Deploying HPE Aruba Networking EdgeConnect Enterprise in Azure Virtual WAN

Deployment Guide

Contents

Document revision history

Project name: Deploying HPE Aruba Networking EdgeConnect Enterprise in Azure Virtual WAN

Document status: Revision B

Date	Document Version	Revisions Made
June 25, 2025	Rev B	Added Create a customer role and assign a user-assigned managed identity, other minor updates.
September 2022	Rev A	Initial document revision.

Prerequisites

- A current Azure account with an Azure Virtual WAN already created. If this is not created, you must create one prior to beginning the EC-V NVA deployment.
- An Azure Virtual Hub created in the Azure region where you want to deploy the EC-V. If this is not created, you must create one prior to beginning the EC-V NVA deployment.
- Access to Aruba EdgeConnect Orchestrator.
- Aruba EdgeConnect Enterprise Account Name and License Key.
- Aruba EdgeConnect Enterprise Appliance Bandwidth Licenses.

Create a customer role and assign a user-assigned managed identity

Deploying EdgeConnect SD-WAN instances within a Virtual WAN Hub requires the following permissions:

```
"Microsoft.Resources/subscriptions/providers/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Network/virtualHubs/read",

"Microsoft.Network/networkVirtualAppliances/delete",

"Microsoft.Network/networkVirtualAppliances/read",

"Microsoft.Network/networkVirtualAppliances/write"
```

Creating a custom role in Azure with the above permissions and assigning it to a user-assigned managed identity, scoped to the resource group where the virtual WAN hub and NVA will be deployed, ensures a secure and controlled deployment of EdgeConnect SD-WAN instances within a virtual WAN hub. It is important that the user-assigned managed identity has READ permissions over the virtual WAN hub you are deploying the EdgeConnect gateway into. If not, you will see an error message such as:

```
Caller does not have access on one or more referenced resource(s). Details: The client with object id
'<>' does not have authorization to perform action 'Microsoft.Network/virtualHubs/read' over scope
'/subscriptions/<>/resourceGroups/<>/providers/Microsoft.Network/virtualHubs/<>
```

Below are the instructions to create a custom role and assign it to a user-assigned managed identity.

Create a custom role

Follow the instructions on this Microsoft page to create a custom role on Azure Portal and assign the above permissions to it: https://learn.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#start-from-scratch

Create a user-assigned managed identity

Follow the instructions on this Microsoft page to create a user-assigned managed identity: https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/how-manage-user-assigned-managed-identities?pivots=identity-mi-methods-azp#create-a-user-assigned-managed-identity

Associate the custom role with the user-assigned managed identity

Associate the custom role with the user-assigned managed identity, as shown in Figure 1:

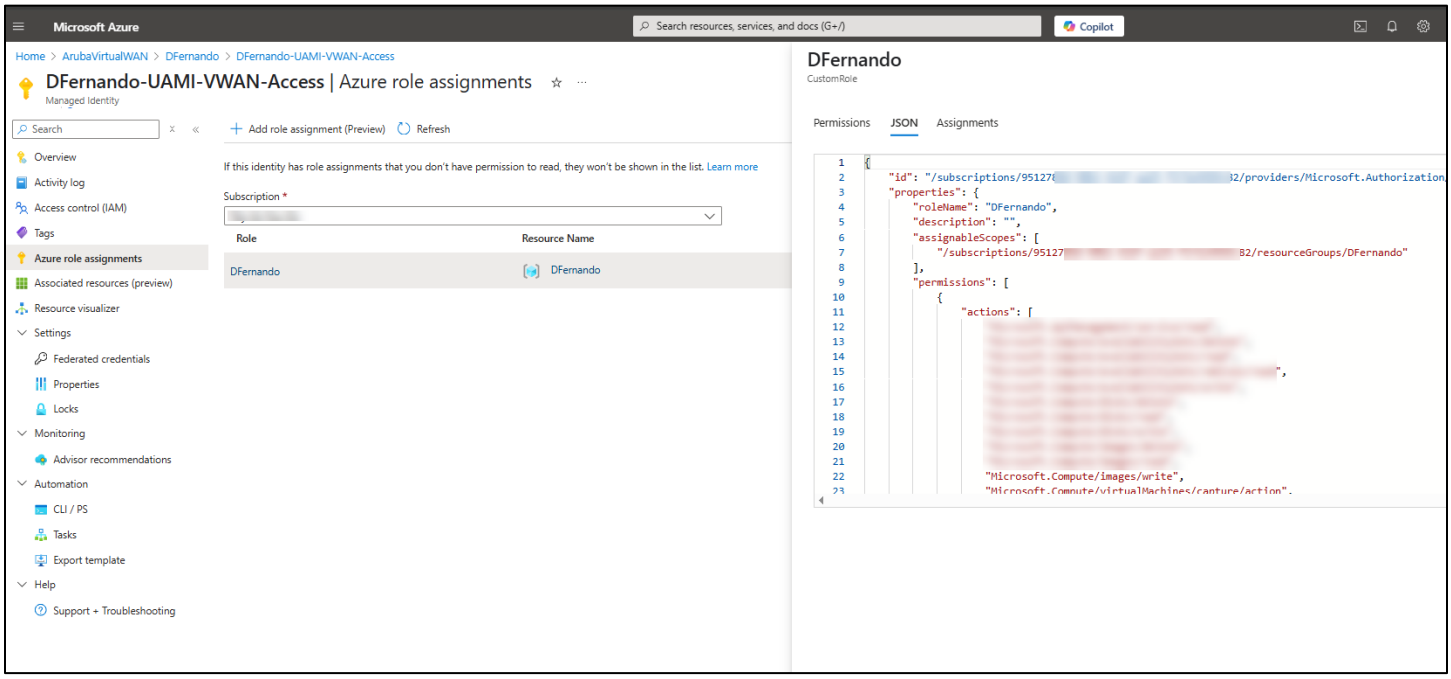

Figure 1. Associating the custom role with the user-assigned managed identity.

Deploy EC-V

Basics tab

1. Search the Marketplace for “EdgeConnect Enterprise” and choose **Aruba EdgeConnect Enterprise for Azure Virtual WAN**.
2. Select the **Aruba EdgeConnect Enterprise in Azure Virtual WAN** tile.
3. Click **Create**. The Create Aruba EdgeConnect Enterprise in Azure Virtual WAN page opens, as shown in Figure 2.

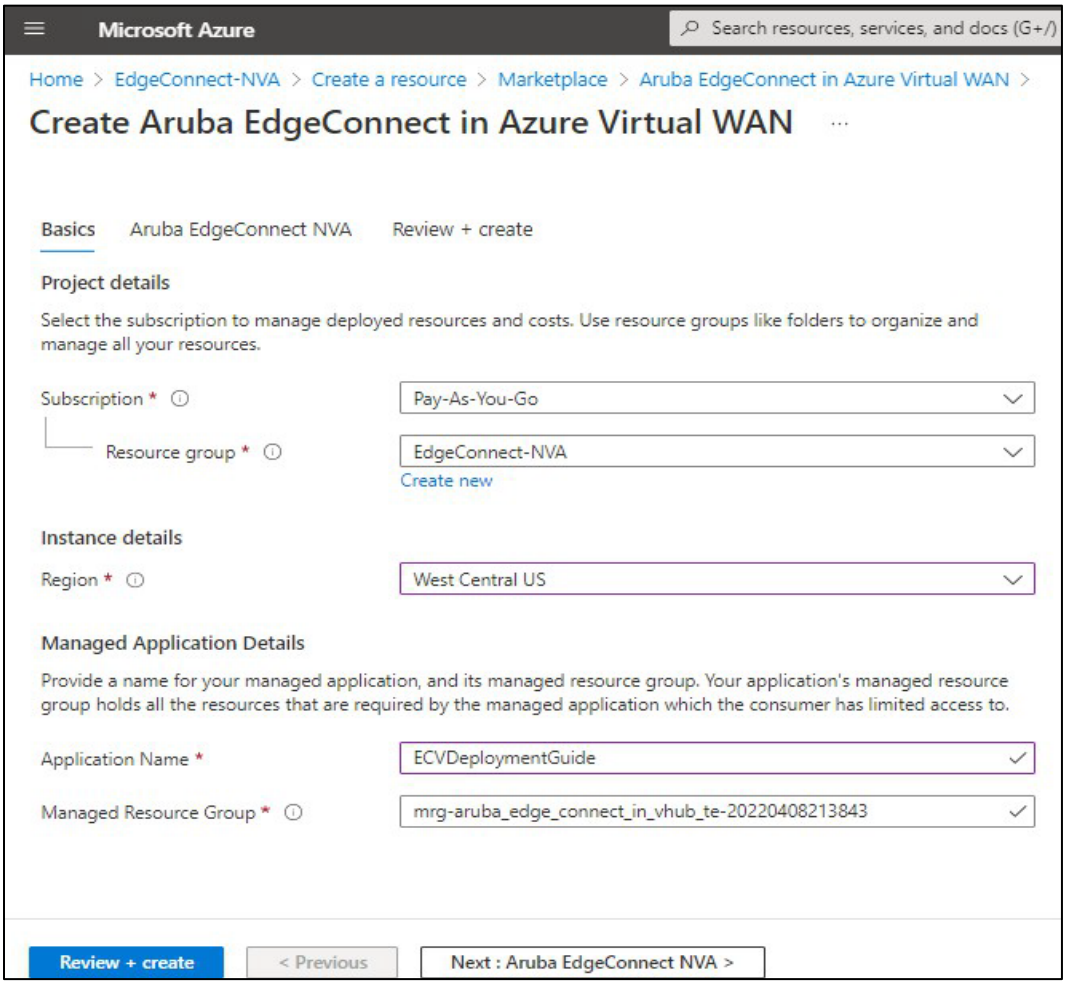

Figure 2. The Create Aruba EdgeConnect Enterprise in Azure Virtual WAN Review + create page.

