FortiGate Deployment Guide

Contents

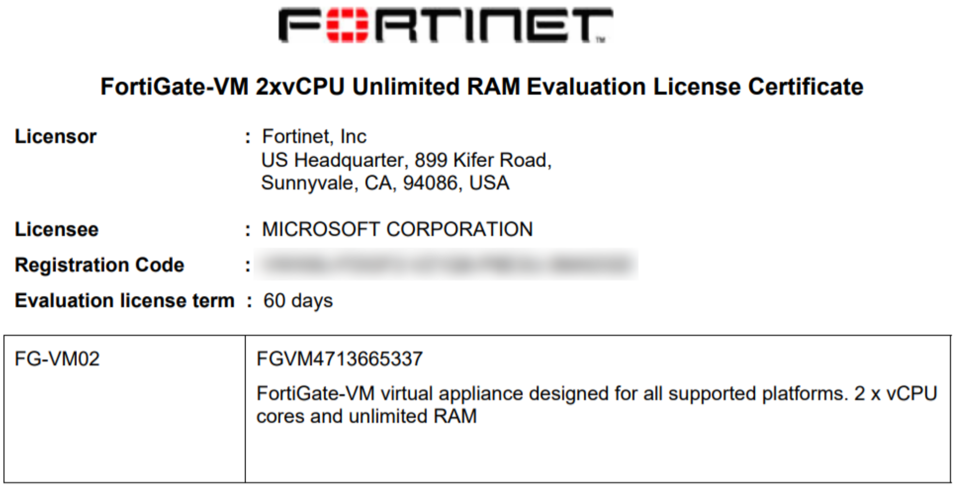
Redeeming the FortiGate License

The Fortinet FortiGate Next-Generation Firewall product is available as a virtual machine in Azure IaaS. There are two licensing modes for this virtual machine –

- Pay-as-you-go (PAYG)
- Bring your own license (BYOL)

While partnering with Fortinet to provide Secure Hybrid Access (SHA) guidance, Fortinet may provide members of the Azure AD Get to Production SHA team with licenses. In cases where no license has been provided, the PAYG deployment will also work.

In cases where a license has been issued, Fortinet provides a registration code that must be redeemed online –



FortiGate-VM 2xvCPU Unlimited RAM Evaluation License Certificate

Licensor : Fortinet, Inc
US Headquarter, 899 Kifer Road,
Sunnyvale, CA, 94086, USA

Licensee : MICROSOFT CORPORATION

Registration Code : [redacted]

Evaluation license term : 60 days

FG-VM02	FGVM4713665337 FortiGate-VM virtual appliance designed for all supported platforms. 2 x vCPU cores and unlimited RAM

1. Register at https://support.fortinet.com/
2. After registration, sign-in at https://support.fortinet.com/
3. Navigate to **Asset** -> **Register/Activate**
4. Enter the Registration Code provided by Fortinet
5. Specify the registration code, select **The product will be used by a non-government user** and click **Next**
6. Enter a Product Description (e.g. FortiGate), set the Fortinet Partner as **Other** -> **Microsoft** and click **Next**
7. Accept the **Fortinet Product Registration Agreement** and click **Next**
8. Accept the **Terms** and click **Confirm**
9. Click the **License File Download** and save the license for later

