.29, 0.25 (unsaved configuration changes present) 00000 allow ucp from me to any 123 out via hn0 keep-state default 00000 count ip from any to any 123 out via hn0 keep-state default 60000 count ip from any to any 135-139,445 in 60200 deny { tcp or udp } from any to any 1026,1027 in 60300 deny { tcp or udp } from any to any 1433,1434 in 60400 deny ip from any to 255.255.255.255 60500 deny up from any to 224.0.0.0/24 in 60600 deny up from any to 20 in 65000 deny up from any to any 520 in 65000 deny up from any to any 520 in 65000 deny log logamount 500 ip from any to any Firewall rules loaded. Firewall rules loaded. Firewall rules loaded. Stopping rsylogd. Waiting for PIDS: 1077. Starting rsylogd. Performing sanity check on sshd configuration. Stopping sshd. Waiting for PIDS: 1160, 1160. Performing sanity check on sshd configuration. Starting sshd. | | | > |
| | Tack search 0 | | | |

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

M-Guard Console Appliance configuration

| M-Guard Console - Appliance M-Guard Eval | - | | \times | | | | | | |
|---|---|--|----------|--|--|--|--|--|--|
| File Project Appliance Guard Help | | | | | | | | | |
| The Project Appliance Out of Project App | 1:06, 0 users, load averages: 0.18, 0.27, 0.24 (unsaved configuration changes present) rime to any 214,001,0014 secup via mito keep-state operation in me to any 123 out via hn0 keep-state idefault any to any idp) from any to any 135-139,445 in idp) from any to any 1026,1027 in idp) from any to any 1433,1434 in any to 255.255.255.255 any to 224.0.0.0/24 in n any to any 520 in mount 500 ip from any to any oled. 77. eck on sshd configuration. 50, 1160. eck on sshd configuration. | | | | | | | | |
| Task result: 0 | | | | | | | | | |

Select "Disconnect".

Select Project --> Configure

M-Guard Console Appliance configuration



M-Guard Console Appliance configuration

| Project Configuration: M-Guard | d Eval (mg | c-project.xml) | | | \times |
|--------------------------------|------------|-----------------------------------|---------------------|---------|----------|
| 🔻 🚞 M-Guard Eval | Name | M-Guard Eval | | | |
| M-Guard Eval | User | root | | | |
| | Address | fe80::215:5dff:fe0 |)1:a303 | | |
| | Folder | | | | |
| | _ | Automatically | connect | | |
| | Status | Unable to create se | ession | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | Delete appliance | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | Save Project Config | uration | Cancel |
| | | | | | |

Select M-Guard Eval

Change the IPv6 Address to your just configured IPv4 Address

M-Guard Console Appliance configuration

| Project Configuration: M-Guard | l Eval (mg | c-project.xml) - | | × |
|--------------------------------|------------|---|-------|--------|
| 🔻 🚞 M-Guard Eval | Name | M-Guard Eval | | |
| M-Guard Eval | User | root | | |
| _ | Address | 10.178.0.2 | | |
| | Folder | | | |
| | | Automatically connect | | |
| | Status | Unable to create session | | |
| | | | | |
| | | | | |
| | | | | |
| | | Delete appliance | | |
| | | Delete appliance | | |
| | | | | |
| | | | | |
| | | | | |
| | | Cours Device the Cours | | Consul |
| | | Save Project Configur | ation | Cancel |

Click "Save Project Configuration"

Right Click on the Appliance and Click "Connect.

M-Guard Console Appliance configuration



Verify SSH Key, Click OK.

Enter New Password you set.

Run the "Save Configuration" process.

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

Right Click Setup-->Set hostname

| M-Guard Console - Appliance M-Guard Eval | | | | | | |
|--|--------------------|-----------------------------------|--|--|--|--|
| File Project Ap | pliance Guard Help | | | | | |
| ▼ 🚞 M-Guard Eval | Status: 12:50PM u | p 1:14, 0 users, load averages: (| | | | |
| M-Guard f | val | 1 | | | | |
| | New Guard | | | | | |
| | Setup 🕨 | Set Hostname | | | | |
| | Get Status | Configure Firewall | | | | |
| | Maintenance 🕨 | Configure Interfaces | | | | |
| | File Transfer | Configure Clock Sync | | | | |
| | Log message | Remote Logging | | | | |
| | Execute Command | Appliance Logging | | | | |
| | Save Configuration | Log Cleanup Configuration | | | | |
| | Disconnect | Authorize SSH Key | | | | |
| | | Restrict SSH | | | | |
| | | Generate TLS CSR | | | | |
| | | Load TLS Certificate | | | | |
| | | View TLS Certificate | | | | |
| | | Load TLS Trust Anchor | | | | |
| | · | View TLS Trust Anchors | | | | |
| 2 items 1 | item selected | Verify Trust | | | | |

M-Guard Console Appliance configuration

| M-Guard | Console | Appliance | configuration |
|---------|---------|-----------|---------------|
| | | | |

| 🔳 Set Ho | stname | — | |
|----------|---------------|----|--------|
| Hostname | xml.guard.net | | |
| | | ОК | Cancel |

Enter Hostname (Your Choice), Click OK.

