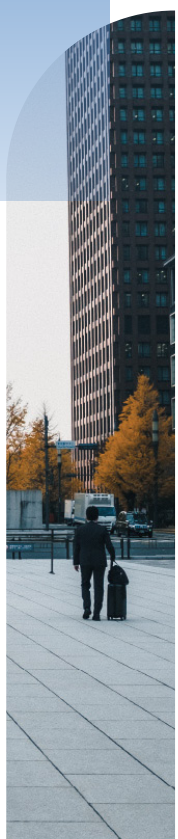
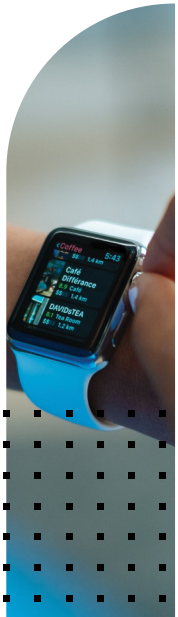
DEPLOYMENT GUIDE

Creating an Azure Connection for an MVE With Fortinet SD-WAN





You can create a network connection from an MVE (a FortiGate) to Azure ExpressRoute with virtual cross connects (VXCs). You can create either a private connection or a public(Microsoft) connection.

Important
Before you begin, create an MVE (FortiGate) in FortiManager. For details, see Creating an MVE [/mve/fortinet/creatingmve/].

FortiManager is an optional component and that FortiGate's can be deployed independently of FortiManager.

There are three parts to adding an ExpressRoute connection to your MVE and FortiManager.

1. Set up your ExpressRoute plan and deploy the ExpressRoute circuit in the Azure console. When deployed, you get a service key. For additional details, see the Microsoft ExpressRoute documentation [https://docs.microsoft.com/en-us/azure/expressroute/].
2. In the Megaport Portal, create a connection (VXC) from your MVE to your ExpressRoute location.
3. In FortiManager, create a new interface and add the details of the ExpressRoute connection.

The instructions in this topic step through the second and third parts.

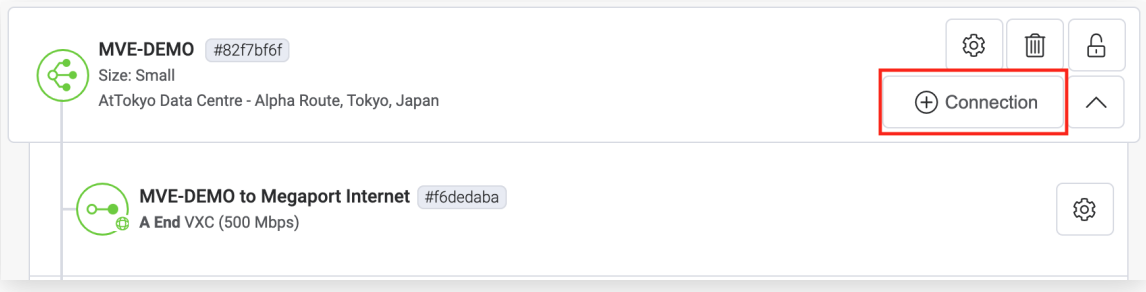
Note
MVE for Fortinet SD-WAN requires configuration steps in both FortiManager and the Megaport Portal for all cloud connections.

