FIREMON

Azure VMI Launch & FMOS Installation

Date: 23 September 2020

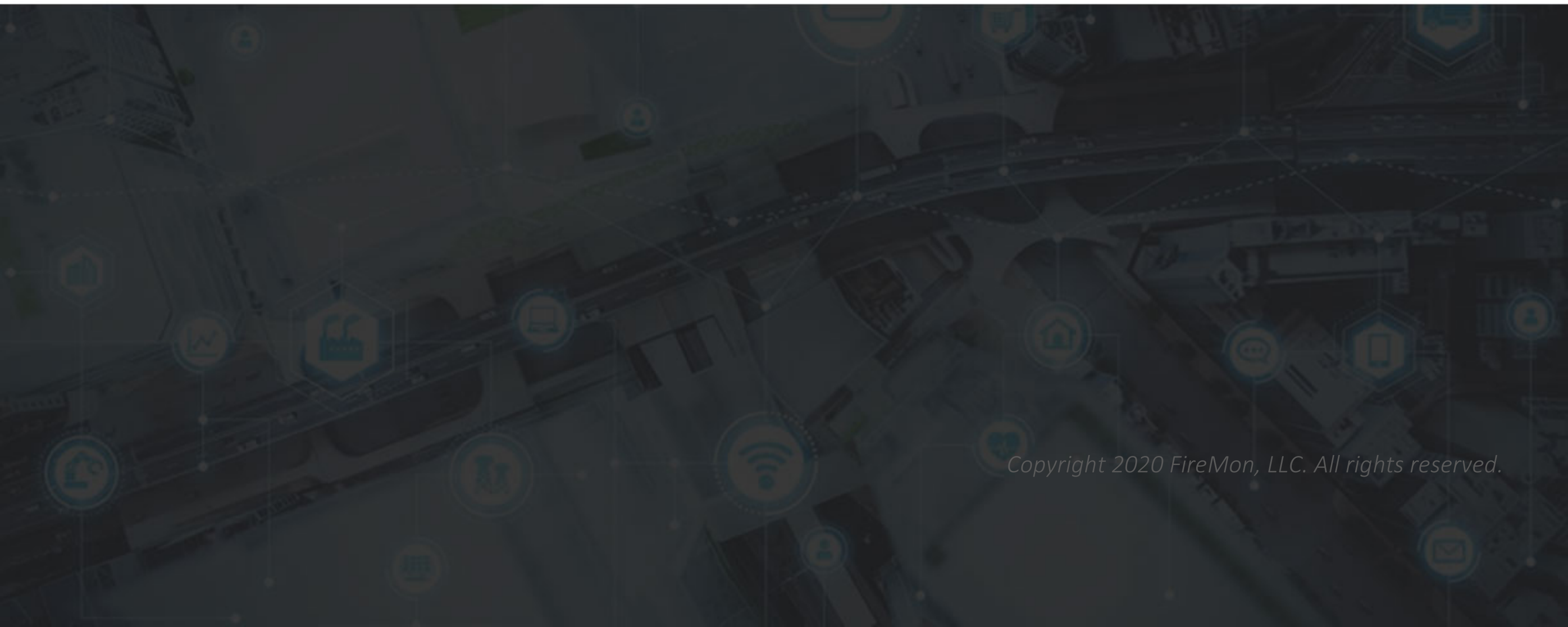


Table of Contents

Overview 3

Step 1: Launch Azure Marketplace VMI 3

Step 2: Create the Virtual Machine 3

Step 3: FMOS Initial Setup Authentication for Azure 5
Initial User Account 5
Setup UI Administration... 5

Step 4: FMOS Initial Setup Completion for Azure 7
FMOS Administrative User 7
Organization Information..7
Machine Configuration 7

Overview

FMOS can run as a virtual machine on the Microsoft Azure cloud platform. FireMon has taken the need to manually set up the VMI by providing it as a download using the Azure Marketplace.

This is a bring your own license (BYOL) VMI, you must already have a SIP license to activate the subscription.

Step 1: Launch Azure Marketplace VMI

1. Log in to the Azure Marketplace.
2. Search for **FireMon** and select the **FireMon Security Intelligence Platform BYOL** entry.
3. Click **Get it Now**.
4. Click **Continue** to accept terms of use, and to create this app in Azure.