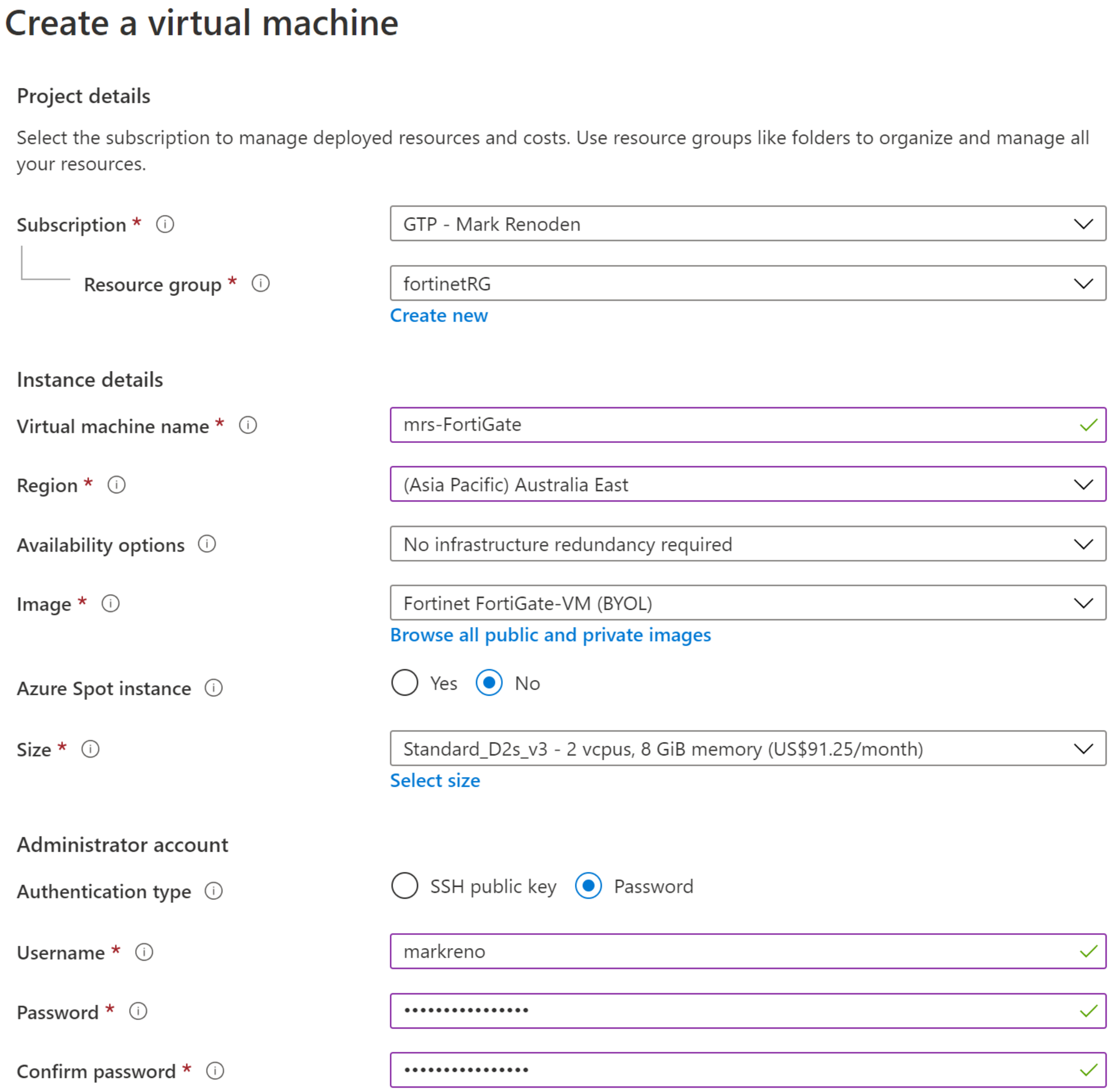
Download Firmware

At the time of writing, the Fortinet FortiGate Azure VM does not ship with the firmware version needed for SAML authentication. The latest version must be obtained from Fortinet.

1. Sign-in at https://support.fortinet.com/
2. Navigate to **Download** -> **Firmware Images**
3. Click **Download** to the right of **Release Notes**
4. Click **v6.00**
5. Click **6.4**
6. Click **6.4.1**
7. Download **FGT_VM64_AZURE-v6-build1637-FORTINET.out** by clicking on the **HTTPS** link on the same row
8. Save the file for later

Deploy the FortiGate VM

1. Navigate to https://portal.azure.com and sign-in to the subscription into which you wish to deploy the FortiGate Virtual Machine
2. Create a new Resource Group or open the Resource Group into which you wish to deploy the FortiGate Virtual Machine
3. Click **Add**
4. Enter "Forti" into the **Search the Marketplace** dialog and select **Fortinet FortiGate Next-Generation Firewall**
5. Select the software plan (BYOL if you have a license or PAYG if not) and click **Create**
6. Populate the VM configuration