Adding the ExpressRoute Connection in the Megaport Portal

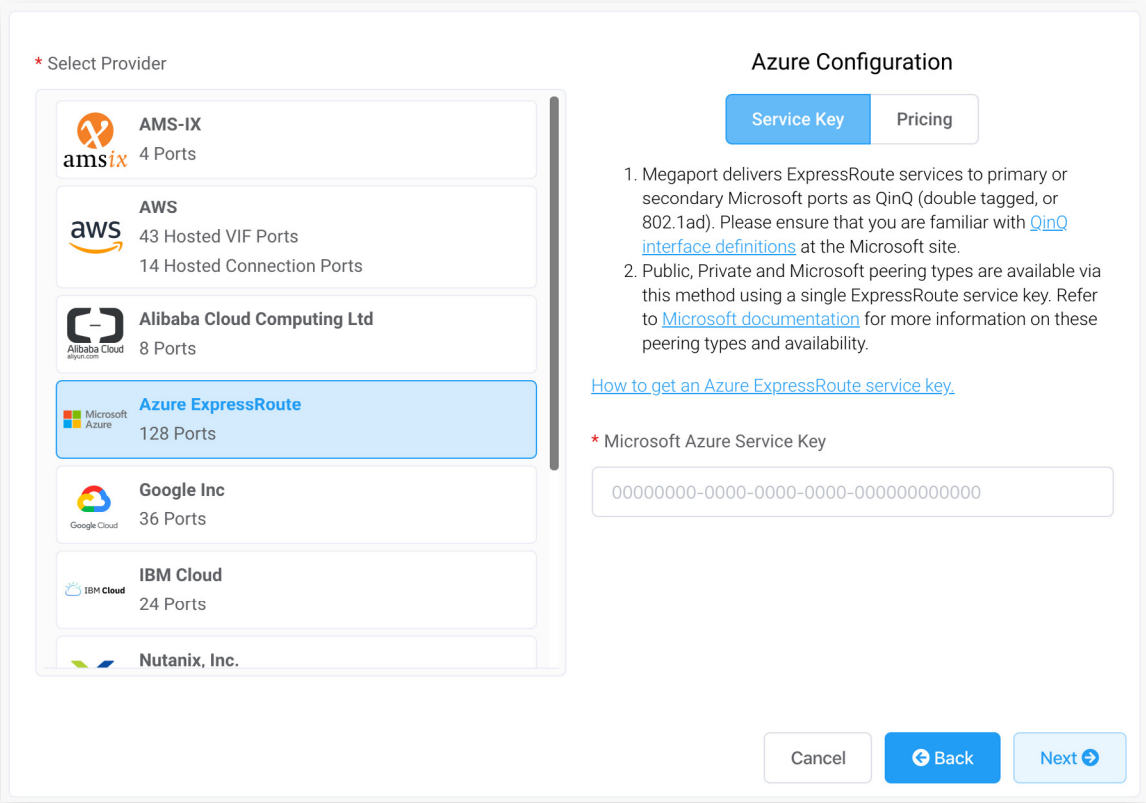
To set up the ExpressRoute connection, you need to create the connection in the Megaport Portal.

To create a connection to ExpressRoute from the Megaport Portal

1. In the Megaport Portal [https://portal.megaport.com], go to the **Services** page and select the MVE you want to use.
2. Click **+Connection** on the MVE.



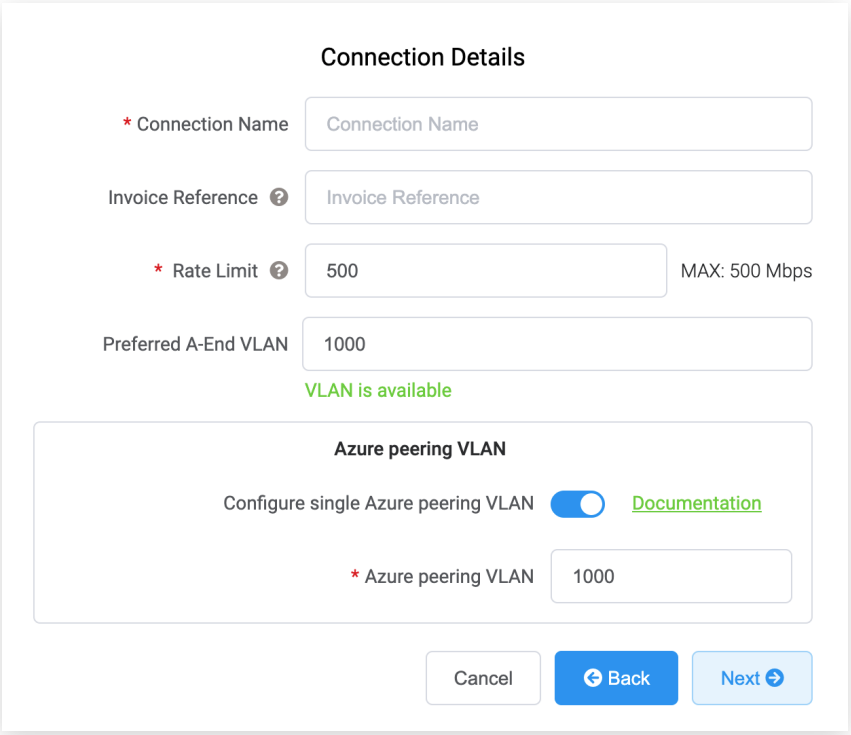
3. Click the Cloud tile.
4. Select Azure ExpressRoute as the provider.