4. Select the **Subscription**.
5. Select the **Resource group**.
6. Select the **Region** where you have created the Azure Virtual Hub.
7. Enter an **Application Name**.

Note

The Application Name can only contain letters and numbers and be between 3 and 32 characters.

---

8. **Do NOT** modify the content of the Managed Resource Group field.
9. Click **Next : Aruba EdgeConnect NVA >**.

HPE Aruba Networking EdgeConnect Enterprise NVA tab

1. Enter a **Deployment Name**. This must be a unique name. This is the name that appears on the Network Virtual Appliances page on the Azure Portal. The name can contain letters, numbers, and dashes, and must be between 3 and 32 characters.
2. Click **+Add**, and then select the user-assigned managed identity you created earlier. This is a mandatory step.

3. Select the **Virtual WAN Hub** to deploy the Aruba EdgeConnect Enterprise NVA.
   a. If no virtual WAN hubs are shown, the region you selected does not have any virtual WAN hubs created yet.
   b. After you select the virtual WAN hub, two separate tool tips appear at the bottom of the page. The first tool tip displays the Azure Virtual Hub's BGP endpoint IP addresses and the ASN that you must use when establishing BGP from the EC-V to the Azure Virtual Hub. Write down these IP addresses and the ASN.
   c. The second tool tip displays that you must create two static routes for establishing BGP sessions.
4. Select the **Scale Unit**. The Scale Unit determines the size and number of resources deployed for an EdgeConnect Enterprise deployment. The higher the Scale Unit, the greater the amount of traffic that can be handled.
5. Enter the **EdgeConnect Enterprise's ASN**. Enter any BGP ASN between 64512 and 65534, excluding 65515, 65517, 65518, 65519, and 65520.

Note

The Azure Virtual Hub only supports 16-bit ASNs. As a result, do not enter a 32-bit ASN on the EdgeConnect Enterprise.

---

6. Enter the **EdgeConnect Enterprise Account Name**. This can be found on the Orchestrator under Cloud Portal.
7. Enter the **EdgeConnect Enterprise Account Key**. This can be found on the Orchestrator under Cloud Portal.
8. *(Optional)* Enter the **EdgeConnect Enterprise Tag**.
9. Enter a **single-line SSH key** for the EdgeConnect Enterprise.

Note

Do NOT enter a multi-line SSH key. Multi-line SSH keys typically start with the text **"**`-----BEGIN SSH2 PUBLIC KEY`**"**

---

10. Click **Next : Review + create**. Note the Virtual WAN Hub BGP Endpoints and ASN displayed below. You will need this information in a future step in this guide.

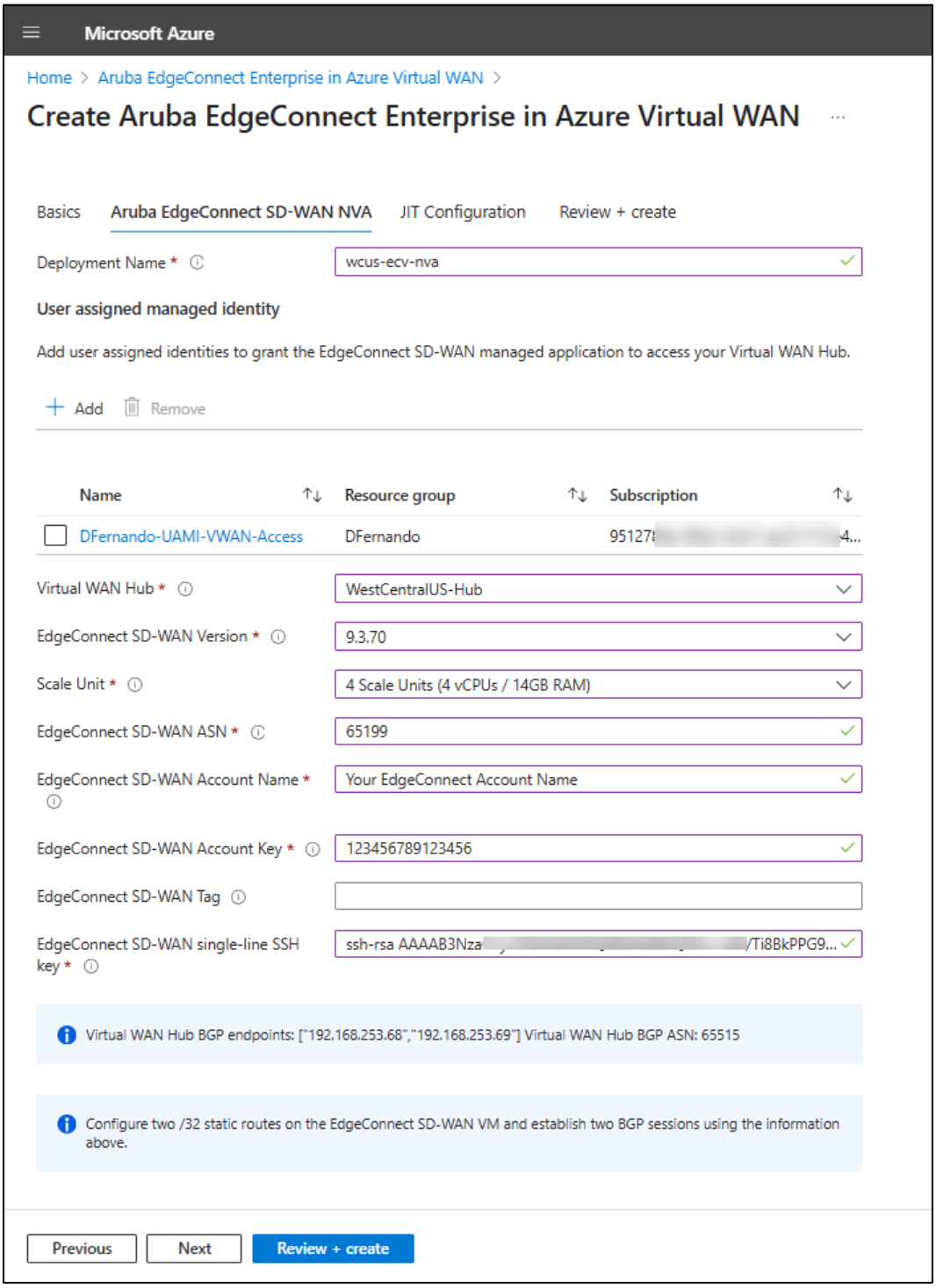

Figure 3. The Create Aruba EdgeConnect Enterprise in Azure Virtual WAN page.

Review + create tab

1. Review the settings you have entered.
2. Select the **I agree to the terms and conditions above** checkbox.
3. Refer to Figure 4 for an example of what the screen should look like.