Create a virtual machine

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	GTP - Mark Renoden
Resource group *	fortinetRG Create new

Instance details

Virtual machine name *	mrs-FortiGate ✓
Region *	(Asia Pacific) Australia East
Availability options	No infrastructure redundancy required
Image *	Fortinet FortiGate-VM (BYOL) Browse all public and private images
Azure Spot instance	○ Yes ● No
Size *	Standard_D2s_v3 - 2 vcpus, 8 GiB memory (US$91.25/month) Select size

Administrator account

Authentication type	○ SSH public key ● Password
Username *	markreno ✓
Password *	•••••••••••••••• ✓
Confirm password *	•••••••••••••••• ✓

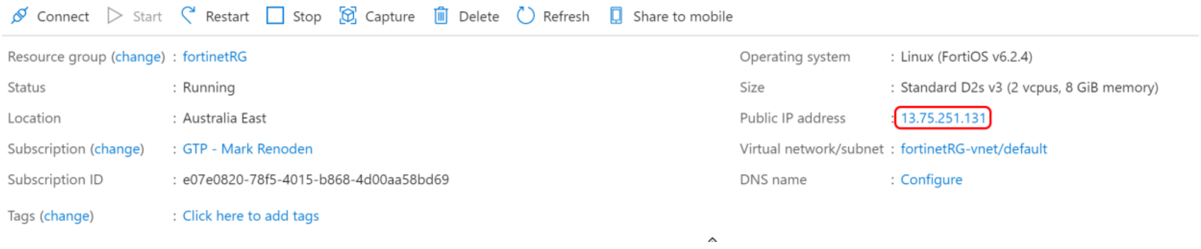
7. Set the Authentication type to **Password** and provide administrative credentials for the VM
8. Click **Review + Create**
9. Click **Create**
10. Wait for the VM deployment to complete

Set a Statuc Public IP Address and Assign a Fully Qualified Domain Name

For a consistent user experience, it is desirable to set the Public IP address assigned to the FortiGate VM to be statically assigned. In addition, mapping it to a fully qualified domain name is also useful for the same reasons.

Set a Static Public IP Address

1. Navigate to https://portal.azure.com and open the settings for the FortiGate VM
2. On the **Overview** screen, click on the public IP address



Resource group (change)	: fortinetRG	Operating system	: Linux (FortiOS v6.2.4)
Status	: Running	Size	: Standard D2s v3 (2 vcpus, 8 GiB memory)
Location	: Australia East	Public IP address	: 13.75.251.131
Subscription (change)	: GTP - Mark Renoden	Virtual network/subnet	: fortinetRG-vnet/default
Subscription ID	: e07e0820-78f5-4015-b868-4d00aa58bd69	DNS name	: Configure
Tags (change)	: Click here to add tags		

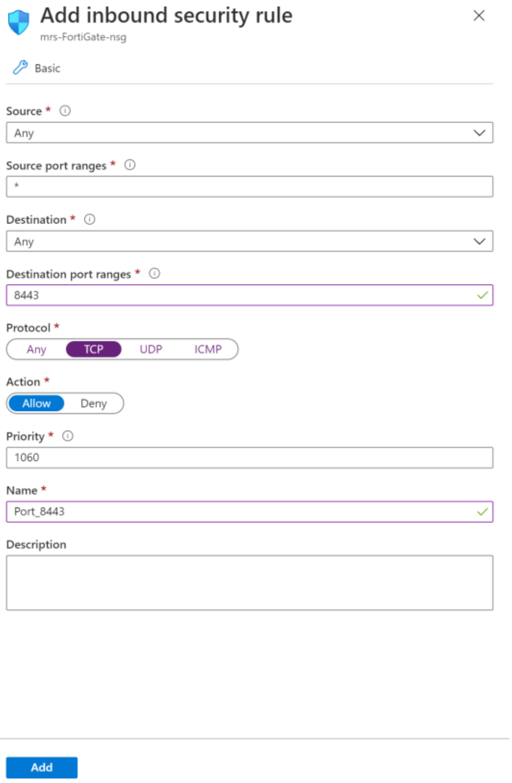
3. Click **Static** and then click **Save**

Assign a Fully Qualified Domain Name

If you own a publicly routable domain name for the environment into which the FortiGate VM is being deployed, create a Host (A) record for the VM that maps to the public IP address that is statically assigned above.