5. Add the ExpressRoute service key into the field in the right-hand pane.
   The Portal verifies the key and then displays the available port locations based on the ExpressRoute region. For example, if your ExpressRoute service is deployed in the Australia East region in Sydney, you can select the Sydney targets.
6. Select the connection point for your first connection.
   To deploy a second connection (and this is recommended), you can create a second VXC—enter the same service key and select the other connection target.
   Some helpful links appear on the configuration screen to resources including the Azure Resource Manager console and some tutorial videos.
7. Specify these connection details:
   - **Connection Name** – The name of your VXC to be shown in the Megaport Portal.
   - **Invoice Reference** – This is an optional field. It can be any text, such as a PO number or billing reference number.
   - **Rate Limit** – This is the speed of your connection in Mbps. The rate limit for the VXC will be capped at the maximum allowable based on the ExpressRoute service key.
   - **Preferred A-End VLAN** – Optionally, specify an unused VLAN ID for this connection (for ExpressRoute this is the S-Tag). This must be a unique VLAN ID on this MVE and can range from 2 to 4093. If you specify a VLAN ID that is already in use, the system displays the next available VLAN number. The VLAN ID must be unique to proceed with the order. If you don't specify a value, Megaport will assign one.
   - **Configure Single Azure Peering VLAN** – By default, this option is enabled for MVE and we strongly recommend keeping it enabled with Fortinet SD-WAN. This option provides a single-tag VLAN solution. You configure peering in Azure with the MVE VLAN (A-End) and the peer VLAN set in Azure (B-End). Note, you can have only one peering type (Private or Microsoft) per VXC with this option.

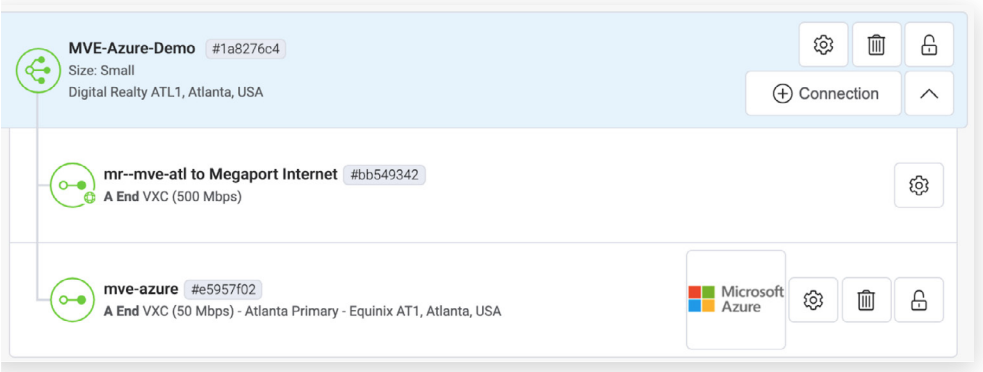
Important
If you do not enable this option, the VXC appears active but it does not recognize traffic.

- **Azure Peering VLAN** – This value needs to match the A-End VLAN.