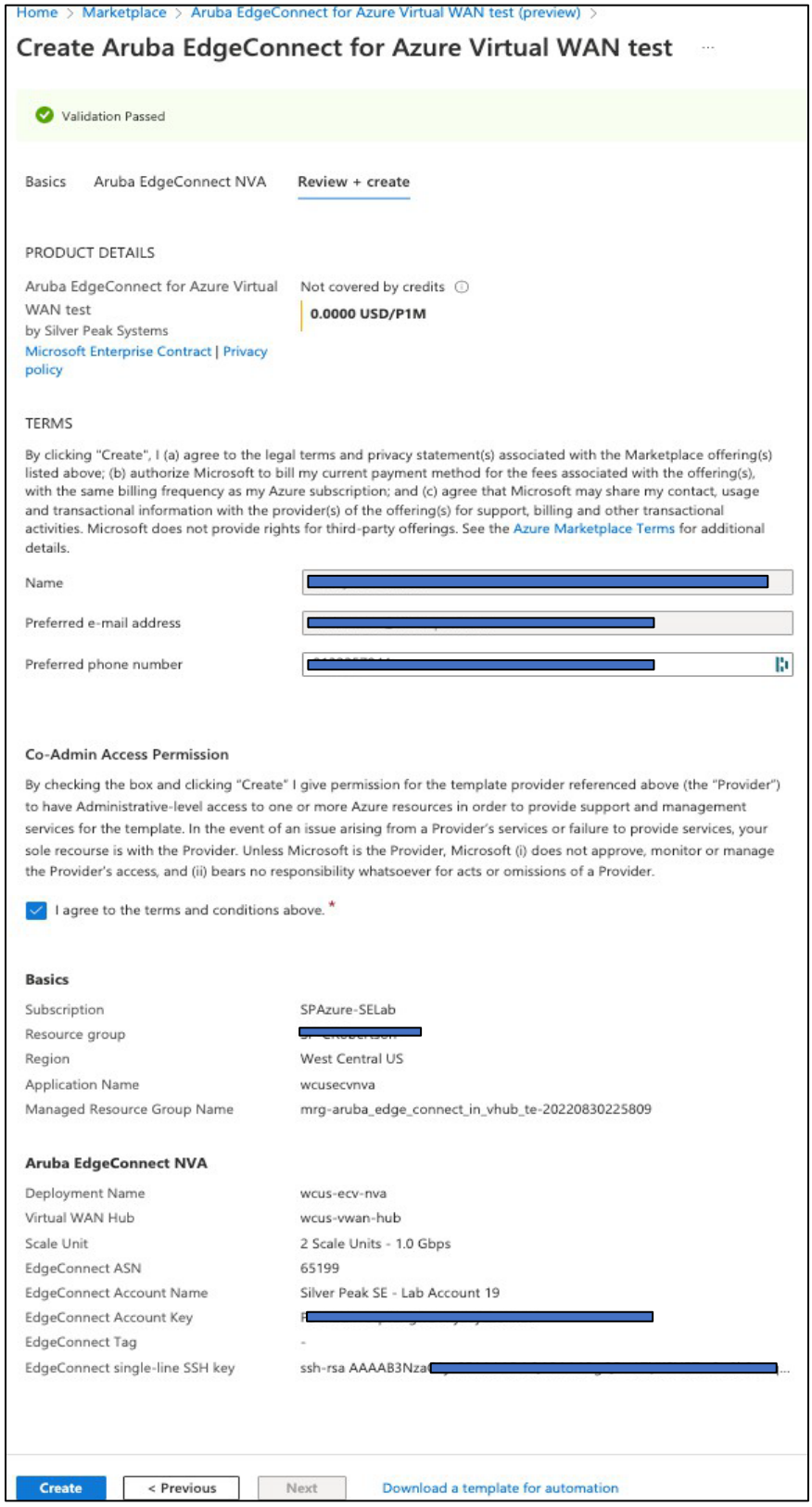

Figure 4. The Create Aruba EdgeConnect for Azure Virtual WAN test page.

4. Click **Create**. The EC-V deployment begins.

Correlate EC-Vs

Within approximately five minutes of the deployment, the two, new EC-Vs will appear on your Orchestrator as shown in Figure 5.

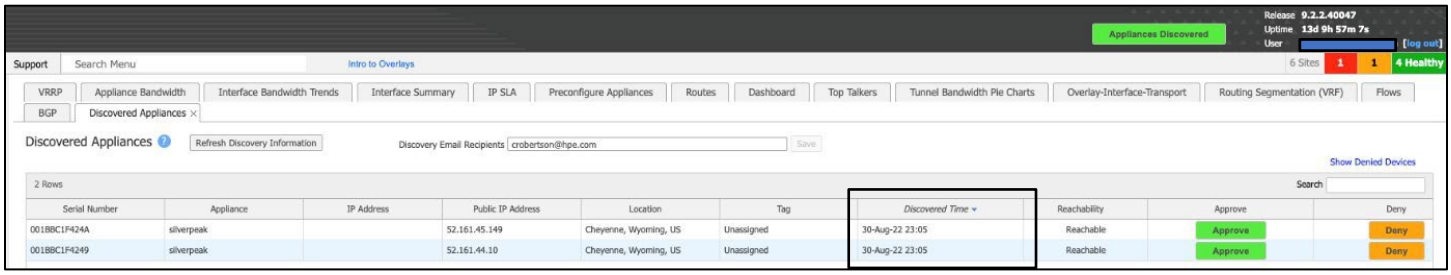

Figure 5. EC-Vs in SD-WAN Orchestrator.

- If you deployed the EC-Vs in a region where Azure supports Availability Zones, each EC-V will be deployed in a unique Availability Zone.
- If you deployed the EC-Vs in a region where Azure does not support Availability Zones, each EC-V will be deployed in an Availability Set.
- As shown in Figure 3 above, the Discovered Time column on the Discovered Devices page shows that both EC-Vs got deployed at the same time (23:05 August 30, 2022).

However, Azure always numbers each EC-V according to the order it deploys them. To find this order, perform the following tasks. The objective here is to ensure that order is preserved when you are adding the EC-Vs to the SD-WAN fabric. You want to approve the first EC-V (that Azure deployed) first followed by the second EC-V:

1. Go to the **Azure Virtual WAN Hub** that you deployed the EC-Vs.
2. Click **Network Virtual Appliance** under Third party providers.
3. Under Instances info column, click the **Click here** link under your deployment.

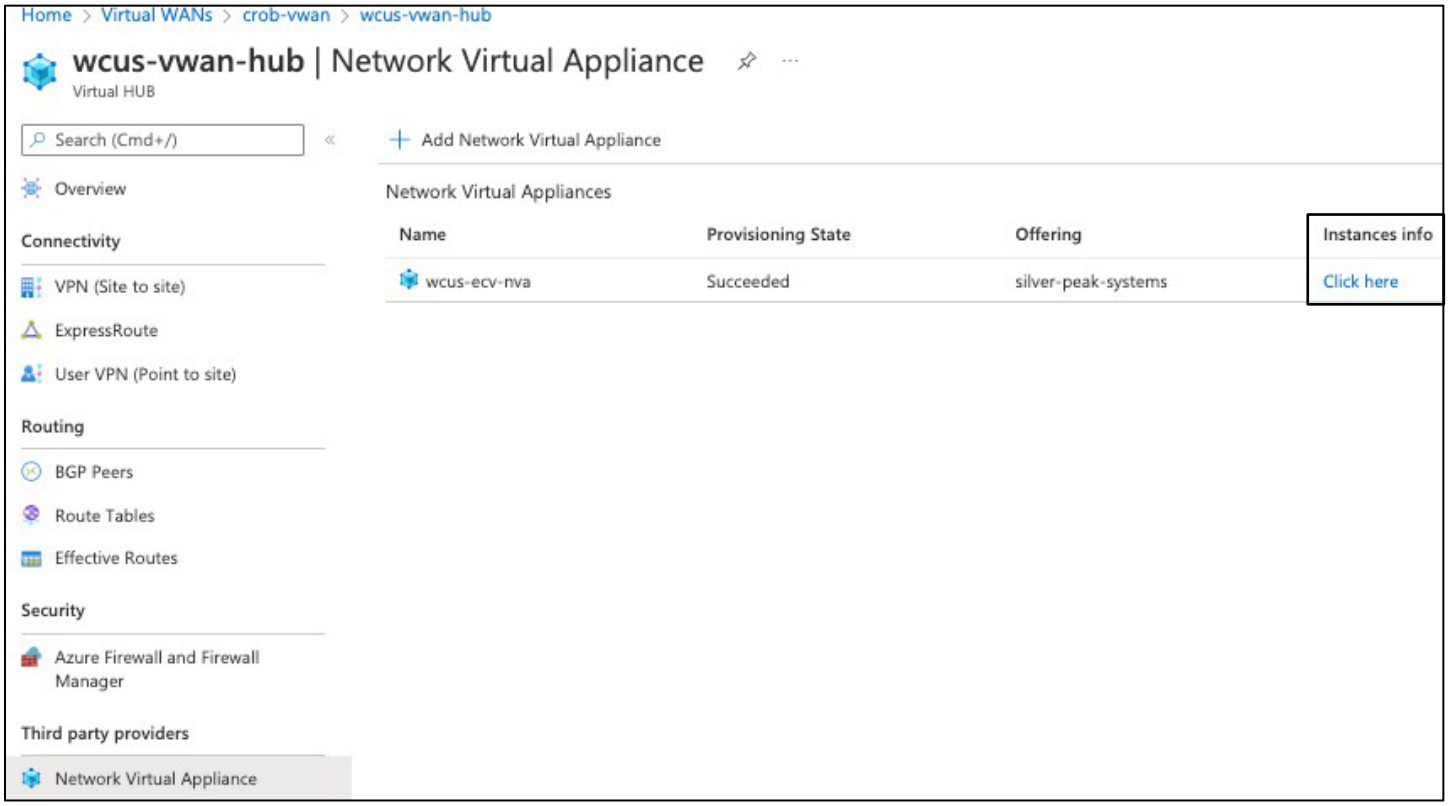

Figure 6. The Network Virtual Appliance page.

Note

If you encounter a message that says “You haven't created a network virtual appliance for this virtual hub yet” the appliances are likely still initializing. If after some time (10-15 minutes) you still do not see the NVA listed, go to the Orchestrator, click **Approve**, and then upgrade the appliances to your desired version as depicted in Figure 7 below. After the appliances are rebooted, you will see them in the Azure dashboard.