Next, we need to Authorize the SSH Key.

| M-Guard Console - Appliance M-Guard Eval | | | | |
|--|---------------------------|-----|---------------------------------|--|
| File Pr | oject Appliance G | | rd Help | |
| 🔻 🚞 M-0 | Guard Eval Status | : 1 | 2:54PM up 1:17, 0 users, load a | |
| | M-Guard Eval Setti | ng | hostname: xml.guard.net. | |
| | New Guard | | | |
| | Setup | ۲ | Set Hostname | |
| | Get Status Maintenance | | Configure Firewall | |
| | | | Configure Interfaces | |
| | File Transfer | | Configure Clock Sync | |
| | Log message | | Remote Logging | |
| | Execute Command | | Appliance Logging | |
| | Save Configuration | | Log Cleanup Configuration | |
| | Disconnect | | Authorize SSH Key | |
| | | | Restrict SSH | |
| | | | Generate TLS CSR | |
| | | | Load TLS Certificate | |
| | | | View TLS Certificate | |
| | | p) | Load TLS Trust Anchor | |
| | | | View TLS Trust Anchors | |
| 2 | items 1 item selecte | d | Verify Trust | |

M-Guard Console Appliance configuration

Right Click Setup-->Authorize SSH Key.



Click OK

Next, we need to Configure the other Interfaces.

M-Guard Console Appliance configuration

| Interface Configuration | | | | × |
|---|----|-------------|--------|-----|
| Interface hn1 - | | | | |
| IP Address * IP Aliases Settings | | | | |
| hn1 is currently not enabled | | | | |
| IP _V 4 | | | | |
| Address 192.168.56.2 | | Prefix Leng | gth 24 | |
| IPv6 | | | | |
| Address | | Prefix Leng | gth 64 | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| * Configuration on this tab has been modified | | | | |
| | ОК | Revert | Can | cel |

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

 \times

Then Click the "Settings" Tab.

M-Guard Console Appliance configuration Interface Configuration Interface hn1 IP Address * IP Aliases Settings * Name hn1 Allow management services Allow GCXP Allow time services

| * Configuration on this tab has been modified | | | |
|---|----|--------|--------|
| | ОК | Revert | Cancel |

Check "Allow GCXP".

Click OK.

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

Run the Save Configuration Process.

You are now ready to Add a "Guard Instance".

Prepare to Add an M-Guard Instance

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

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

Select Project \rightarrow Rule Catalogs.

M-Guard Console Rule Catalogs



The following is displayed.

| M-Gua | rd Console | e Rule Catalogs | | | | |
|------------|--|---|--|---|--------|--|
| 💽 Rule | Rule Catalogs for Project M-Guard Eval – | | | | | |
| Rule cata | logs provides co | ontent verification rules for Guard co | onfiguration. | | | |
| Select the | e rule catalogs t | o use from the list of built-in catalog | gs. You may also import rule catalogs. | | | |
| Active | Туре | Name | Synopsis | Description | Export | |
| | Built-in | Rule Catalog for arbitrary XML | A catalog of general XML rules | This catalog provides a set of generally applicable rules for checking arbitrary XML content. | Remove | |
| | Built-in | Demo Protocol | 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. | View | |
| | | | | | | |
| | | | | | Incert | |
| | | | | | import | |
| | | | | Save | Cancel | |

Check the two Checkboxes and Click "Save".

M-Guard Console Rule Catalogs

| 📧 Rule | Rule Catalogs for Project M-Guard Eval | | | | | | |
|--------------|---|--------------------------------|--------------------------------|---|------|------|--|
| Rule catal | Rule catalogs provides content verification rules for Guard configuration. | | | | | | |
| Select the | elect the rule catalogs to use from the list of built-in catalogs. You may also import rule catalogs. | | | | | | |
| Active | Туре | Name | Synopsis | Description | Expo | ort | |
| \checkmark | Built-in | Rule Catalog for arbitrary XML | A catalog of general XML rules | This catalog provides a set of generally applicable rules for checking arbitrary XML content. | Remo | ove | |
| | Built-in | Demo Protocol | 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 | ew. | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | Impo | ort | |
| | | | | Save | Car | ncel | |

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

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

Select Project→Application Profiles...



M-Guard Application Profiles

The following is displayed.

| M-Guard Application Profile. | s | | | | |
|--|---|--|---------------|--------|----------|
| GCXP Application Profiles for Proj | ect M-Guard Eval | | | | \times |
| GCXP application profiles can be used instance should behave in the context The list of currently imported application | to assist with the configu of a given application. on profiles is detailed belo | ration of a Guard instance. They contain informa | tion on how a | a Guar | d |
| Name | Version | Description | | Im | port |
| | | | | Rer | move |
| | | | | 1 | View |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | No profiles | imported | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | Save Change | es | Cancel |

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

Configuring a new M-Guard Instance

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

From the Guard Appliance Select "New Guard...".



The following is displayed

M-Guard Create New Guard Instance

| 💽 New Gu | ard Instance | | | | | × |
|-------------------------|-------------------------------------|--|---|--------------------|---------|---------|
| Before creat | ng a new guard | instance, the follow | ving information is | required: | | |
| Names | | | | | | |
| A name to | identify the jail | that will contain th | e new guard. | | | |
| Jail Name | | | | | | |
| GCXP Appl | ication Profile | | | | | |
| GCXP appl Select the | ication profiles appropriate pro | specify how applica file or None to con | tion data is to be e figure GCXP manua | κchanged ι Ily. | using (| GCXP. |
| GCXP App | lication Profile | | | | | - |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | OK | Cancel |
| | | | | | On | Caricer |

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

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

Check the "Allow GCXP responses in flow" Checkbox.