Create a New Inbound Network Security Group Rule for TCP port 8443

1. Navigate to https://portal.azure.com and open the settings for the FortiGate VM
2. Click on **Networking** in the left-hand menu. The network interface will be listed and the Inbound port rules displayed
3. Click **Add inbound port rule**
4. Create a new inbound port rule for TCP 8443



Add inbound security rule

mrs-FortiGate-nsg

Source * : Any

Source port ranges * : *

Destination * : Any

Destination port ranges * : 8443

Protocol * : Any [✓ TCP] UDP ICMP

Action * : [✓ Allow] Deny

Priority * : 1060

Name * : Port_8443

Description

5. Click **Add**

Create a Custom Azure App for FortiGate

1. Navigate to https://portal.azure.com and open the Azure Active Directory blade for the tenant that will provide Identity for FortiGate sign-ins
2. Click **Enterprise Applications** in the left-hand menu
3. Click **New Application**
4. Click **Non-gallery application**
5. Provide a name (e.g. FortiGate) and click **Add**
6. Click **Users and groups** in the left-hand menu
7. Add users who will be able to sign-in and click **Assign**
8. Click **Single sign-on** in the left-hand menu
9. Click **SAML**
10. Under **Basic SAML Configuration** click the pencil to edit the configuration
11. Configure
    - Identifier (Entity ID) to be https://<address>/remote/saml/metadata
    - Reply URL (Assertion Consumer Service URL) to be https://<address>/remote/saml/login
    - Logout URL to be https://<address>/remote/saml/logout

      Where <address> is the FQDN or the public IP address assigned to the FortiGate VM

      Record each of these URLs for later use –

      - Entity ID
      - Reply URL
      - Logout URL
12. Click **Save**
13. Close the Basic SAML Configuration
14. Under **3 – SAML Signing Certificate**, download the **Certificate (Base64)** and save it for later
15. Under **4 – Set up (App Name)**, copy the Azure Login URL, Azure AD Identifier and Azure Logout URL and save them for later
    - Azure Login URL
    - Azure AD Identifier
    - Azure Logout URL
16. Under **2 – User Attributes and Claims**, click the pencil to edit the configuration
17. Click **Add new claim**
18. Set the Name to **username**
19. Set the Source attribute to **user.userprincipalname**
20. Click **Save**
21. Click **Add a group claim**
22. Select **All groups**
23. Check **Customize the name of the group claim**
24. Set the Name to **group**
25. Click **Save**

Prepare for Group Matching

FortiGate allows for different user portal experiences after sign-in based on group membership. For example, there may be one experience for the Marketing group and another for the Finance group.

Configure this as follows –

Create Groups for Users

1. Navigate to https://portal.azure.com and open the Azure Active Directory blade for the tenant that will provide Identity for FortiGate sign-ins
2. Click **Groups**
3. Click **New Group**
4. Create a group with
   - Group type = Security
   - Group name = <a meaningful name>
   - Group description = <a meaningful description for the group>
   - Membership type = Assigned
   - Members = <users for the user experience that will map to this group>
5. Repeat steps 3 and 4 for any additional user experiences
6. After the groups have been created, select each group and record the Object Id for each one
7. Save these Object Ids and group names for later