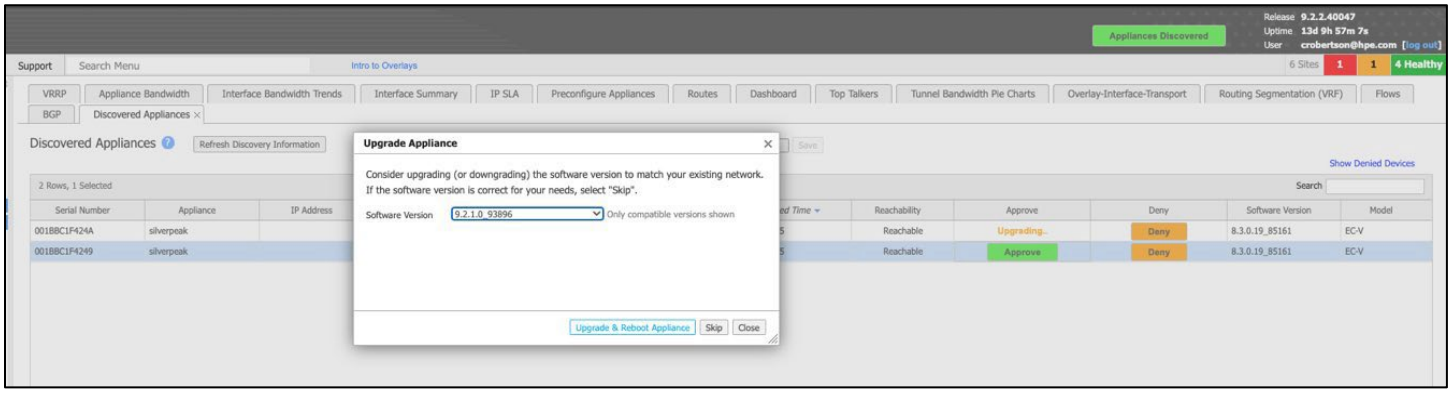

Figure 7. The Upgrade Appliance dialog box.

4. A window opens that shows the IP addresses of each EC-V in the deployment. Under the NVA instance name, “0” denotes the first EC-V and “1” denotes the second EC-V as shown in Figure 6.

Notes

- Azure only assigns one public IP address per EC-V. This public IP address is assigned to the WAN0 interface.
- Each subnet is created as a /28 by Azure, this is not modifiable. The gateway address is always the first useable IP of the assigned subnet.

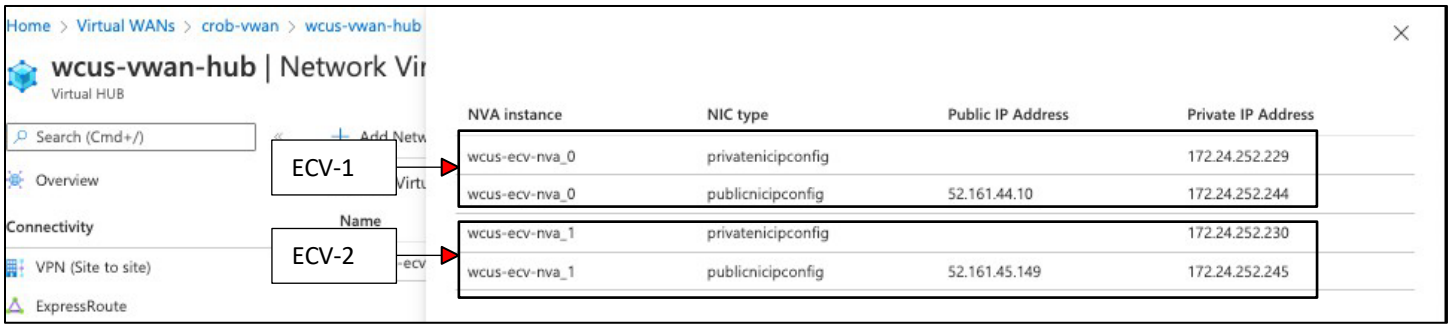

Figure 8. EC-Vs on the Network Virtual Appliance page.

- In ECV-1, the public IP address of the WAN0 interface is 52.161.44.10
- In ECV-1, the private IP address of the WAN0 interface is 172.24.252.244
  - The gateway IP address would be 172.24.252.241
- In ECV-1, the private IP address of the LAN0 interface is 172.24.252.229
  - The gateway IP address would be 172.24.252.225
- In EC-V-2, the public IP address of the WAN0 interface is 52.161.45.149
- In EC-V-2, the private IP address of the WAN0 interface is 172.24.252.245
  - The gateway IP address would be 172.24.252.241
- In EC-V-2, the private IP address of the LAN0 interface is 172.24.252.230
  - The gateway IP address would be 172.24.252.225

Note

Although Azure assigned the above IP addresses to the EC-Vs at the hypervisor-level, these IP addresses are not yet assigned at ECOS-level, i.e., the EC-V is still in Server Mode with no IP addresses or MAC addresses assigned yet.

In the upcoming sections of this guide, we cover how to find MAC addresses from the Azure Portal, assign MAC addresses, and change the deployment mode from Server to In-line Router Mode.

Add EC-Vs to the SD-WAN Fabric

1. Now that you are aware of IP addresses of each EC-V, find the public IP address of ECV-1. In the guide example, this IP address is 52.161.44.10.
2. Open the Discovered Devices page on the Orchestrator and find the same public IP address.

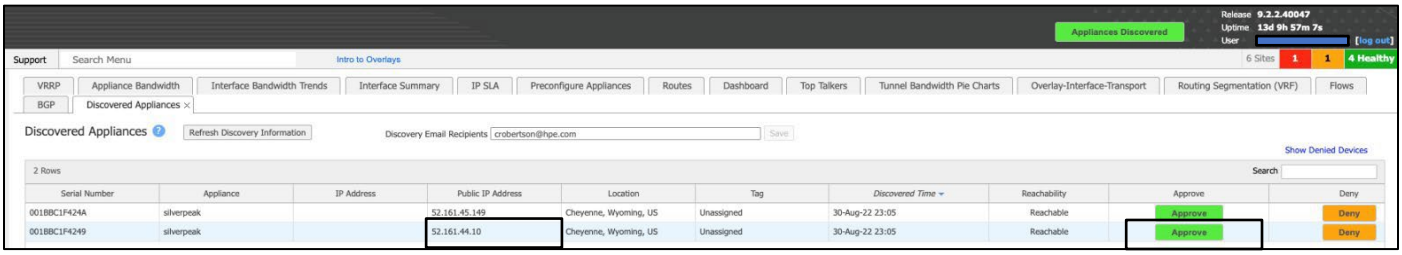

Figure 9. Discovered EC-Vs in SD-WAN Orchestrator.

3. Click **Approve** to start adding the EC-V to the SD-WAN fabric.
4. While adding the EC-Vs to the SD-WAN fabric:
   a. Upgrade the EC-V to your desired version (if not done previously), otherwise click **Skip**.

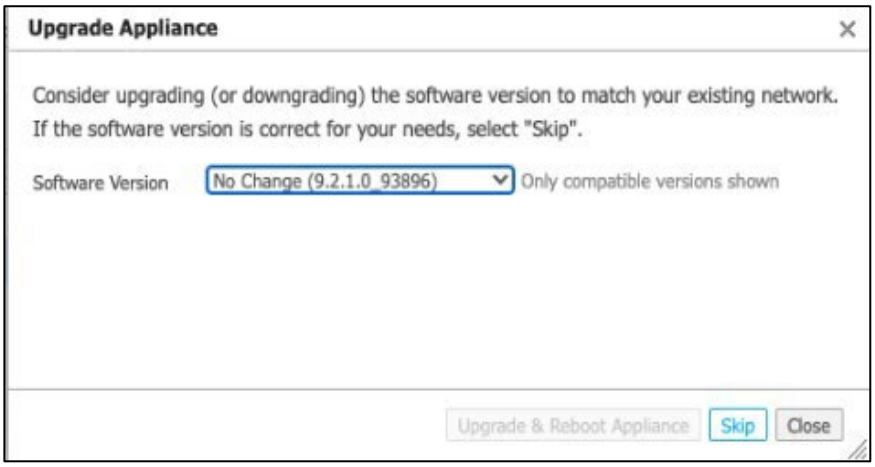

Figure 10. The Upgrade Appliance dialog box.

   b. On the Apply Appliance Preconfiguration screen, select **Run Manual Configuration Wizard**.