M-Guard Create New Guard Instance

| New Guard Instance | | | | × |
|---|---|------------------|----------|--------|
| Before creating a new guard | instance, the following information is | required: | | |
| Names | ······· | | | |
| | 44-4 | | | |
| A name to identify the jai | that will contain the new guard. | | | |
| Jail Name DemoP | | | | |
| GCXP Application Profile | | | | |
| | | | | |
| GCXP application profiles Select the appropriate pro | specify how application data is to be ex ofile or None to configure GCXP manua | kchanged Ily. | using GC | .хр. |
| GCXP Application Profile | Demo Protocol (0.1) | | | * |
| Profile Demo Protocol has | the following configurable options: | | | |
| Allow GCXP response | s in response flow | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | OK | Cancel |

Click "OK"

The following is displayed

M-Guard Create New Guard Instance

| M-Guard Console - Guard DemoP | | | | | | - | o | × |
|---------------------------------|------------------|----------------------------------|--------------|-------------------------------|---------------------|--------------------------|---------------|-----|
| File Project Appliance Guard He | elp | | | | | | | |
| 🔻 🚞 M-Guard Eval | Status: This cor | figuration has not yet been ap | plied to th | e appliance | | | | |
| 🔻 🌄 M-Guard Eval | Profile: | Demo Protocol | Version: | 0.1 | Tag: Dem | юР | Enab | ole |
| DemoP | Inbound Pee | r | | | Outbound Pe | er | | |
| | Peer address | IPv4 or IPv6 address | | | Peer address | IPv4 or IPv6 address | | |
| | Verify pe | eer's identity | | | Peer port | TCP port number | | |
| | Peer name | Domain name | | | ✓ Verify pe | er's identity | | |
| | | | | | Peer name | Domain name | | |
| | | | | | | | | |
| | | | | | | : | Τ | |
| | | | | | | <u>.</u> | | |
| | \ ` | | | Local | | • | | |
| | | | _ | | | | | _ |
| | Listen-on | hn1 | - | | Conne | ect-fro hn2 | | • |
| | Listen-on | | Ho Ho | stna | Conne | ect-fro | 1 | |
| | Listen port | TCP port number | | | | | / | |
| | | . | Flo | w na Response | | | 4 | |
| | | | | Flow rules | | | | |
| | | | Flo | w na Request | | | | |
| | | | | Flow rules | | | | |
| | A Missing re | equired fields: 'Peer name (inbo | und)', 'List | en-on address', 'Listen port' | , 'Peer name (outbo | ound)', 'Peer address (o | utbound)', 'P | eer |
| | | | | | Apply | Apply & Start | Cancel | |
| | | | | | | | 2011001 | |

Some notes on filling in the fields.

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

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

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

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

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

On the Guard networking, the options are as follows:

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

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

Below is how we have configured ours.





Click "Apply".

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

| e Project Appliance | e Guard Help | | | | | | | | | | |
|---------------------|--|-----------------------------|----------------|------------------------------------|---|----------|--------------|--------------|--------------------|----------|---|
| M-Guard Eval | Status: Guard confi | guration is incomplete. I | LS must be con | ifigured bef | ore it can be started | | | | | | |
| M-Guard Eval | Profil | le: Demo Protocol | Ver | sion: 0.1 | | Tag: | Demo | P | | Enable | |
| demop.guard.net (D | Inbound Peer | | | | | Outbo | und Pee | r | | | |
| | Peer address | 92,168.56.1 | | | | Peer a | ddress | 192,168,10 | 5.1 | | |
| | Verify peer's | identity | | | | Peer n | ort | 5269 | | | |
| | Peer name | edside quard net | | | | Ve | rify nee | r's identity | | | |
| | | casiaciguaramet | | | | Peer p | ame (| blackside o | uard not | | |
| | | | | | | T CCT II | unic | - | ouronnet | | |
| | ł | | | | Local | | | ÷ | | | |
| | Listen-on int | hn1 | • | | Local | | Cont | nect-from | hn2 | | |
| | Listen-on int Listen-on ad | hn1 192.168.56.5 | · / 24 | Hostname | Local demop.guard.net | | Cont | nect-from | hn2 | | |
| | Listen-on int Listen-on ad Listen port | hn1 192.168.56.5 5269 | • / 24 | Hostname | Local demop.guard.net | | Con | nect-from | hn2 | 5.5 | / |
| | Listen-on int Listen-on ad Listen port | hn1 192.168.56.5 5269 | / 24 | Hostname | Local demop.guard.net Response | | Cont | nect-from | hn2 192.168.100 | 5.5 | / |
| | Listen-on int Listen-on ad Listen port | hn1 192.168.56.5 5269 | / 24 | Hostname Flow name | Local demop.guard.net Response <u>Flow rules</u> | | Coni Coni | nect-from | hn2 | 5.5 | / |
| | Listen-on int Listen-on ad Listen port | hn1 192.168.56.5 5269 | / 24 | Hostname Flow name | Local demop.guard.net Response Flow rules Request | | Cont | nect-from | hn2 192.168.100 | 5.5 • | / |
| | Listen-on int Listen-on ad Listen port | hn1 192.168.56.5 5269 | × / 24 | Hostname Flow name Flow name | Local demop.guard.net Response Flow rules Request Flow rules | | Coni | nect-from | hn2 192.168.100 | 5.5 | / |

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

M-Guard Create New Guard Instance – configure TLS



The Following is displayed.

| M-Guard Create New Guard Instance – configure TLS |
|---|
| ■ Configure TLS × |
| Configure TLS Certificate |
| This will configure TLS for this guard. It will issue and install a certificate for 'demop.guard.net' and install the project's CA certificate as a trust anchor. |
| Any existing TLS configuration will be overwritten. Do you wish to proceed? |
| Yes No |
| Click "Yes". |
| After a Short period of time. |
| M-Guard Create New Guard Instance – configure TLS |



Click "OK".

The Following is displayed.



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

M-Guard Console - Guard demop.guard.net (DemoP) ٥ File Project Appliance Guard Help Status: guard is running as pid 35846. 🔻 🚞 M-Guard Eval 🔻 😽 M-Guard Eval Profile: Demo Protocol Version: 0.1 ✓ Enable Tag: DemoP Inbound Peer Outbound Peer Peer address 192.168.56.1 Peer address 192.168.106.1 Peer port 5269 ✓ Verify peer's identity Peer name redside.guard.net ✓ Verify peer's identity Peer name blackside.guard.net V Loci Listen-on int... hn1 Connect-from ... hn2 Listen-on ad... 192.168.56.5 / 24 Hostname demop.guard.net Connect-from ... 192.168.106.5 / 24 Listen port 5269 Flow name Response Flow rules Request Flow name Flow rules Apply & Restart Cancel

M-Guard Create New Guard Instance – configure TLS

Save Configuration.