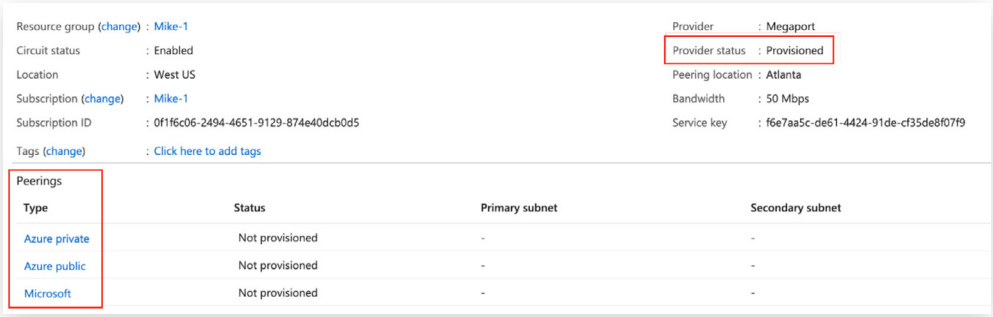


8. Click **Next** and proceed through the ordering process.

When the VXC configuration completes, the VXC icon is green.

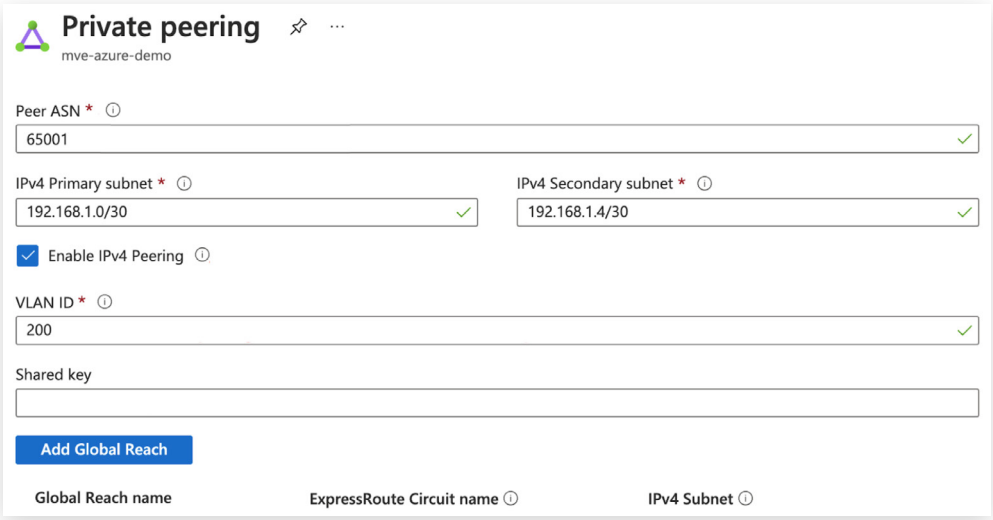


In the Azure Resource Management console, the provider status will be `Provisioned`.



When provisioned, you need to configure peerings. You can configure private and Microsoft peering. Click the peer to configure and provide these details:

- **Peer ASN** – Enter the ASN for the MVE.
- **IPv4 Subnets** – From each of these subnets, MVE uses the first usable IP address and Microsoft uses the second usable IP for its router.
- **VLAN ID** – Enter the A-End VLAN from the MVE. (Note, the VLAN ID in the Azure console can be different from the A-End VLAN.)
- **Shared Key** – Optionally, enter an MD5 password for BGP.



Adding the ExpressRoute Connection to FortiManager

After you create the connection from your MVE to Azure and set up the connection in the Azure console, you need to configure it in FortiManager. This involves creating an interface and configuring BGP settings, ASNs, VLANs, and MD5 values.