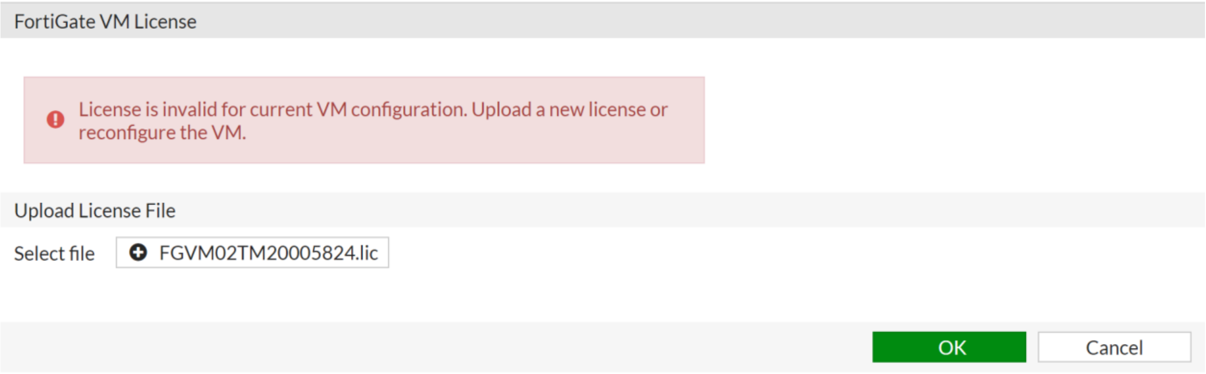
Configure the FortiGate VM

Install the License

1. Navigate to https://<address>

   here <address> is the FQDN or the public IP address assigned to the FortiGate VM

2. Continue past any certificate errors
3. Sign-in using the administrator credentials provided during the FortiGate VM deployment
4. If the deployment uses the BYOL model, a prompt to upload a license will be shown. Select the license file created earlier and upload it, click **OK** and restart the FortiGate VM –



FortiGate VM License

License is invalid for current VM configuration. Upload a new license or reconfigure the VM.

Upload License File

Select file: FGVM02TM20005824.lic

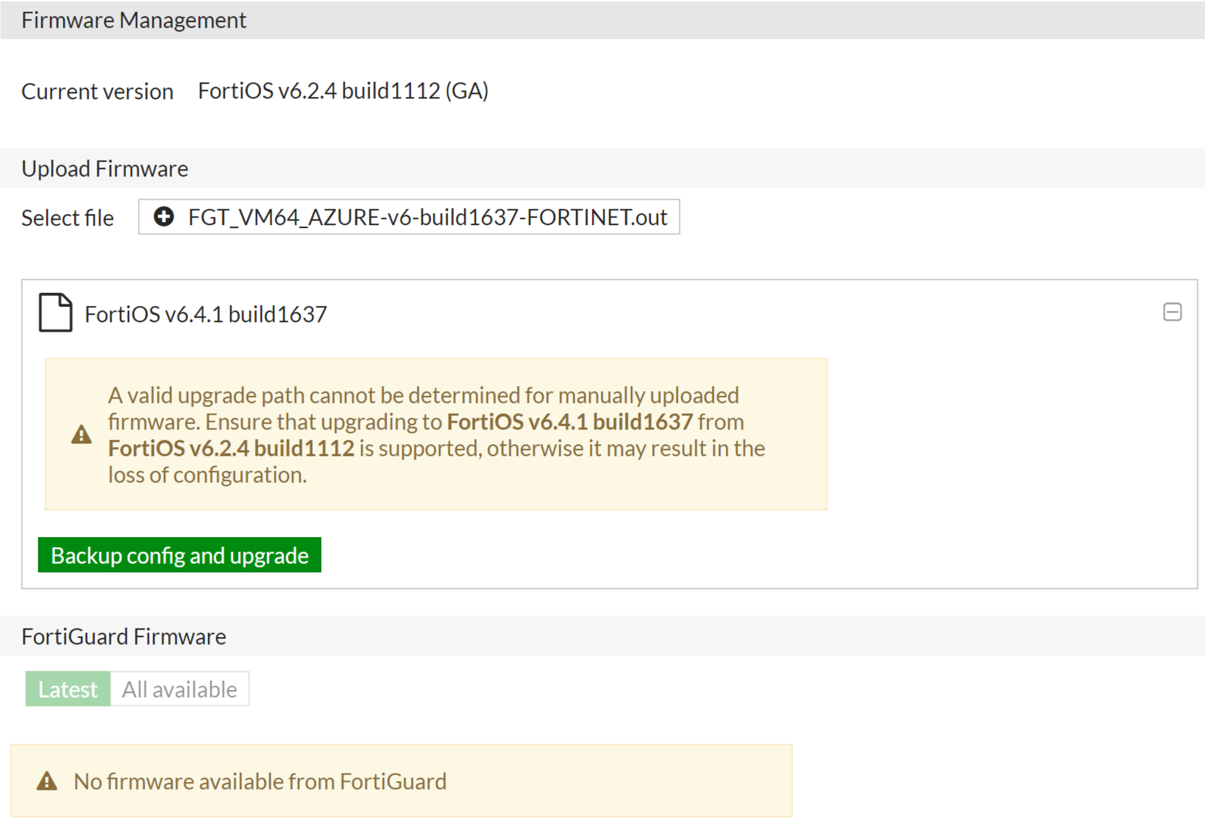
5. After the reboot, sign-in again with the administrator credentials to validate the license