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

M-Guard Create New Guard Instance – Configure Firewall

| M-Guard Cor | nsole - Appliance N | 1-G | uard Eval |
|---------------------|---------------------|------|----------------------------------|
| File Project | Appliance Gu | | Help |
| ▼ 🚞 M-Guard | Eval Status | : 12 | 2:25PM up 47 mins, 0 users, load |
| 🗾 🌄 😽 M-Gi | Jard Eval | | |
| dem ^{, Ne} | ew Guard | | |
| Se | tup | Þ | Set Hostname |
| Ge | et Status | | Configure Firewall |
| M | aintenance | Þ | Configure Interfaces |
| Fil | e Transfer | | Configure Clock Sync |
| Lo | g message | | Remote Logging |
| Ex | ecute Command | | Appliance Logging |
| Sa | ve Configuration | | Log Cleanup Configuration |
| Di | sconnect | | Authorize SSH Key |
| | | | Restrict SSH |
| | | | Generate TLS CSR |
| | | | Load TLS Certificate |
| | | | View TLS Certificate |
| | | | Load TLS Trust Anchor |
| | | | View TLS Trust Anchors |
| | | | Verify Trust |
| | | | |

The following is displayed.

M-Guard Create New Guard Instance – Configure Firewall

| Firewall Configuration | on | — | | × |
|---|--|------------|----------|---------|
| M-Guard Appliance has be changed using this di | a host-level firewall that restricts network traffic. Various setting alog. | s for this | firewa | ill may |
| Enable Firewall | | | | |
| ✓ Log firewall denials | | | | |
| These port sets should b 77,5333-5335: | e provided as a comma-separated list of port numbers or numb | oer ranges | ;, e.g.: | |
| Do not log ports | 135-139,445 1026,1027 1433,1434 | | | |
| Logging UDP ports | 514,162 | | | |
| Logging TCP ports | 514,601,6514 | | | |
| GCXP Ports | 24,35,57,59,75,77,87 | | | |
| | | Ok | | Cancel |

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

| M-Guard Create New | Guard Instance – Configure Firewall | | | |
|---|---|--------------|------------|-------|
| Firewall Configuration | on | — | | × |
| M-Guard Appliance has be changed using this di | a host-level firewall that restricts network traffic. Various settir alog. | igs for this | ; firewall | may |
| ✓ Enable Firewall | | | | |
| ✓ Log firewall denials | | | | |
| These port sets should b 77,5333-5335: | e provided as a comma-separated list of port numbers or nun | nber range | es, e.g.: | |
| Do not log ports | 135-139,445 1026,1027 1433,1434 | | | |
| Logging UDP ports | 514,162 | | | |
| Logging TCP ports | 514,601,6514 | | | |
| GCXP Ports | 24,35,57,59,75,77,87,5269 | | | |
| | | Ok | Ca | ancel |

Click "OK".

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

Select Appliance→Setup→Remote Logging...

M-Guard Create New Guard Instance – Configure Remote Logging



The following is displayed.

| M-Guard Create New G | uard Instance – Configure Remote L | ogging | | |
|--|---------------------------------------|----------------|----------|------|
| 📧 Remote Logging Co | _ | | \times | |
| The M-Guard Appliance logging server. | can be configured to send its logging | information to | a remote | 2 |
| Selector | daemon.* | | | |
| Protocol/Transport | syslog | | | Ŧ |
| Logging Server Address | | | | |
| Logging Server Port | | | | |
| | | | | |
| | | Save | Can | ncel |

Complete as below.

| M-Guard Create New Guard Instance – Configure Remote Logging | | | | | | | |
|---|-------------|------|-----|-----|--|--|--|
| 📧 Remote Logging Co | nfiguration | — | | × | | | |
| The M-Guard Appliance can be configured to send its logging information to a remote logging server. | | | | | | | |
| Selector | daemon.* | | | | | | |
| Protocol/Transport | syslog | | | • | | | |
| Logging Server Address | 10.178.0.1 | | | | | | |
| Logging Server Port | 514 | | | | | | |
| | | | | | | | |
| | | Save | Can | cel | | | |

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

Click "Save".

Save the Configuration.

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

Setup up the GCXP Producer and Consumer Certificates

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

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

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

Start GCXP Producer

| | ~ | | | | | | П | × |
|----------------------|--------|-----------|------------|----------|-------|---|---|---|
| Command Prompt | X | + * | | | | | | |
| | | | | | | | | |
| C:\M-Guard>java -jar | M-Guar | d-Console | -1.5.5.jar | gcxp-pro | ducer | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | - |
| | | | | | | | | |
| Start GCXP Producer | | | | | | | | |
| Enter SSH Passphrase | | | | | | × | | |

| | ~ |
|--|--------|
| M-Guard Console is configured to use an SSH key in C:\M-Guard\M-Guard Eval. You 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. | ı need |
| | |

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

ОК

Cancel

| Start GCXP Producer | | | | |
|-----------------------|-----------|---|---------|----------|
| M-Guard GCXP Producer | | - | | \times |
| File Configure Help | | | | |
| Status | | | | |
| Not configured | Configure | | Connect | |
| Log | | | | |
| | | | | |
| Content to Send | | | | |
| Send - Clear | | | | |
| | | | | Exit |

Click "Configure \rightarrow Certificate \rightarrow Create Certificate Signing Request..."

