

## **RFM-VM**

---

### **Virtual appliance guidelines**

---

## REVISION HISTORY

REVISION	DATE	CHANGES	Written by	Checked by
A	13/05/2022	Creation	D. Jeannin	P. Duchesne

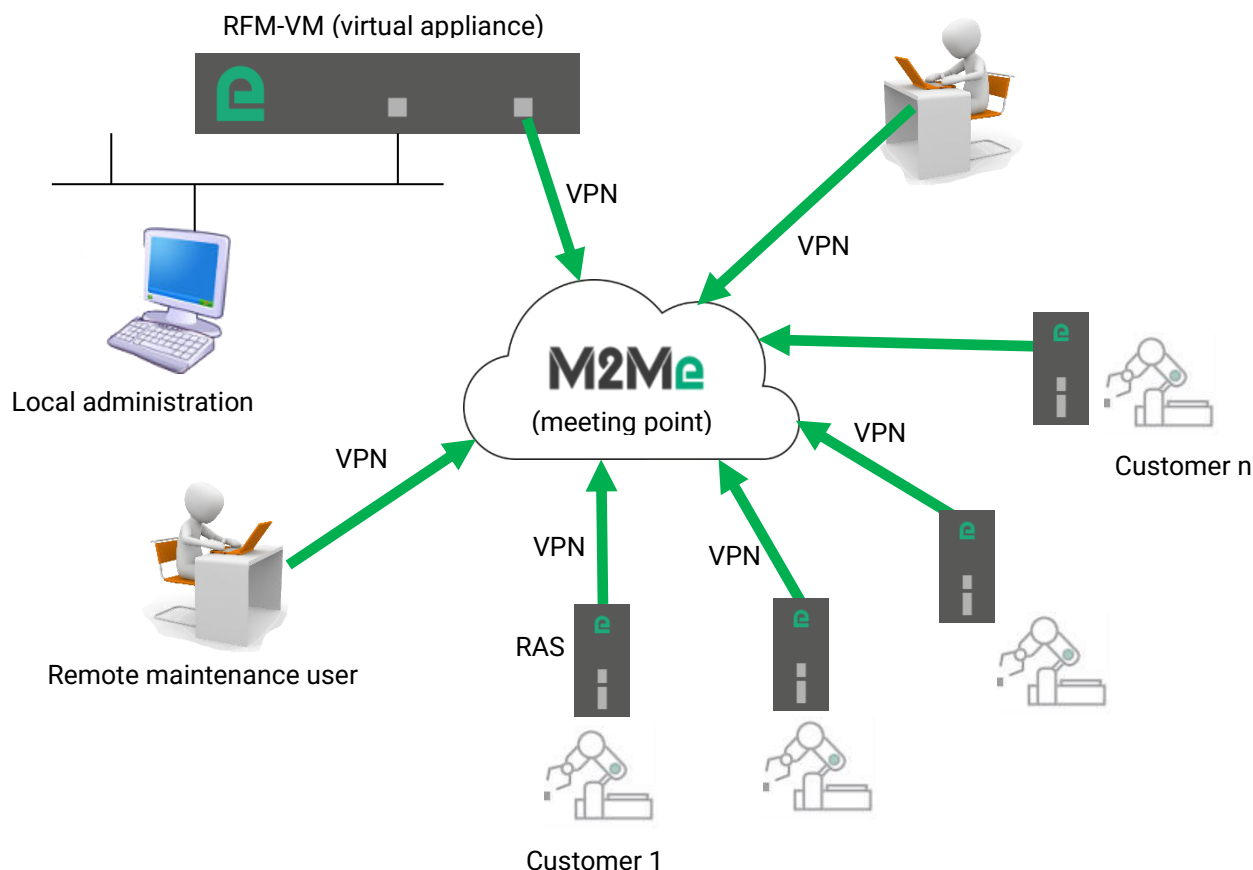
## Table of Contents

1	Description .....	4
2	Features.....	4
3	Technical characteristics .....	5
4	Security .....	5
4.1	Network flow map .....	5
4.2	OpenVPN Ciphers .....	6
4.3	Personal data management .....	6
4.4	Vulnerability management .....	6
4.5	Configuration secrets management .....	7
5	Installation on VMWare ESXi.....	7
6	Networking configuration steps.....	7
7	Configuring the remote access to the Fleet management system .....	7
8	Backups .....	8

## 1 Description

The RFM-VM is a virtual appliance that manage the credentials and access rights of the remote maintenance users on a fleet of Etic telecom Machine Access Box connected to the M2Me service.