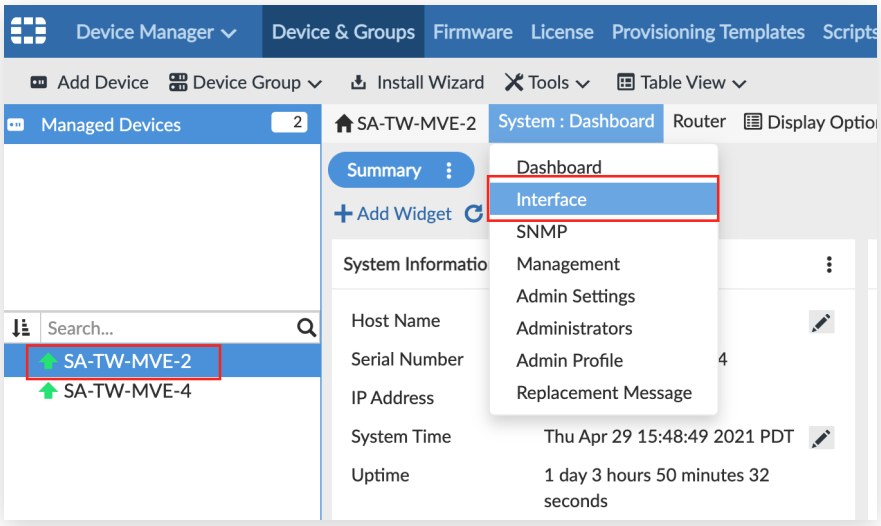
To add the Azure Cloud connection in FortiManager

1. Collect the connection details from the Azure console.
   Display the details of the connection you created in Azure for this connection. Note the values for the **Peer ASN, Shared Key, VLAN ID,** and **IPv4 Primary Subnet.**

2. Collect the connection details from the Megaport Portal.
   Click the gear icon for the Azure connection from your MVE and click the Details view. Note the value for the **A-End VLAN.**
3. Log in to the FortiManager.

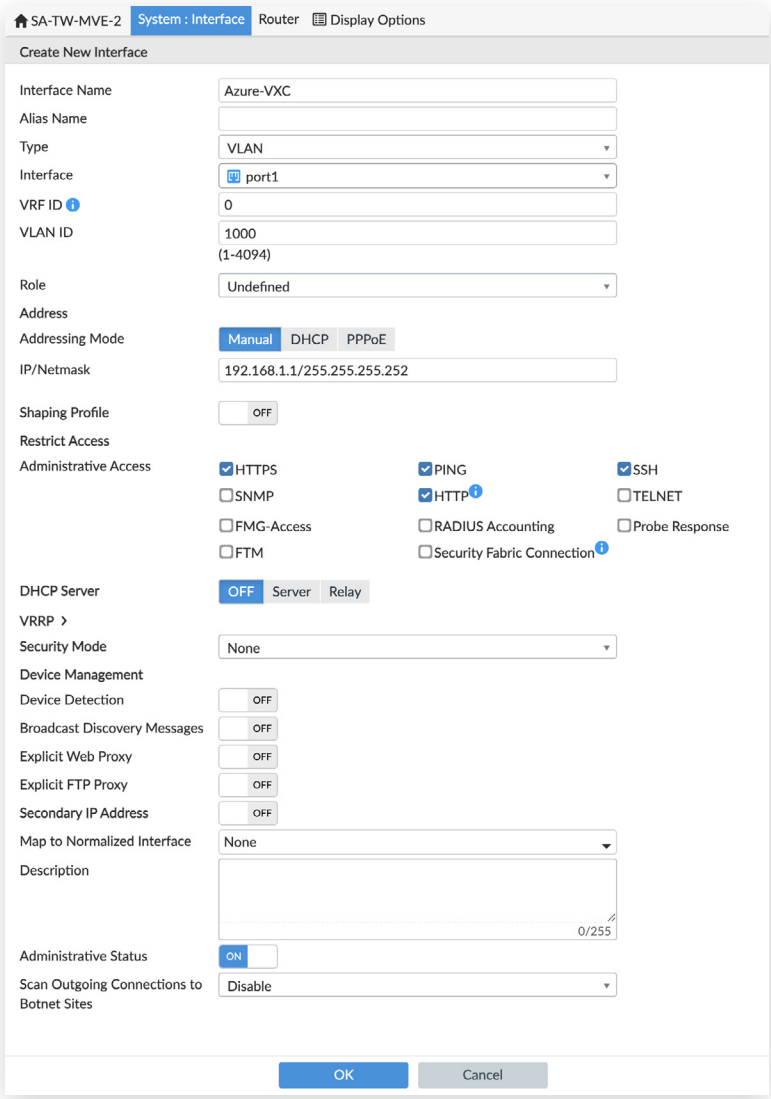
> **Note**
> You can also log in on your MVE instance: https://<mve-ip-address>.