Create GCXP Producer Certificate

| 🔳 M- | Guard GCXP Producer | | | |
|--------|-------------------------|---|--|---|
| File | Configure Help | | 1 | |
| Status | Certificate | ÷ | Create Certificate Signing Request | Ì |
| | Configure XML Transform | | Remove Pending Certificate Signing Request | 1 |
| _ | Configure Repeat Send | | Import Certificate Chain | |
| Log | | | Show Current Certificate | |
| | | | Remove Current Certificate Configuration | |

The following is displayed.

| Create | GCXP | Producer | Certificate | |
|--------|------|----------|-------------|--|
| | | | | |

| Create CSR | for GCXP producer | _ | | \times |
|-------------------|--|------|-------|----------|
| The certificate s | igning request will be created for the GCXP producer w | ith: | | |
| Domain name: | redside.guard.net | | | |
| | | _ | | |
| | | Crea | ite (| Cancel |
| | | | | |

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

Click "Create".

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

| Create GCXP Producer Certificate | | | |
|--|-----------------------------|--------------------|--------|
| Select Folder for Certificate Signing Request | | | × |
| $\leftarrow \rightarrow \checkmark \uparrow$ isode Software \rightarrow CSRs and Certs | ~ C | Search CSRs and Ce | rts 🔎 |
| Organise 🔻 New folder | | | ≣ • 🕐 |
| 🛂 Videos 🖈 Name | Date modified | Туре | Size |
| System32 | No items match your search. | | |
| > 📮 This PC | | | |
| > 📫 DVD Drive (D:) C | | | |
| > 🧐 Network | | | |
| File name: redside_guard_net_csr.pem | | | ~ |
| Save as type: | | | ~ |
| | | | |
| ∧ Hide Folders | | Save | Cancel |

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



Click "OK".

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

On the M-Guard Console, click on "Project \rightarrow Certificate Authority...".

M-Guard Console issue GCXP Producer Certificate



The following is displayed.

M-Guard Console issue GCXP Producer Certificate

| Project CA for 'M-Guard Eval' | | \times |
|---|------------------|-------------|
| The Project's certificate authority is used to issue TLS certificates for GCXP peers. Select the | 'Process CSR' | |
| CA Certificate | | |
| The certificate authority certificate is named "M-Guard Eval" The certificate expires in 3644 day(s) | | |
| Export Renew Process CSR | <u>Get detai</u> | ls Close |

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

| Select CSR file | | , | | | × |
|--|------------|-------------------------------|------------------|-----------------------|--------|
| $\leftarrow \rightarrow \checkmark \uparrow$ | | ode Software > CSRs and Certs | ~ C | Search CSRs and Certs | م |
| Organise 🔻 Ne | ew folder | | | ≣ • | |
| Pictures | * | Name | Date modified | Туре | Size |
| 🕖 Music | * [|] redside_guard_net_csr.pem | 16/01/2025 12:56 | PEM File | 2 KB |
| 🔀 Videos | * | | | | |
| System32 | | | | | |
| 늘 Isode Softwa | ire | | | | |
| > 📃 This PC | | | | | |
| > 📫 DVD Drive (D |);) C | | | | |
| > 💁 Network | - | | | | |
| | File name: | | ~ | All Files | ~ |
| | | | | Open | Cancel |

M-Guard Console issue GCXP Producer Certificate

Select the CSR File and Click "Open.

| M-Guard Console issue GCXF | Producer Certificate | | | | | |
|--|----------------------|-------|-----|------|--|--|
| Issue Certificate | | — | | × | | |
| M-Guard certificate authority (CA) will now issue a certificate for the GCXP peer. Please enter the domain name(s) of the peer: | | | | | | |
| | redside.guard.net | | | | | |
| Domain Name(s): | | | | | | |
| | (| Issue | Car | ncel | | |

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

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

M-Guard Console issue GCXP Producer Certificate

| 💽 Certif | icate Issued | × |
|----------|--|---|
| i | The certificate has been successfully issued and the certificate chain has been written to "C:\\sode Software\CSRs and Certs\redside_guard_net_chain.pem". This can now be passed to the GCXP peer for installation. | |
| | ОК | |

Click "OK".

Now go back to your GCXP Producer and import the certificate chain. Click on "Configure \rightarrow Certificate \rightarrow Import Certificate Chain..."

Import GCXP Producer Certificate

| 🔳 M- | M-Guard GCXP Producer | | | |
|--------|-------------------------|------------|--|--|
| File | Configure | Help | | |
| Status | Certificate | • | Create Certificate Signing Request | |
| | Configure XML Transform | | Remove Pending Certificate Signing Request | |
| - | Configure R | epeat Send | Import Certificate Chain | |
| Log | | | Show Current Certificate | |
| | | | Remove Current Certificate Configuration | |

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

| Import GCXP Producer Cer | tificate | | | |
|---|---------------------------------|------------------|-----------------------|--------|
| Import Certificate Chain for GC | KP producer | | | × |
| \leftrightarrow \rightarrow \checkmark \uparrow | Isode Software > CSRs and Certs | ~ C | Search CSRs and Certs | م ; |
| Organise 🔻 New folder | | | ≣ • | · 🔲 🕐 |
| 🕖 Music 🔹 🖈 | Name | Date modified | Туре | Size |
| 🔀 Videos 🔹 🖈 | redside_guard_net_chain.pem | 16/01/2025 13:05 | PEM File | 4 KB |
| System32 | redside_guard_net_csr.pem | 16/01/2025 12:56 | PEM File | 2 KB |
| 📒 Isode Software | | | | |
| CSRs and Certs | | | | |
| > 💻 This PC | | | | |
| > 🖆 DVD Drive (D:) C | | | | |
| > 💁 Network | | | | |
| File nam | e: redside_guard_net_chain.pem | ~ | PEM Files Open | Cancel |

Select the "chain" file and not the "csr" file and Click "Open".