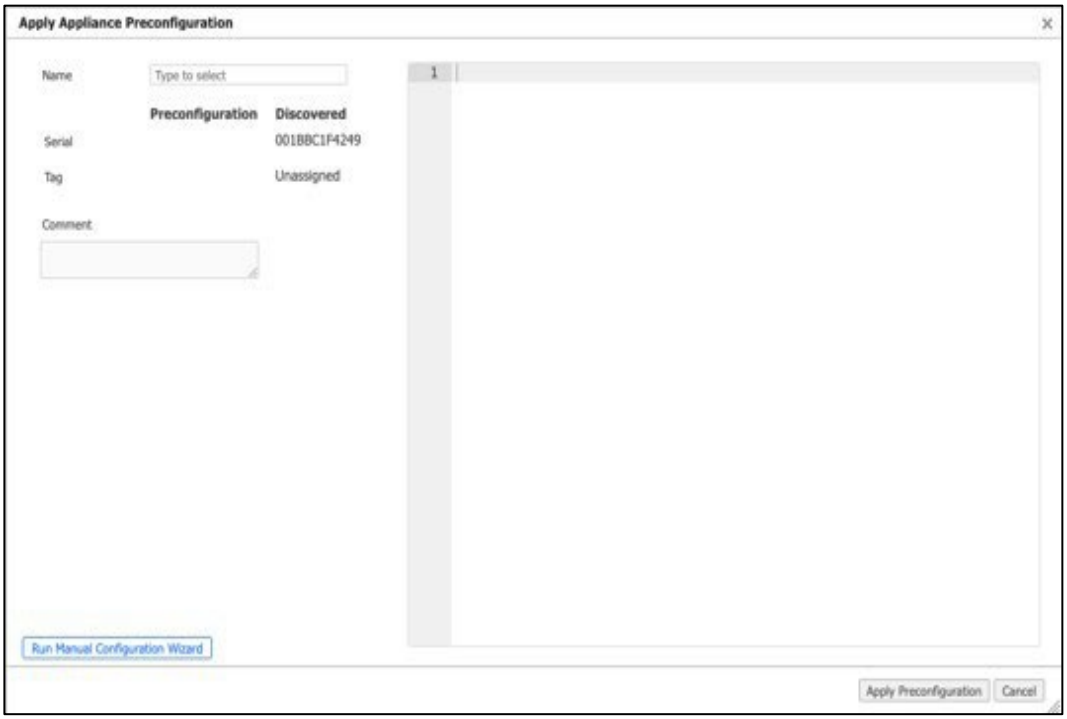

Figure 11. The Apply Appliance Preconfiguration page.

c. Configure the Hostname, Group, Admin Password, Location Information, and select the **Hub Site** check box if the NVA will act as a hub for SDWAN spokes.

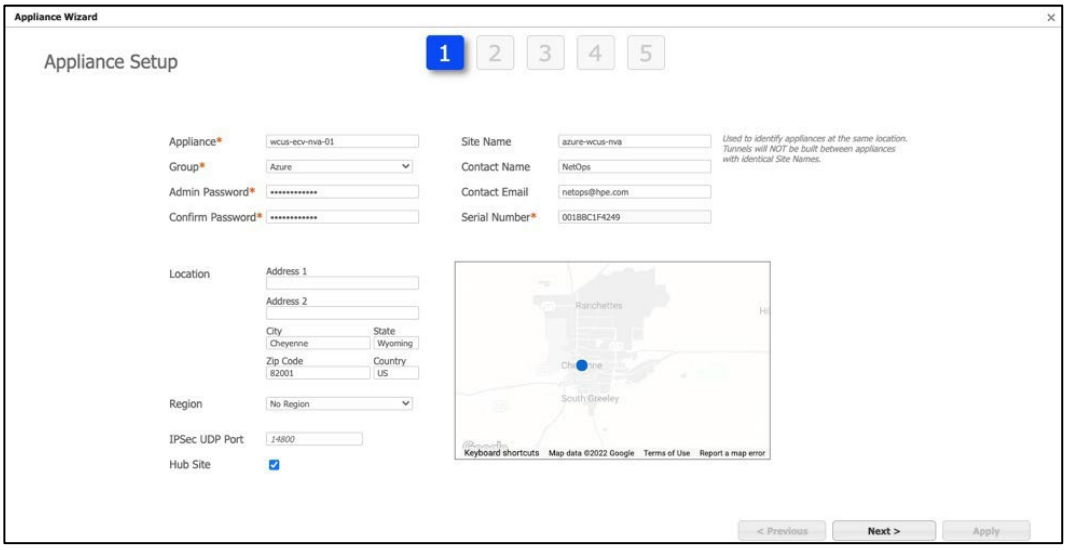

Figure 12. Page 1 of the Appliance Wizard.

Note

Ensure that you enter the same Site Name on both EC-Vs to prevent them from forming tunnels with each other.

d. **Do not change the deployment mode from Server to In-line Router Mode yet.** Click Next, do not make any changes on this screen. You will do this AFTER adding the EC-V to SD-WAN fabric and assigning MAC addresses.

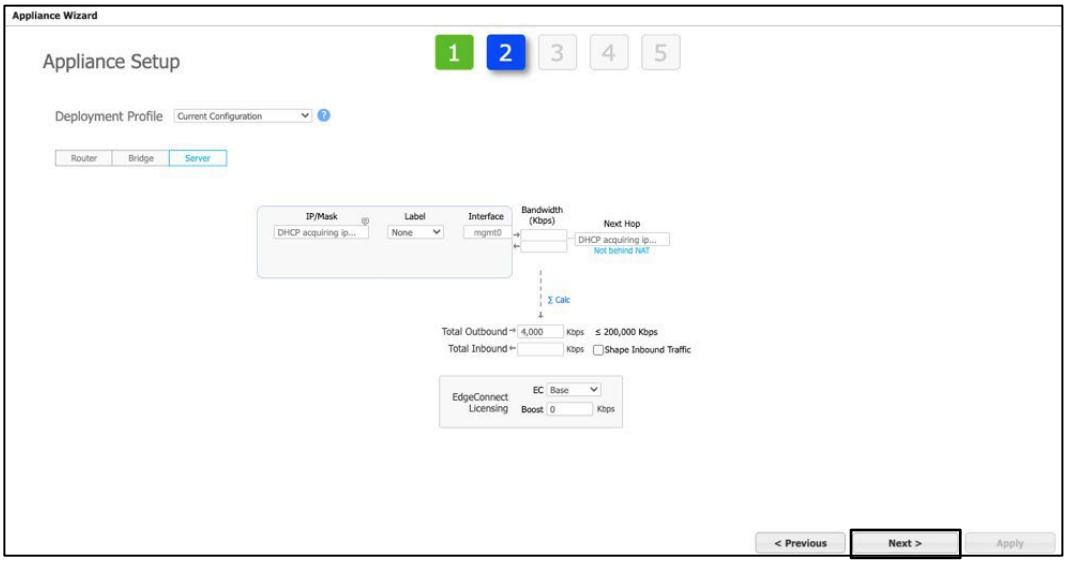

Figure 13. Page 2 of the Appliance Wizard.

e. Continue through the appliance wizard, when you reach step 5 de-select any templates and do not apply overlays currently. You will apply overlays after completing the mac address assignments and deployment changes.

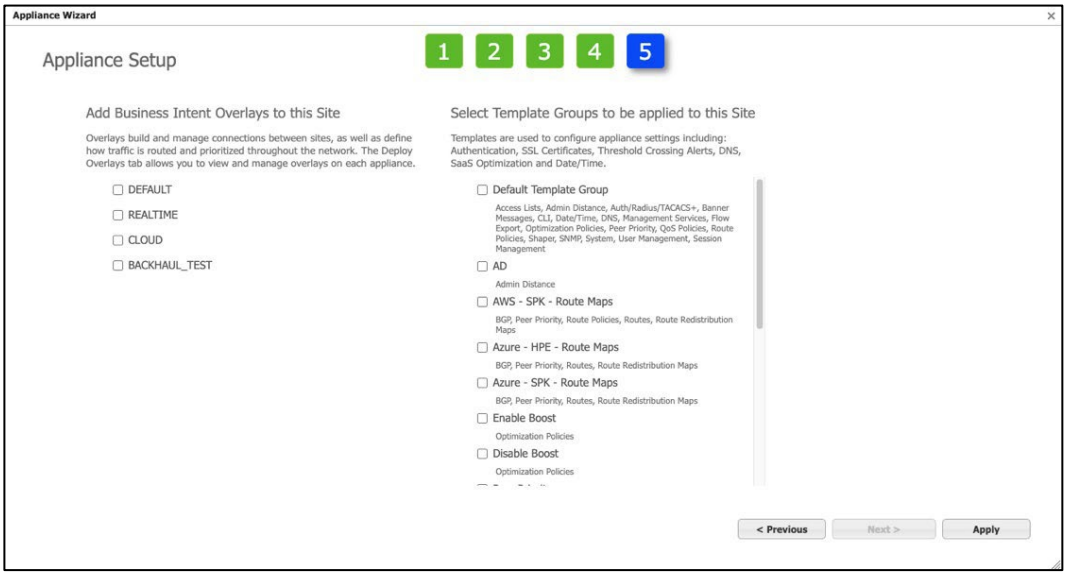

Figure 14. Page 5 of the Appliance Wizard.

5. Repeat these steps (1-4) for the other EC-V. Ensure to enter the same Site Name on both EC-Vs to prevent them from forming tunnels with each other.