4. From your managed device, go to the **System** menu and choose **Interface.**



The page displays `port1` as your physical interface.

5. Click **+Create New > Interface** and provide this information:
   - **Interface Name** – Specify a meaningful name for the interface.
   - **Alias Name** – Optionally, provide an alternate name.
   - **Type** – Choose VLAN.
   - **Interface** – Choose the parent interface: `port1`.
   - **VLAN ID** – Specify the A-End VLAN listed for this Azure Connection in the Megaport Portal.
   - **Role** – Choose Undefined.
   - **Addressing Mode** – Select Manual.
   - **IP/Netmask** – These values are available in the Azure console. The IP addresses and CIDR appear in the IPv4 Primary Subnet field; MVE uses the first usable IP address and Azure uses the second usable IP for its router. For this field, enter the MVE (first usable) IP address.
   - **Administrative Access** – Specify how you want to access this interface, such as HTTPS, PING, and SSH.
   - **DHCP Server** – Click **OFF.**



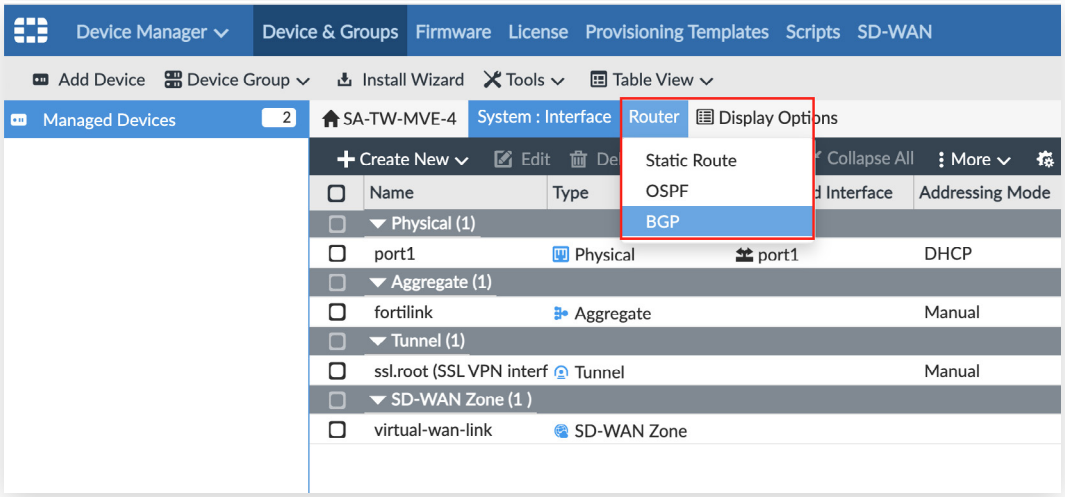
6. Click **OK.**
   The new VLAN interface appears with your `port1` physical interface.

You can run an `execute ping` command from FortiOS to verify the connection.