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







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

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

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

Start GCXP Consumer



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

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

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

Similarly, use M-Guard Console's "Project \rightarrow Certificate Authority..." to issue the certificate for this request from the consumer.

And finally, back to the GCXP Consumer, import the issued certificate for "blackside.guard.net" with "Configure \rightarrow Certificate \rightarrow Import Certificate Chain..."

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

Configure GCXP Producer and Consumer

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

| Configure GCXP Consumer | | | |
|-------------------------------|---|--------|---|
| M-Guard GCXP Consumer | - | | × |
| File Configure Help | | | |
| Status | | | |
| Not configured Configured | e | Listen | |
| Log | | | |
| Received Content | | | |
| 0 messages received | | Clear | |

Click on the "Configure..." button:

Configure GCXP Consumer

| Configure | M-Guard GCXP Consum — | | × | | |
|--|-----------------------|--|------|--|--|
| Specify name of the peer connecting to GCXP consumer (typically a Guard instance) and port that GCXP consumer is to listen on. Leave both fields blank to clear. | | | | | |
| Peer name | | | | | |
| Listen port | | | | | |
| | Clear | | Save | | |

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

| Configure GCX | ^p Consumer | | | |
|--|---|--|--|--|
| Configure M-Guard GCXP Consum – | | | | |
| Specify name of a Guard instand Leave both field | f the peer connecting to GCXP consumer (typically ce) and port that GCXP consumer is to listen on. ds blank to clear. | | | |
| Peer name | demop.guard.net | | | |
| Listen port | 5269 | | | |
| | Clear Cancel Save | | | |

Click on "Save".

Configure GCXP Consumer

| M-Guard GCXP Consumer | - | | \times |
|---|---|--------|----------|
| File Configure Help | | | |
| Status | | | |
| Ready to listen for peer demop.guard.net Configure. | | Listen | |
| log | | | |
| | | | |
| Received Content | | | |
| | | | |
| 0 messages received | | Clear | |

Click "Listen".

Configure GCXP Consumer – 🗆 🗙 M-Guard GCXP Consumer File Configure Help Status Listening for connection from peer demop.guard.net Stop Log Awaiting connection from peer... Received Content 0 messages received Clear

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

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

| Configure GCXP Producer | | |
|-------------------------|-------------------|----------|
| M-Guard GCXP Producer | - 0 | \times |
| File Configure Help | | |
| Status | | |
| Not configured | Configure Connect | |
| Log | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| Content to Send | | |
| | | |
| | | |
| | | |
| | | |
| Send Clear | | |
| | | Ewit |

Click on the "Configure..." button:

| Configure GCXP Pro | oducer | | | | |
|---|------------------|-------|-------|--|----------|
| Configure | M-Guard GCXP Pro | ducer | | | \times |
| Specify configuration information for the peer the GCXP Producer will connect to (typically a Guard instance). Leave all fields blank to clear. | | | | | |
| Peer name | | | | | |
| Peer address | | | | | |
| Peer port | | | | | |
| | | Clear | Cance | | Save |

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

| Configure GCXP Pro | ducer | | | |
|---|-------------------|--|--|--|
| 💽 Configure M-Guard GCXP Producer 🛛 🛛 🗙 | | | | |
| Specify configuration information for the peer the GCXP Producer will connect to (typically a Guard instance). Leave all fields blank to clear. | | | | |
| Peer name | demop.guard.net | | | |
| Peer address | 192.168.56.5 | | | |
| Peer port | 5269 | | | |
| | Clear Cancel Save | | | |

Click "Save"

| Configure GCXP Producer | | | |
|---|-----------|---------|---|
| M-Guard GCXP Producer | - | | > |
| File Configure Help | | | |
| Status | | | |
| Ready to connect to 192.168.56.5:5269 (demop.guard.net) | Configure | Connect | |
| Log | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Content to Send | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Send 👻 Clear | | | |
| | | | |

Click on the "Connect..." button

| Configure GCXP Producer | | | | |
|---|-----------|---|-----------|----------|
| M-Guard GCXP Producer | | - | | \times |
| File Configure Help | | | | |
| Status | | | | |
| Connected to 192.168.56.5:5269 (demop.guard.net) | Configure | | Disconnec | .t |
| Log | | | | |
| Connecting to peer TLS Handshake (producer) completed. GCXP (producer) started. | | | | |
| Content to Send | | | | |
| | | | | |
| Send 💌 Clear | | | | |
| | | | | Exit |

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

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

| M-Guard GCXP Consumer | - | |
|--|-----------|------|
| File Configure Help | | |
| tatus | | |
| Awaiting GCXP messages from peer demop.guard.net | Configure | Stop |
| og | | |
| Awaiting connection from peer Accepted connection from peer. TLS Handshake (consumer) completed. GCXP (consumer) started. | | |
| ceived Content | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Send messages between GCXP Producer and Consumer

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

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

GCXP Producer Configure Catalogue

| M-Guard GCXP Producer | | | | | | | |
|-----------------------|--|--|--|--|--|--|--|
| File Configure Help | | | | | | | |
| ole Data | | | | | | | |
| xample Catalogs | | | | | | | |
| rom File | | | | | | | |
| | | | | | | | |
| | | | | | | | |

The following will be displayed.

GCXP Producer Configure Catalogue

| 🔳 Config | ure Example Cat | talogs | | | |
|--------------|------------------|-------------------------------------|-------------------------------|--|--------|
| Example cat | talogs provide e | xample content for use in GCXP | consumer. | | |
| Select the e | xample catalog | to use from the list of built-in ca | atalogs. | | |
| Active | Туре | Name | Synopsis | Description | Import |
| | Built-in | Base XML examples | Basic XML snippets | Some basic XML snippets for testing rules from the built-in XML base rule catalog | Remove |
| | Built-in | Demo protocol examples | Examples of the demo protocol | Example XML of the demo protocol, for use with testing M-Guard Console's demo protocol rules | View |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | Save | Cancel |

Enable the Built-in "Demo protocol examples" option.