Locate MAC addresses

To find MAC addresses assigned by Azure, you must first log into the Linux shell of the EC-V. To open the Linux shell:

1. Right-click on the first EC-V on the Orchestrator tree, and then click **CLI Session**. This opens a CLI shell of the EC- V on a new window.
2. In the CLI session window, run the following commands:

   ```
   enable

   show interface eth0

   show interface eth1
   ```

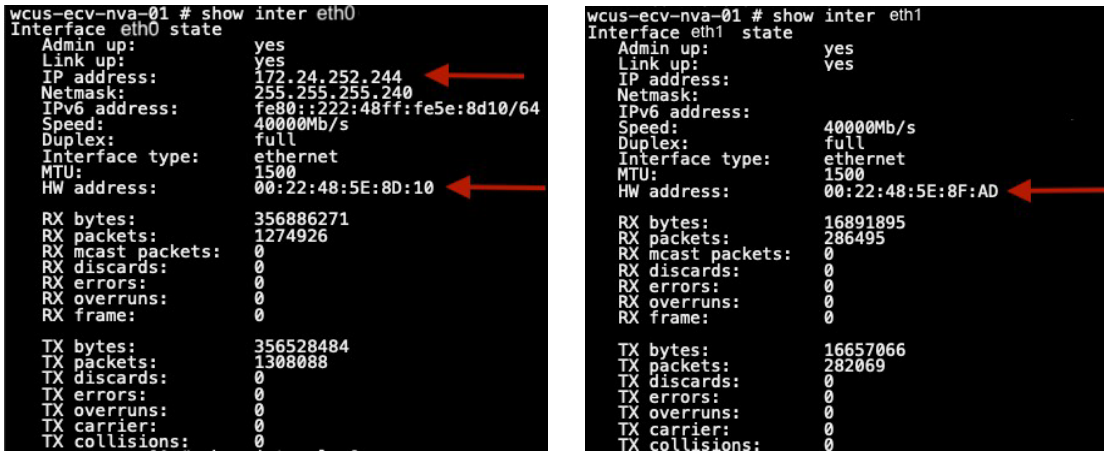

Figure 15. Locating MAC addresses through the CLI.

3. Record the MAC/IP/Mask info for eth0, this will be configured as "wan0".
4. Record the MAC info for eth1, this will be configured as "lan0".

Note

If eth1 (aka lan0) does not present an IP address in the CLI output, you will need to ensure you have the IP address that is listed in the “Instance Info” dialog from the Azure portal. This information was gathered in Step 4 of the “Correlate EC-Vs” section.

NVA instance	NIC type	Public IP Address	Private IP Address
wcus-ecv-nva_0	privatenicipconfig		172.24.252.229
wcus-ecv-nva_0	publicnicipconfig	52.161.44.10	172.24.252.244
wcus-ecv-nva_1	privatenicipconfig		172.24.252.230
wcus-ecv-nva_1	publicnicipconfig	52.161.45.149	172.24.252.245

Figure 16. NVA instance information.

5. Repeat the steps above to find the IP/MAC addresses for ECV-2.

Assign MAC addresses

Perform the following tasks to assign the MAC addresses you found using the above CURL command:

1. Select **ECV-1** on the Orchestrator tree.
2. Open the **Interfaces** tab.
3. Click the edit icon.
4. Search for the **WAN0** interface.
5. Click the drop-down menu on the **MAC** column.
6. Select the **WAN0 MAC address**.
7. Click **Apply**.

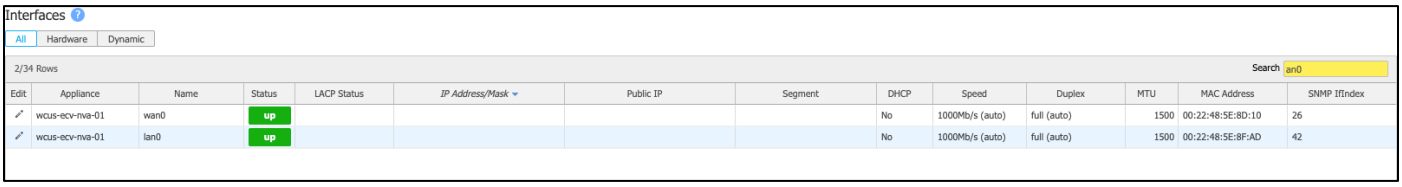

Figure 17. The Interfaces tab in Orchestrator.

8. Follow steps four to seven above to assign the LAN0 MAC address to the LAN0 interface. After assigning MAC addresses on both WAN0 and LAN0 interfaces, you will receive an alarm mentioning that the appliance requires a reboot. **DO NOT REBOOT THE EC-V YET.** We will reboot the EC-V after assigning IP addresses in the next topic.
9. Now that you have assigned MAC addresses on both interfaces on ECV-1, repeat the steps to assign MAC addresses on ECV-2.

Shut down MGMT0

Perform the following tasks to disable the unassigned mgmt0 interface to clear the alarm it is generating:

1. Select **ECV-1** on the Orchestrator tree.
2. Open the **Interfaces** tab.
3. Click the edit icon.

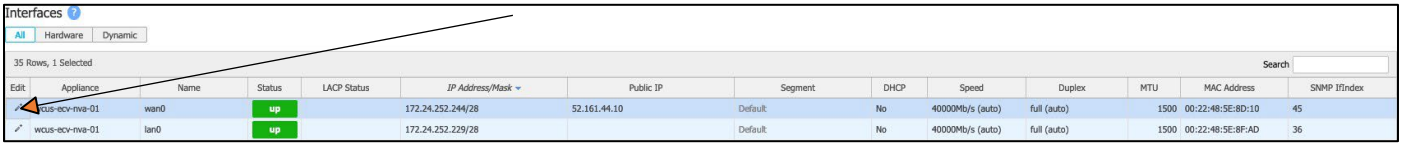

Figure 18. Shutting down MGMT0 on the Interfaces tab in Orchestrator.

4. Click **All Interfaces**.

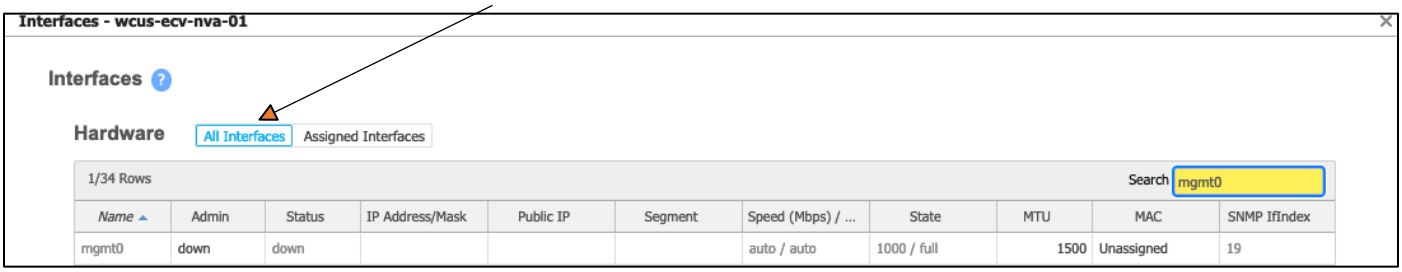

Figure 19. The All Interfaces sub-tab on the Interfaces tab in Orchestrator.

5. Search for the **mgmt0** interface.
6. Click the drop-down menu on the **Admin** column.
7. Select **down**.
8. Click **Apply**.
9. Repeat these steps for ECV-02.

Assign IP addresses

Perform the following tasks to assign IP addresses on the EC-V:

1. Select **EC-V-1** on the Orchestrator tree.
2. Open the **Deployment** tab.
3. Click the edit icon.
4. Click the **Router** tab.
5. Set the FW Mode to **Stateful+SNAT**.
6. Assign the WAN0 IP/Mask and LAN0 IP/Mask based on the information you collected from the previous section Correlate EC-Vs.
7. Enter the **WAN0 Next Hop IP** address. The WAN0 subnet's first useable IP address is the next hop IP address of the WAN0 subnet.
8. Enable **Stateful+SNAT** on the WAN0 interface.
9. Set the WAN0 Label.