Step 2: Create the Virtual Machine

1. Open the Microsoft Azure portal, and navigate to virtual machines. (**Azure Services** > **Virtual Machines**).
2. Click **Add** > **Virtual Machine**.
3. In the **Basics** section:
   - **Subscription**: Select the FireMon subscription.
   - **Resource Group**: Click **Create new** or select an existing group from the list.
   - **Virtual machine name**: Type a name for the VM.
   - **Region**: Select your location.
   - **Image**: Select the FireMon VMI from the list.
   - **Size**: Select from the list recommended by image publisher.
     Recommended: A minimum of 32 GB of RAM
   - **Authentication type**: Select **Password**. This information will be used to log in to the FMOS Initial Setup form.
     - **Username**
     - **Password**
     - **Confirm password**
   - **Public inbound ports**: Select **Allow selected ports**.
   - **Select inbound ports**: Select **443** (HTTPS) and **22** (SSH) from the list.
     Note: Port 443 is used to access web-based applications, port 22 is for admin access.
4. Click **Next: Disks** to continue to add disks.

5. In the **Disks** section:
    - **OS disk type**: Select **Premium SSD**.
    - **Encryption type**: Select the default value.
    - Click **Create and attach a new disk** and add a data disk size of at least 1024 GB.
        - **Name**: use the default name provided or enter a new name
        - **Source type**: Select **None (empty disk)**
        - **Size**: Click **Change size** to select **1024 GiB** if not already selected
        - **Encryption type**: Select the **Default**
        - **Enable shared disk**: Select **No**
        - Click **OK**

Note: An additional empty disk size of 1024 GB must be added to prevent a setup process failure.

6. Click **Review + create** to review the settings entered.
7. Click **Create** to begin the virtual machine creation process. This process may take several minutes.
8. Once your machine is created, click on the newly created VM from the list, then under **Settings** select **Networking** to allow inbound port 55555 for the FMOS Control Panel server (needed for the Initial Setup configuration).
    - Click **Add inbound port rule**.
    - **Source**: Type the **IP address of the new VM**
    - **Source IP addresses:** Type the IP address of the user accessing the VM
    - **Source port ranges**: Type an asterisk (*****)
    - **Destination**: Select **Any**
    - **Destination port ranges**: Enter **55555**
    - **Protocol**: Select **TCP**
    - **Action**: Select **Allow**
    - **Priority**: Type **100**
    - **Name:** Type a unique name (example: FMOS-CP)
    - Click **Add**

Note: Verify that ports 443 and 22 are also listed as allowed. If not, repeat the steps to add these ports.

Step 3: FMOS Initial Setup Authentication for Azure

The initial setup process for machines deployed in cloud environments differs from the process for machines deployed in traditional data centers. Because cloud environments do not typically provide a mechanism for accessing the graphical console of a machine, the FMOS Initial Configuration Wizard is not available. Instead, FMOS provides a web-based alternative, the FMOS Initial Setup UI.

The FMOS Initial Setup UI is hosted by the FMOS Control Panel server, and as such is available over TLS on TCP port 55555.

> **Note**: The FMOS Control Panel always uses a self-signed certificate initially, so browsers will present a security warning. This cannot be avoided, because the machine has not yet been configured and so does not have a host name or access to a trusted certificate authority.

The FMOS Initial Setup is responsible for collecting critical information about the system that is required to perform the initial deployment. Among the values it collects are the credentials for the first FMOS administrative user. This user is authorized to log in to the FMOS CLI using SSH, run the **`fmos`** command, and use the FMOS Control Panel.

Initial User Account

When FMOS boots for the first time in a cloud environment, it will automatically create the initial administrative user account. This must be done before you can complete the FMOS Initial Setup process.