Click "Save".

Select "File \rightarrow Load Example Data..."



Expand "Demo Protocol Examples"

The following is displayed.

GCXP Producer Load Example Data

💽 Load Example Data

M-Guard Console provides a number of example snippets to use for testing M-Guard Console. Select the desired one below then press the select button to load it.

| Name | Description | | | | | |
|--|---|--|--|--|--|--|
| Demo protocol examples | Example XML of the demo protocol, for use with testing M-Guard Console's demo protocol rules | | | | | |
| Simple Stanza | An example stanza of the demo protocol | | | | | |
| With comment | A demo protocol stanza which includes an XML comment | | | | | |
| With three body elements | A demo protocol stanza with three body elements | | | | | |
| No language attribute | A demo protocol stanza without a language attribute within the body element | | | | | |
| With large body | A demo protocol stanza with a body element of over 200 bytes | | | | | |
| With ESS label | A demo protocol stanza with an XEP-258 ESS security label | | | | | |
| With NATO metadata (simple) | A demo protocol stanza with a NATO metadata label applied to the whole stanza | | | | | |
| With NATO metadata (alternative) | A demo protocol stanza with alternative NATO metadata label | | | | | |
| With NATO XMPP-style metadata (sim | A demo protocol stanza with a NATO XMPP metadata label applied to the whole stanza | | | | | |
| With NATO XMPP-style metadata (alter | A demo protocol stanza with alternative NATO XMPP metadata label | | | | | |
| | Cancel Select | | | | | |

Select "Simple Stanza"

GCXP Producer Load Example Data

| M-Guard GCXP Producer | | - | | × |
|---|-----------|---|----------|------|
| File Configure Help | | | | |
| Status | | | | |
| Connected to 192.168.56.5:5269 (demop.guard.net) | Configure | | Disconne | ct |
| Log | | | | |
| Connecting to peer TLS Handshake (producer) completed. GCXP (producer) started. | | | | |
| Content to Send | | | | |
| <demo xmlns="http://isode.com/guard/demo-protocol/0"></demo> | | | | |
| Send Clear | | | | |
| | | | | Exit |

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

GCXP Receive Example Data

| M-Guard GCXP Consumer | - | | \times |
|--|---|-------|----------|
| File Configure Help | | | |
| Status | | | |
| Awaiting GCXP messages from peer demop.guard.net | | Stop | |
| Log | | | |
| Awaiting connection from peer Accepted connection from peer. TIS Handshake (consumer) completed. GCXP (consumer) started. Accepting forwarded message (id=000000000000000000000000000000000000 | | | |
| start of data <demo xmlns="http://isode.com/guard/demo-protocol/0"><body xml:lang="en">This is my body</body><date-time>2019-11-20T10:24:53</date-time>/demo> end of data</demo> | | | |
| 1 message received | | Clear | |

Your Guard is successfully passing Data.

Now to test some Rules.

Return to M-Guard Console and select the Guard.

M-Guard Console Configure Rules



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

M-Guard Console Configure Rules

| Configure Flow Request | | | \times |
|--|-----------------|-----------------------|-------------|
| Content Rules | | | |
| Allow requests | (| Advanc | ed |
| Rules Applied from Inbound to Outbound | | | |
| Rule Catalog for arbitrary XML 1 | | | â |
| Demo Protocol 1 | | | |
| ▼ DemoP Base Rules | | | |
| Prohibit xml:id | | | |
| ▼ Body Rules | | | |
| Restrict number of body elements | | | |
| Minimum number of body elements allowed. 0 | | | |
| Maximum number of body elements allowed. | | | |
| Restrict body length | | | |
| Maximum Body Length 20 | | | |
| Prohibit language tag | | | |
| Require language tag | | | |
| Restrict Janouage tag | | | ~ |
| Rate Limiting | | | |
| This option enables rate limiting. When enabled, the Guard instance will not commence proces (other than the first) until the specified minimum interval has elapsed since commencement of the previous message. | sing o the p | of a mess rocessin | age g of |
| Minimum internal (millionenade) | | | |
| Minimum Interval (milliseconds) | | | |
| A | oply | Car | ncel |

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

Click "Apply".

| M-Guard Console - Guard File Project Appliance | d demop.guard.net (De Guard Help | :moP) | | | | | - 0 X |
|---|-------------------------------------|------------------|--------------|-----------------|--------------|---------------------|---------------|
| M-Guard Eval | Status: guard is runni | ng as pid 35846. | | | | | |
| * 🌄 M-Guard Eval | Profile: | Demo Protocol | Version: 0.1 | | Tag: Dem | юР | V Enable |
| | Inbound Peer | | | | Outbound Pe | er | |
| | Peer address 192 | 2.168.56.1 | | | Peer address | 192.168.106.1 | |
| | ✓ Verify peer's id | lentity | | | Peer port | 5269 | |
| | Baar nama Irad | ride quard not | | | Varify pa | ar's identity | |
| | reername | side.guard.net | | | Veniy pe | | |
| | | | | | Peer name | blackside.guard.net | |
| | | | _ | Local | | • | • |
| | Listen-on int | nn1 | - | | Cor | nnect-from hn2 | • |
| | Listen-on ad | 192.168.56.5 / 2 | .4 Hostname | demop.guard.net | | anact from 102.1 | 59 106 5 / 24 |
| | Listen port | 5269 | | | CO | 192.1 | / 24 |
| | | + | Flow name | Response | | | |
| | | - | | Flow rules | | - | |
| | | | Flow name | Request | | | |
| | | | | Flow rules | | | |
| | | | | | | | |
| | | | | | Apply | Apply & Res | tart Cancel |