Update Firmware

1. Navigate to https://<address>

   here <address> is the FQDN or the public IP address assigned to the FortiGate VM

2. Continue past any certificate errors
3. Sign-in using the administrator credentials provided during the FortiGate VM deployment
4. In the left-hand menu, click **System**
5. In the left-hand menu under System, click **Firmware**
6. In the Firmware Management page, click **Browse** and select the firmware file downloaded earlier
7. Ignore the warning and click **Backup config and upgrade** –



Firmware Management

Current version FortiOS v6.2.4 build1112 (GA)

Upload Firmware

Select file FGT_VM64_AZURE-v6-build1637-FORTINET.out

FortiOS v6.4.1 build1637

A valid upgrade path cannot be determined for manually uploaded firmware. Ensure that upgrading to **FortiOS v6.4.1 build1637** from **FortiOS v6.2.4 build1112** is supported, otherwise it may result in the loss of configuration.

Backup config and upgrade

FortiGuard Firmware

Latest All available

No firmware available from FortiGuard

8. Click **Continue**
9. When prompted to save the FortiGate configuration (as a .conf file), click **Save**
10. Wait for the firmware to upload, for it to be applied and for the FortiGate VM to reboot
11. After the FortiGate VM reboots, sign-in again with the administrator credentials
12. When prompted to perform Dashboard Setup, click **Later**
13. When the tutorial video begins, click **OK**

Change the Management Port to TCP 8443

1. Navigate to https://<address>

   here <address> is the FQDN or the public IP address assigned to the FortiGate VM

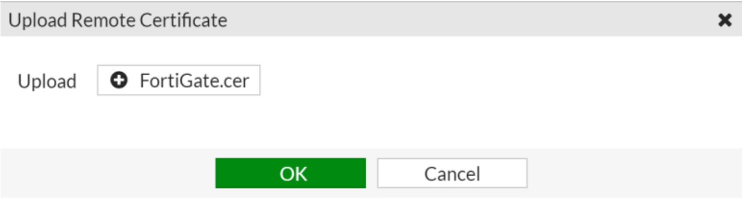
2. Continue past any certificate errors
3. Sign-in using the administrator credentials provided during the FortiGate VM deployment
4. In the left-hand menu, click **System**
5. Under Administration Settings, change the HTTPS port to **8443**
6. Click **Apply**
7. After the change applies, the browser will attempt to reload the Administration page but it will fail. From now on, the administration page address will be https://<address>:8443

Upload the Azure Active Directory SAML Signing Certificate

1. Navigate to https://<address>:8443

   here <address> is the FQDN or the public IP address assigned to the FortiGate VM

2. Continue past any certificate errors
3. Sign-in using the administrator credentials provided during the FortiGate VM deployment
4. In the left-hand menu, click **System**
5. Under System, click **Certificates**
6. Click **Import** -> **Remote Certificate**
7. Browse to the certificate downloaded from the FortiGate custom App deployment in the Azure tenant, select it and click **OK**


Upload Remote Certificate

Upload ⊕ FortiGate.cer

Upload and Configure a Custom SSL Certificate

You may wish to configure the FortiGate VM with your own SSL certificate that supports the FQDN you are using. If you have access to an SSL certificate packaged with the private key in .PFX format, it may be used for this purpose