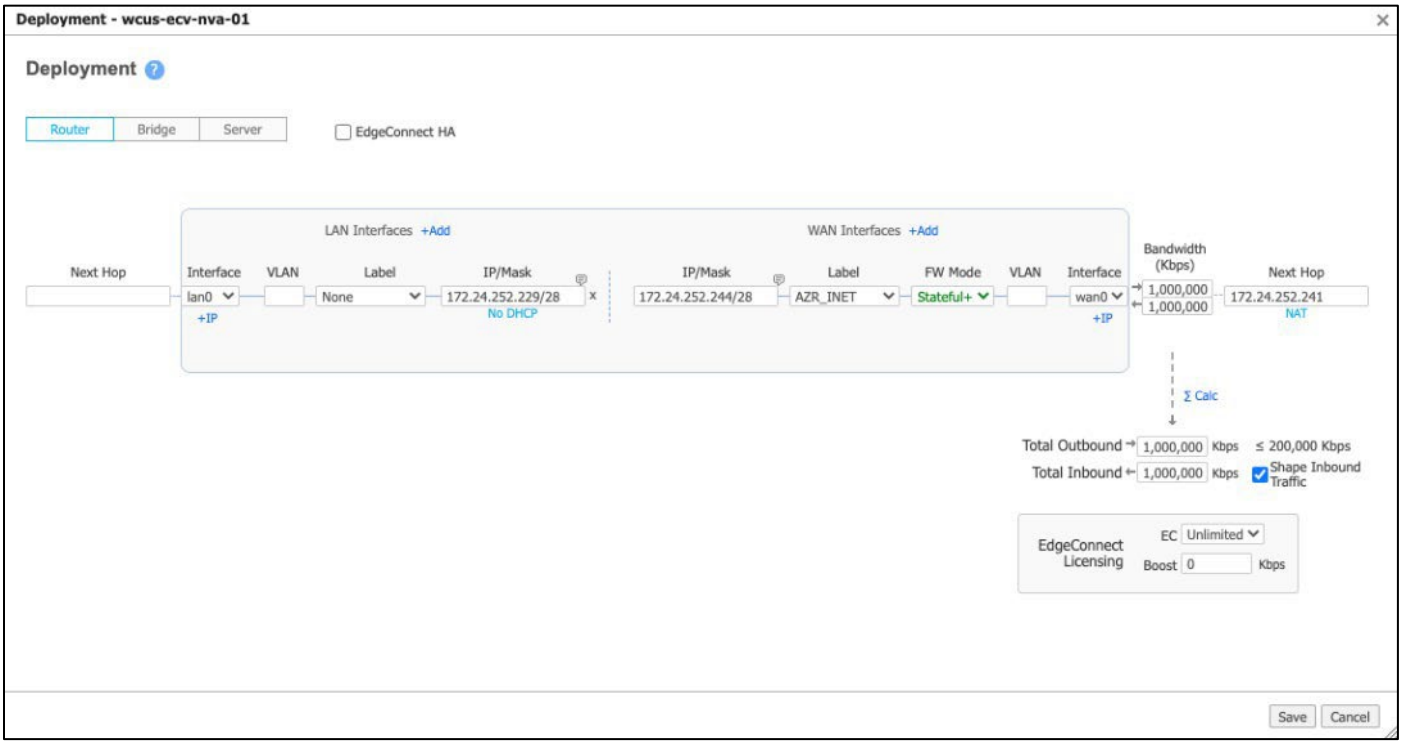

Figure 20. The Deployment tab in Orchestrator.

10. Enter Boost bandwidth, if necessary.
11. Click **Save**.
12. Click **Apply and Reboot** on the Reboot Appliance dialog box. The appliance begins rebooting.
13. Repeat the above steps on ECV-2. Wait for approximately 15 minutes for the appliance to be fully operational again.

Create two static routes for enabling BGP

Now that the EC-V is fully configured and operational, you are ready to enable BGP. To do so, you must first create static routes:

1. Select **ECV-1** on the Orchestrator tree.
2. Open **Configuration > Routes** and select **Local/Static**.
3. Click the edit icon.
4. Click **Add Route**.
5. Enter the following settings:

Setting	Description
Subnet/Mask	Enter the first BGP endpoint (/32) IP address. Refer to Figure 3 or Figure 32 to find these IP addresses.
Next Hop	Enter the LAN0 next-hop IP address.
Interface	LAN0

Setting	Description
Zone	Default
Metric	Leave default value (50).
Tag	ANY
Comments	Optional

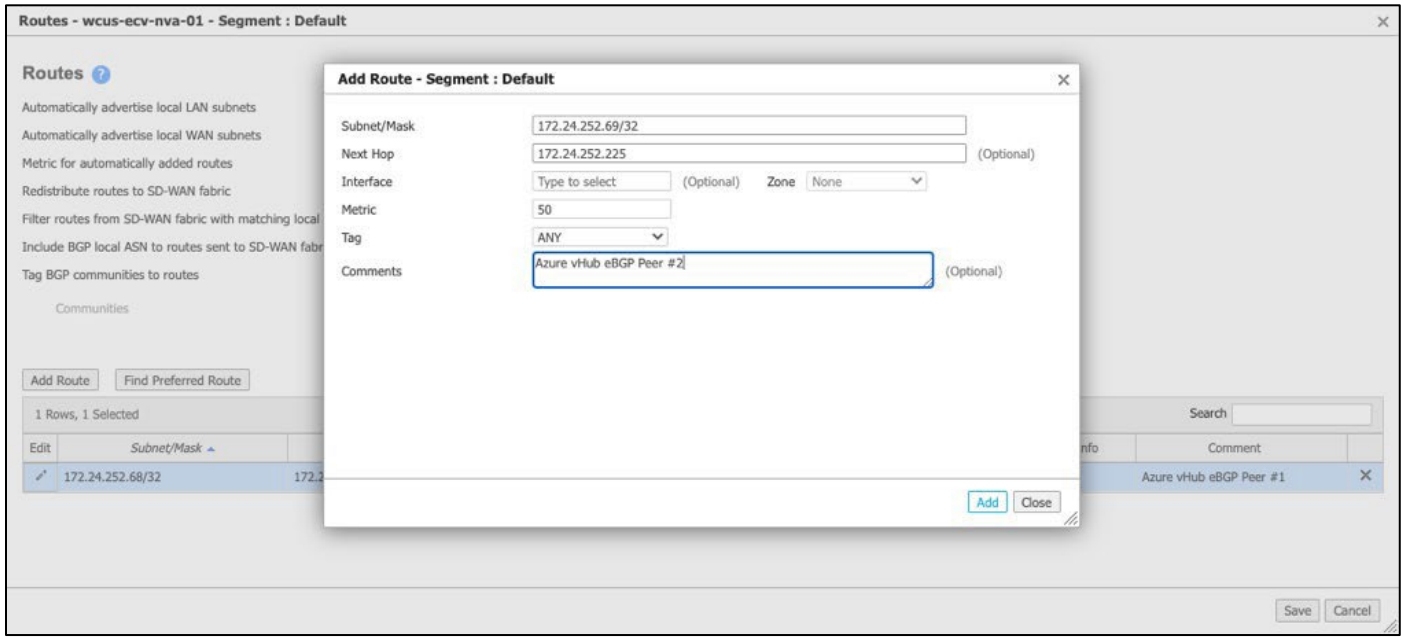

Figure 21. A configured Add Route table in Orchestrator.

6. Click **Add**.
7. Create the second static route for the second BGP endpoint. Figure 8 shows both static routes.

Figure 22. Creating static routes on the Routes tab in Orchestrator.

8. Repeat these steps for ECV-02.

Create static routes for Azure health probes

1. Select **ECV-1** on the Orchestrator tree.
2. Open **Configuration > Routes** and select **Local/Static**.
3. Click the edit icon.

4. Click **Add Route**.
5. Enter the following settings:

Setting	Description
Subnet/Mask	168.63.129.16/32
Next Hop	Enter the LAN0 next-hop IP address.
Interface	LAN0
Zone	Default
Metric	Leave default value (50).
Tag	ANY
Comments	Optional

Figure 23. Creating static routes for Azure Health Probes in Orchestrator.

6. Repeat these steps for ECV-02.

Apply templates and overlays

Now that the appliances are up and operational, we can apply templates and overlays to these appliances.

Note

If you do not currently have your desired BGP route-maps configured as part of your templates you can configure them now.

1. Select **ECV-1** on the Orchestrator tree.
2. Open **Configuration > Apply Template Groups**.
3. Select your desired template groups and click **Apply**.