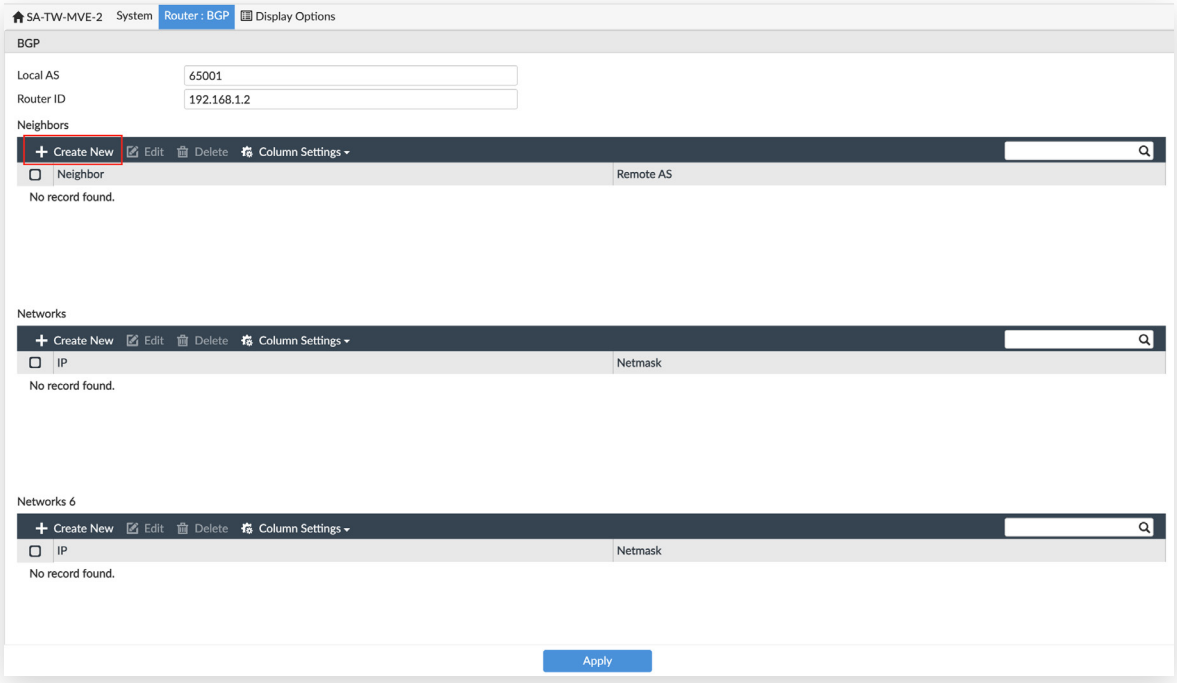
Note
You need to push the configuration to the MVE, which happens when you have AutoUpdate configured. If you cannot successfully ping the connection, go to Manage Devices in FortiManager, select the MVE, and choose **Refresh Device** from the More menu. If prompted, select AutoUpdate for the **Config Status.**

At this point, we have created the interface and next we need to create the BGP session.

1. In FortiManager, go to **Router > BGP.**



2. Provide this information:
   - **Local AS** – Provide the ASN for the MVE connection. Use the **Peer ASN** from the Azure console.
   - **Router ID** – Enter the first usable IP address from the **IPv4 Primary Subnet** from the Azure console.



3. In Neighbors, click **+Create New.**
4. For the neighbor **IP**, add the second usable IP address from the **IPv4 Primary Subnet** from the Azure console.
5. For **Remote ASN**, enter the Azure-side ASN of 12076.
   This is a fixed value, and appears in the connection details on the Azure console.

6. Click **OK.**
7. Click **Apply.**
   The neighbor is configured but we need to add the BGP Auth information if you defined this in the Azure console. (This was optional.) The web interface does not let you define this and you need to use the command line to add the BGP details.
8. SSH to the MVE instance using your private key file.
   For example:
   `ssh -i ~/.ssh/megaport-mve-instance-1-2048 admin@162.43.143.XX`
9. Use these commands to add a password for the BGP neighbor.

```
config router bgp
    config neighbor
        edit "<neighbor ip>"
            set password <auth password>
        next
    end
```

Validating Your Azure Connection

You can review connection details, including the connection state, from the CLI with these commands:

- `get system interface` – Displays configuration details and current status for the device interfaces.
- `get router info bgp neighbor` <ip-address> – Displays configuration details and current status for the BGP neighbors.

September 28, 2021 12:16 AM

1243501-0-0-EN