1. Navigate to https://<address>:8443

   here <address> is the FQDN or the public IP address assigned to the FortiGate VM

2. Continue past any certificate errors
3. Sign-in using the administrator credentials provided during the FortiGate VM deployment
4. In the left-hand menu, click **System**
5. Under System, click **Certificates**
6. Click **Import** -> **Local Certificate**
7. Click **PKCS #12 Certificate**
8. Browse to the .PFX file containing the SSL Certificate and the Private Key
9. Provide the .PFX password
10. Provide a meaningful name for the Certificate
11. Click **OK**
12. In the left-hand menu, click **System**
13. Under System, click **Settings**
14. Under Administration Settings, expand the drop down next to HTTPS server certificate and select the SSL certificate imported above
15. Click **Apply**
16. Close the browser window and then navigate again to https://<address>:8443
17. Sign-in with the FortiGate administrator credentials and observe the correct SSL certificate in use

Perform Command Line Configuration

Perform Command Line Configuration for SAML Authentication

1. Navigate to https://portal.azure.com and open the settings for the FortiGate VM
2. In the left-hand menu, click on **Serial Console**
3. Sign-in at the Serial Console with the FortiGate VM administrator credentials

   For the next step, the URLs recorded earlier will be required. Namely –

   - Entity ID
   - Reply URL
   - Logout URL
   - Azure Login URL
   - Azure AD Identifier
   - Azure Logout URL

4. At the Serial Console, execute the following commands –

   ```
   config user saml
   edit azure
   set entity-id <Entity ID>
   set single-sign-on-url <Reply URL>
   set single-logout-url <Logout URL>
   set idp-single-sign-on-url <Azure Login URL>
   set idp-entity-id <Azure AD Identifier>
   set idp-single-logout-url <Azure Logout URL>
   set idp-cert REMOTE_Cert_1
   set user-name username
   set group-name group
   end
   ```

   NOTE: The Azure Logout URL contains a **?** character. This requires a special key sequence in order for it to be correctly provided to the FortiGate Serial Console. The URL is typically

   ```
   https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0
   ```

   To provide this in the Serial Console, proceed by typing

   ```
   set idp-single-logout-url https://login.microsoftonline.com/common/wsfederation
   ```

   Then type CTRL+V
   Then paste the rest of the URL in to complete the line

   ```
   set idp-single-logout-url
   https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0
   ```

5. To confirm the configuration, execute –

   ```
   show user saml
   ```

Perform Command Line Configuration for Group Matching

1. Navigate to https://portal.azure.com and open the settings for the FortiGate VM
2. In the left-hand menu, click on **Serial Console**
3. Sign-in at the Serial Console with the FortiGate VM administrator credentials
4. At the Serial Console, execute the following commands –

```
config user group
edit <group 1 name>
set member azure
config match
edit 1
set server-name azure
set group-name <group 1 Object Id>
next
end
next
```

Repeat these command from edit `<group 1 name>` but for each additional group that will have a different portal experience in FortiGate

```
end
```

Perform Command Line Configuration for Authentication Time Out

1. Navigate to https://portal.azure.com and open the settings for the FortiGate VM
2. In the left-hand menu, click on **Serial Console**
3. Sign-in at the Serial Console with the FortiGate VM administrator credentials
4. At the Serial Console, execute the following commands –

```
config system global
set remoteauthtimeout 60
end
```