The M2Me service is a networking cloud built to give an IP connectivity to devices that cannot be reached from the Internet.



## 2 Features

The RFM-VM is built to manage in a centralized way the access rights management to a fleet of RAS devices (remote access boxes by Etic Telecom).

- User list and credentials
- Password policy (password strength and renewal management)
- Temporary users
- Access rights to the RAS
- M2Me client device list

### 3 Technical characteristics

Virtual appliance

Target Hypervisor: Vmware ESXi

RAM: 1Go

HDD: 25Go

CPU: 1

Network 1: Administration

Network 2: WAN

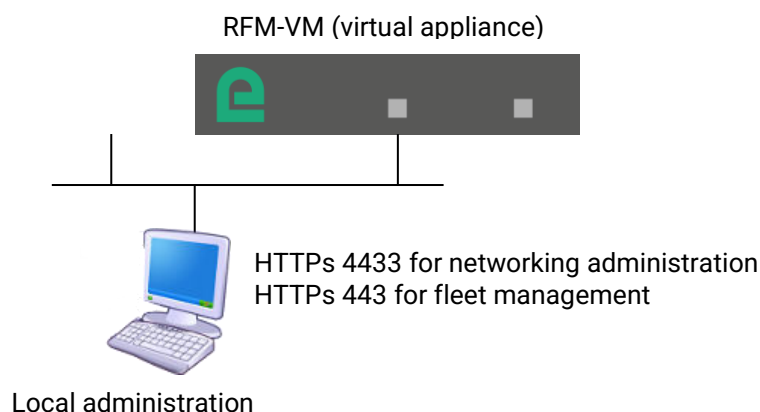
Administration can be done by remote access (OpenVPN on M2Me service) if needed.

### 4 Security

#### 4.1 Network flow map

The RFM exposes 2 web servers on the administration port (Network device 1):

- The administration interface (on http 8080 by default -> should be changed to HTTPs 4433). On this interface protected by login/password we can do the networking configuration of the appliance
- The fleet management interface on HTTPs 443. This interface is the interface that is daily used by the fleet administrator.



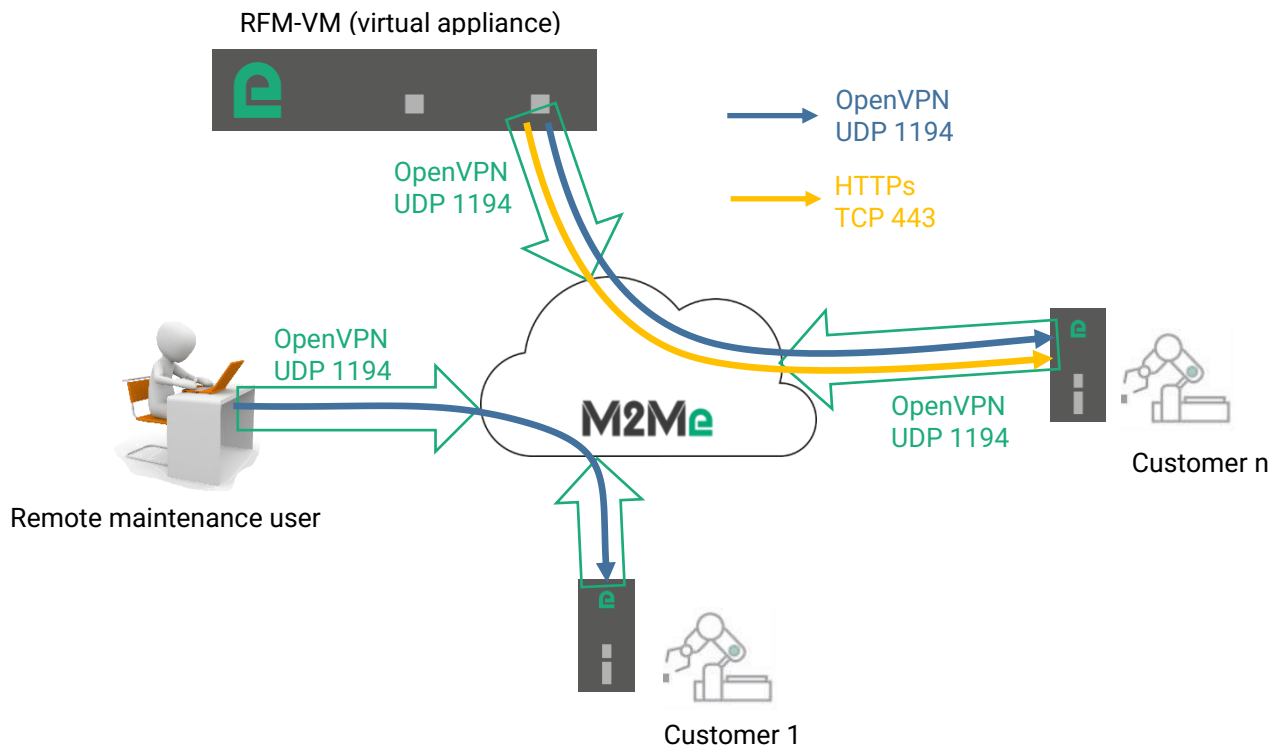
The RFM-VM is only doing outgoing connection to eticnet1.com (the M2Me OpenVPN service) with one of the following protocol/port:

- UDP 50000
- UDP 1194
- UDP 5000
- UDP from 50001 to 51000
- TCP 50000
- TCP 1194
- TCP 5000
- TCP 443
- TCP 80
- TCP from 50001 to 51000

The RFM choose automatically one outgoing open port on the previous list. This outgoing port can be forced by configuration.

When connected the RFM-VM opens 2 ports inside the M2Me service VPN:

- An HTTPs API (HTTPs 443) needed by the M2Me clients to get the list of the devices it can access
- An OpenVPN server (UDP 1194) for remote access for administration



## 4.2 OpenVPN Ciphers

- M2Me service VPN uses BF-CBC with MD5 authentication (this VPN doesn't transit any sensitive information)
- Remote access VPN is negotiated by NCP. At this day a connection done with a M2Me client uses AES-256-GCM.

## 4.3 Personal data management

No data are transferred to the Etic Telecom infrastructure. The Etic Telecom infrastructure doesn't store any information owned by our customers (user list, credentials, access rights...).

## 4.4 Vulnerability management

The vulnerability management on the RFM-VM product is done by Etic Telecom. The firmware releases are scheduled on a yearly basis, but security fixes can be done during the year if needed. Each customer registered on our "partners club" is informed that a new software release is available. The installation is done by the owner of the virtual appliance.

## 4.5 Configuration secrets management

The configuration can be extracted from the RFM by the administrator. The administrator can encrypt the configuration file during the extraction process to avoid exposing sensitive information.

## 5 Installation on VMWare ESXi

On VMware Esxi hypervisor create a new virtual machine from OVF or OVA file.  
Choose a name for the VM and select the OVA file given by Etic Telecom and create the VM  
Connect the administration network adapter to the right vSwitch.

## 6 Networking configuration steps

Go to the WEB administration interface: <http://192.168.0.128:8080>

Secure the administration WEB access:

- "> Setup > Security > Administration rights"
- Set an administration password
- Set "Password protect the configuration interface"
- Set "Password protect the configuration interface" to "HTTPs only"
- Disable the ssh server

Administration is now available on <https://192.168.0.128:4433>

Configure the Internet access:

- If you want to connect on the network adapter 1: from the menu "> Setup > LAN Interface > Ethernet and IP".
- If you want to connect on the network adapter 2: from the menu "> Setup > WAN Interfaces > Ethernet".

Enable the M2Me service connection on the menu "> Remote access > M2Me\_Connect"

Check if the appliance is connected to the M2Me service ("Diagnostics > Network status > M2Me")

Get the product key on the "About" page

## 7 Configuring the remote access to the Fleet management system

Fleet management system is available on the port TCP 443 <https://192.168.0.128:443>

Default user is login= "etic" password = "etictelecom"

Click on the "Fleet management" logo

On the user section create a user. On the user creation form select the checkbox "RAS manager administrator"

You can now remove the default "etic" user.

If you do the fleet management administration through a remote access connection (if administration port not available), you must configure the remote access VPN to the RFM. This can be done through the fleet management interface:

- On the "device page" add a new device
- Fill the form with the RFM-VM product key and the administration credentials (use direct access mode)
- On the "user page" create an administration group, add the users that should administrate the RFM and add access to the RFM
- On the "device page" click on the "synchronize button" for the RFM
- You can now access to the RFM through the M2Me service.

You can now give the user credential and the product key to the team who is doing the fleet management administration.

## **8 Backups**

The RFM can be configured to do a daily backup of the fleet management system on the hard drive of the virtual machine.