The process for creating the user at first boot will be:

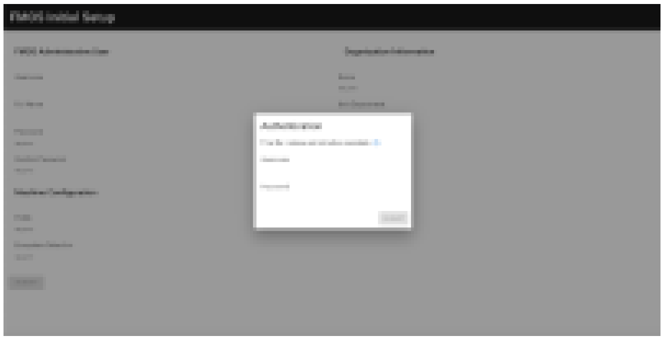
- The system will copy the OVF metadata from the virtual removeable disc to persistent storage.
- The system will create a new Linux user account. The username is as specified by the user during VM creation, which is provided in the OVF metadata.
- The system will assign the FMOS Administrator privilege to the account.
- The system will set the password for the new account. The password is as specified by the user during VM creation, which is provided in the OVF metadata; if the user specified an SSH key instead of a password, the password is the first 12 characters of the base64-encoded SHA256 fingerprint of the SSH public key.

Setup UI Administration

Because the administrator must be prompted for the instance ID before being allowed to change the password for the initial FMOS administrator account, the FMOS Initial Setup must be protected with authentication. This will ensure that the user provides proper credentials before being allowed to perform the Initial FMOS Setup process and thereby changing the initial account password.

The authentication procedure will be:

1. Open a web browser to navigate to the hostname or IP address of SIP for the Azure VM. For example, **https://<hostname_or_IPaddress>:55555/setup**, replacing <*hostname_or_IPaddress*> with the host name or IP address of the instance to configure.
2. The UI will display an **Authentication** dialog box before opening the FMOS Initial Setup form.

   a. **Username** is the **username for the created VM**.
   b. **Password** is the **password for the created VM**.
   c. Click **Submit**.
3. Following successful authentication, the UI will hide the Authentication dialog box and display the FMOS Initial Setup form.
4. Continue to Step 4: FMOS Initial Setup Completion for Azure.

Step 4: FMOS Initial Setup Completion for Azure

After the FMOS initial setup authentication completes, you will continue to enter information in the required fields to finish setup of an Azure cloud deployment.

FMOS Administrative User

1. The username is read-only and cannot be changed, but you can update the password.
    a. **Username**—The username for the VM.
    b. **Full Name** (optional) — The full name of the FMOS admin user.
    c. **Password**—The password for the VM.
    d. **Confirm Password** — Retype the VM password.

Organization Information

2. Enter your organization's information.
    a. **Name** —The name of your company or organization.
    b. **Unit/Department** (optional) —The name of the department, team, unit, etc.
    c. **City** (Optional) —The location of the organization or where the machine is deployed.
    d. **State/Province** (optional) —The state or province of the organization or where the machine is deployed.
    e. **Country** (optional) —The country of the organization or where the machine is deployed.

Machine Configuration

3. Enter the FQDN.
4. Select the type of deployment this will be.
    a. **Single-Server Deployment**—This server is the only server in the deployment. It will perform all the functions of SIP without communicating with other servers.
    b. **Existing Deployment**—This server will be part of a deployment that already exists in the organization. The specific functions this server will perform will be configured later.
    c. **New Deployment**—This is the first server in a new multi-server deployment. It will hold the Database and Enterprise Search roles.
5. Click **Submit**.

6. Click the **FMOS Control Panel** link in the deployment progress message to continue configuration, and log in using your CLI credentials.

During initial deployment, the FMOS Control Panel server certificate will be replaced. Browsers will typically warn users when a server's certificate has changed, so accessing the FMOS Control Panel after using the FMOS Setup UI may generate such a warning. It is safe to proceed.

7. After the deployment process completes, you can log in to Security Intelligence Platform to continue setting up your network, such as adding users and devices.
   a. Open another browser tab.
   b. Enter the IP address of your Azure VM, For example, **https://<hostname_or_IPaddress>**.
   c. Enter your username and password:
      - Username is **firemon** (case-sensitive)
      - Password is the MAC address for the VM with colons removed and lowercase letters instead of uppercase letters. For example, a MAC address of 00:05:95:A1:2B:CC would be 000595a12bcc. This is a one-time password to use at first installation and will need to be reset after initial login.
      - Click **Log In**

Note: Reference the *Getting Start Guide* for more configuration information.