Create VPN Portals and Firewall Policy

1. Navigate to https://<address>:8443

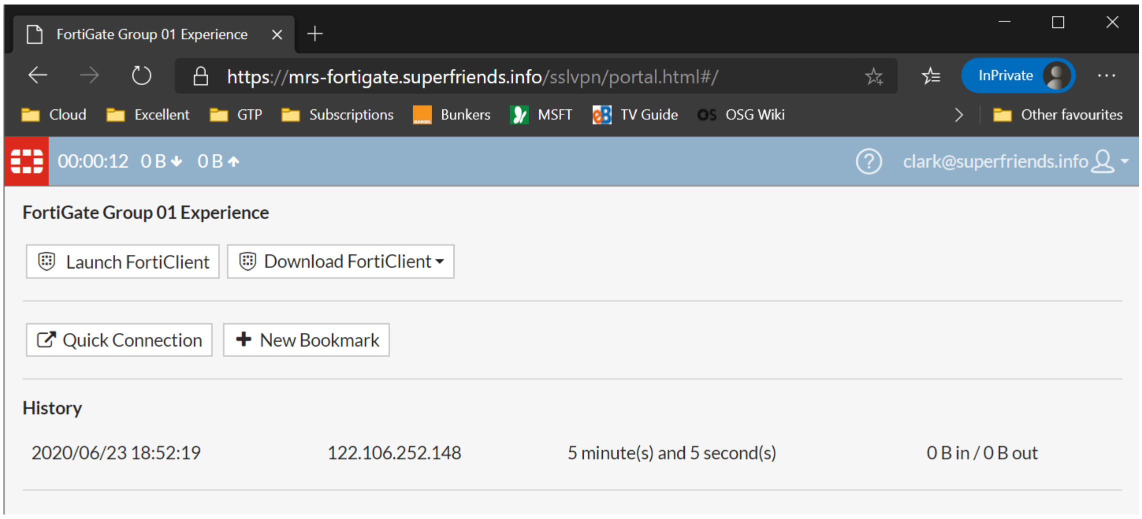
   here <address> is the FQDN or the public IP address assigned to the FortiGate VM

2. Sign-in using the administrator credentials provided during the FortiGate VM deployment
3. In the left-hand menu, click **VPN**
4. Under VPN, click **SSL-VPN Portals**
5. Click **Create New**
6. Provide a name (usually matching it to the Azure Group used to provide the custom portal experience)
7. Click the plus sign (**+**) next to Source IP Pools, select the default pool and click **Close**
8. Customize the experience for this group. For testing, this can be customization of the Portal Message and the Theme. This is also where you can create custom bookmarks that direct users to internal resources
9. Click **OK**
10. Repeat steps 5 to 9 for each Azure Group that will have a custom portal experience
11. Under VPN, click **SSL-VPN Settings**
12. Click the plus sign (**+**) next to Listen on Interfaces
13. Select **Port1** and click **Close**

14. If a custom SSL certificate was previously installed, change Server Certificate to use the custom SSL certificate in the drop-down menu
15. Under Authentication/Portal Mapping, click **Create New**
16. Choose the first Azure Group and match it with the Portal of the same name
17. Click **OK**
18. Repeat steps 15 to 17 for each Azure Group / Portal pair
19. Under Authentication/Portal Mapping, edit **All Other Users/Groups**
20. Set the portal to **full-access**
21. Click **OK**
22. Click **Apply**
23. Scroll to the top of the SSL-VPN Setting page and click on the warning **No SSL-VPN policies exist. Click here to create a new SSL-VPN policy using these settings**
24. Provide a name such as **VPN Grp1**
25. Set Outgoing Interface to **port1**
26. Click **Source**
27. Under Address, select **all**
28. Under User, select the first Azure Group
29. Click **Close**
30. Click **Destination**
31. Under Address, this would usually be the internal network. Select login.microsoft.com for testing
32. Click **Close**
33. Click **Service**
34. Click **All**
35. Click **Close**
36. Click **OK**
37. In the left-hand menu, click **Policy & Objects**
38. Under Policy & Objects, click **Firewall Policy**
39. Expand **SSL-VPN tunnel interface (ssl.root) -> port1**
40. Right-click the VPN policy created earlier (**VPN Grp1**) and select **Copy**
41. Right-click under the VPN policy and select **Paste** -> **Below**
42. Edit the new policy, providing it with a different name (say **VPN Grp2**) and changing the group is applies to (another Azure Group)
43. Right-click the new policy and set the status to **Enabled**

Test Sign-In Using Azure

1. Using an in-private browser session, navigate to https://<address>
2. The sign-in should redirect to Azure Active Directory for sign-in
3. After providing credentials for a user who has been assigned to the FortiGate App in the Azure tenant, the appropriate user portal should be shown



FortiGate Group 01 Experience

History

2020/06/23 18:52:19	122.106.252.148	5 minute(s) and 5 second(s)	0 B in / 0 B out