Then click on "Apply & Restart" on the Guard:

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

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

| MI-GUARG GCAP Producer | | _ | | |
|---|-----------|---|----------|----|
| ile Configure Help | | | | |
| tatus | | | | |
| Connected to 192.168.56.5:5269 (demop.guard.net) | Configure | | Disconne | ct |
| og | | | | |
| ILS Handshake (producer) completed. SCXP (producer) started. | | | | |
| Sending request (id=00000000:0000001). Connection failed: no next item. Connecting to peer ILS Handshake (producer) completed. GCXP (producer) started. | | | | |
| Sending request (id=00000000:0000000). Connection failed: no next item. Conneting to peer TLS Handshake (producer) completed. GCXF (producer) started. | | | | |
| <pre>Sending request (id=000000010000000). Connection failed: no next item. Connecting to peer TLS Handshake (producer) completed. GCXP (producer) started.</pre> | acters | | | |

Click "Send".

GCXP Producer Send Long Message

| Guard GCXP Producer | | - | | × |
|---|-----------|---|----------|------|
| File Configure Help | | | | |
| Status | | | | |
| Connected to 192.168.56.5:5269 (demop.guard.net) | Configure | | Disconne | ct |
| Log | | | | |
| <pre>TLS Handshake (producer) completed. GCXP (producer) started. Sending request (id=0000000:00000001). Connecting to peer TLS Handshake (producer) completed. GCXP (producer) started. Sending request (id=00000000:00000002). Got response (id=00000000:00000002): not accepted.</pre> | | | | |
| <pre><demo xmlns="http://isode.com/guard/demo-protocol/0"></demo></pre> | racters | | | |
| | | | | Exit |

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

Also, nothing is received on the Consumer.

Additionally, an "Alert" is received on the Syslog server.

| Syslog Serve | r Alert | | | | | |
|--------------------|--------------|-----------------------|----------|-----------|------------------------------------|---|
| 📰 Visual Syslog S | Server 1.6.3 | | | | | – 🗆 X |
| Setup Fo | A Process | sing Highlighting Got | new Mo | re View p | vrev View next View file | Clear About Terminate |
| Message filtering | 3 III | All messages match | | | | |
| Displaying 25 mess | anes | | | | | |
| Time | | Host | Facility | Priority | Tag | Messane |
| Jan 16 13:32:57 | 10.178.0.2 | demop.guard.net | daemon | notice | DemoP[35847] blackside.guard.net | start |
| Jan 16 13:45:50 | 10.178.0.2 | demop.guard.net | daemon | info | DemoP[35847] redside.guard.net Pas | message id=00000000:00000001 type=Request: okav |
| Jan 16 13:45:50 | 10.178.0.2 | demop.guard.net | daemon | debua | DemoP[35847] blackside.guard.net | deliver id=00000000:00000001 type=Reguest |
| Jan 16 13:45:50 | 10.178.0.2 | demop.guard.net | daemon | debug | DemoP[35847] blackside.guard.net | write complete, queue empty |
| Jan 16 14:04:51 | 10.178.0.2 | demop.guard.net | daemon | notice | | DemoP[35847] M-Guard stopped |
| Jan 16 14:04:52 | 10.178.0.2 | demop.guard.net | daemon | notice | | DemoP[64605] M-Guard running |
| Jan 16 14:04:52 | 10.178.0.2 | demop.guard.net | daemon | notice | DemoP[64605] dst | 192.168.106.1:5269 (blackside.guard.net) |
| Jan 16 14:04:52 | 10.178.0.2 | demop.guard.net | daemon | notice | DemoP[64605] src | 192. 168. 56. 5: 5269 (redside.guard.net) |
| Jan 16 14:04:52 | 10.178.0.2 | demop.guard.net | daemon | notice | | DemoP[64605] Accepting on 192.168.56.5:5269 (redside.guard |
| Jan 16 14:06:30 | 10.178.0.2 | demop.guard.net | daemon | notice | | DemoP[64605] Incoming connection from 192.168.56.1:51895 o |
| Jan 16 14:06:30 | 10.178.0.2 | demop.guard.net | daemon | debug | | DemoP[64605] Incoming connection accepted, proceeding with 1 |
| Jan 16 14:06:30 | 10.178.0.2 | demop.guard.net | daemon | debug | | DemoP[64605] Incoming connection TLS negotiation successful. |
| Jan 16 14:06:30 | 10.178.0.2 | demop.guard.net | daemon | notice | | DemoP[64605] Connecting to 192.168.106.1:5269 (blackside.gu |
| Jan 16 14:06:30 | 10.178.0.2 | demop.guard.net | daemon | debug | | DemoP[64605] Outgoing connection TLS negotiation successful. |
| Jan 16 14:06:30 | 10.178.0.2 | demop.guard.net | daemon | notice | DemoP[64605] redside.guard.net | start |
| Jan 16 14:06:30 | 10.178.0.2 | demop.guard.net | daemon | notice | DemoP[64605] blackside.guard.net | start |
| Jan 16 14:08:09 | 10.178.0.2 | demop.guard.net | daemon | alert | | DemoP[64605] redside.guard.net Content Alert - reject (Drop): |
| Jan 16 14:08:09 | 10.178.0.2 | demop.guard.net | daemon | debug | DemoP[64605] redside.guard.net | deliver id=00000000:00000002 type=Response |
| Jan 16 14:08:09 | 10.178.0.2 | demop.guard.net | daemon | debug | DemoP[64605] redside.guard.net | write complete, queue empty |
| | | | | | | |

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

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

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

What Next?

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

Whitepapers

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

Copyright

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

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

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

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

This manual is © copyright Isode Limited 2025.