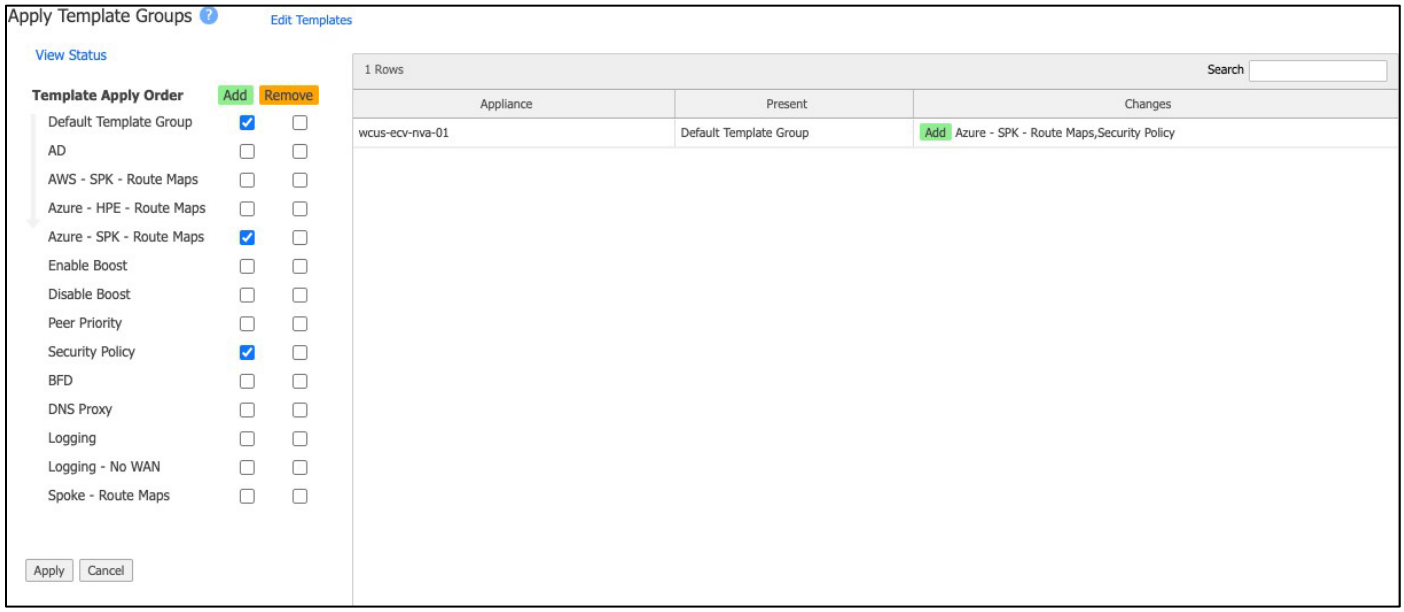

Figure 24. The Apply Template Groups tab in Orchestrator.

4. Select **ECV-1** on the Orchestrator tree.
5. Open **Configuration > Apply Overlays**.
6. Select your desired overlays and click **Apply**.

Figure 25. The Apply Overlays tab in Orchestrator.

Enable BGP

Now that the static routes are created, perform the following tasks to establish the BGP sessions:

1. Select **ECV-1** on the Orchestrator tree.
2. Open **Configuration > BGP**.
3. Click the edit icon.
4. Under BGP Peers, click **Add**.
5. Enter the following settings:

Setting	Description
Peer IP	Primary Azure BGP Peer (same address as the /32 Static Route added in the previous step)
Peer Adjacency	Single Hop
Local Interface	lan0
Peer ASN	65515
Override ASN	Not selected
Peer Type	Branch
Soft Reconfiguration	Selected
Outbound route map	Select your templated route-map.[1]
Inbound route map	Select your templated route-map.[2]
Keep Alive Timer	5
Hold Timer	15

[1] If you do not have BGP outbound route-maps created in templates, please see Appendix for the recommended local route-map configuration.
[2] If you do not have BGP inbound route-maps created in templates, please see Appendix for the recommended local route-map configuration.

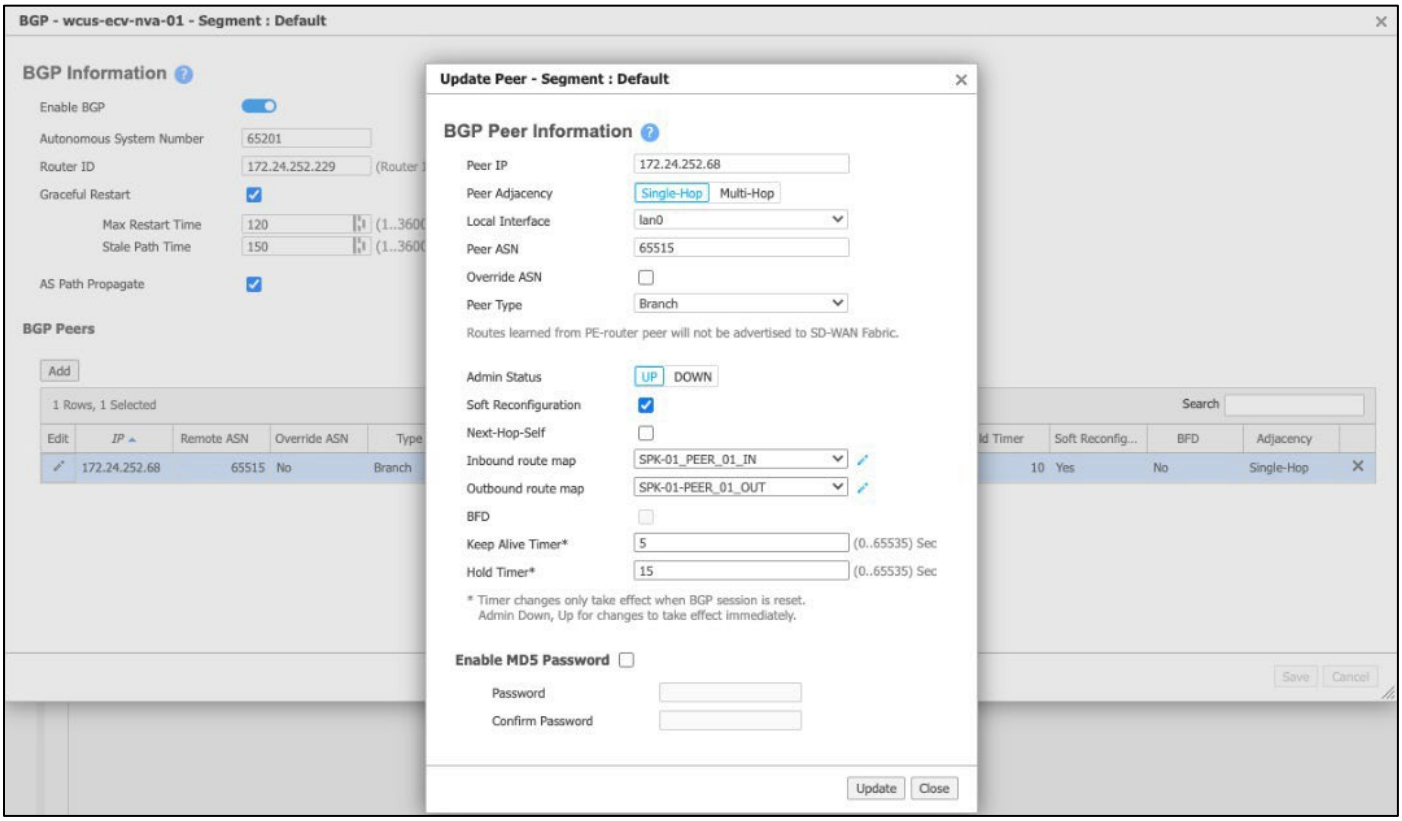

Figure 26. The Update Peer dialog box in Orchestrator.

6. Repeat the steps above for the second peer. Make note of the route-map applied to Peer 1 and 2; these should be configured according to your desired operation.

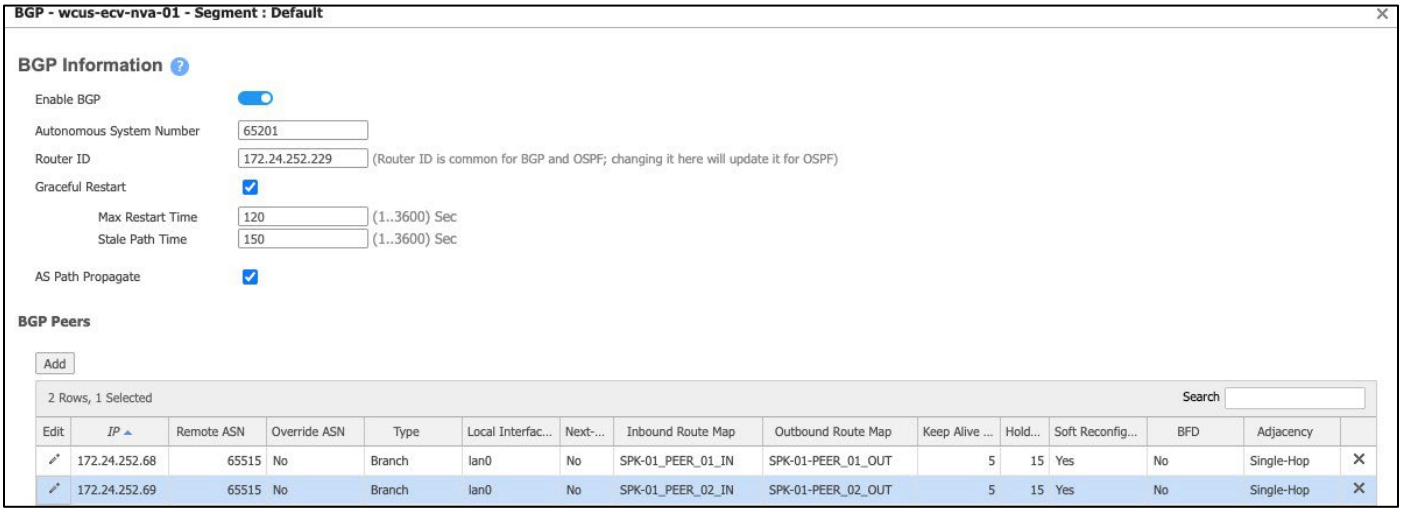

Figure 27. The BGP Information tab in Orchestrator.

7. Repeat the steps above for ECV-2.

Appendix

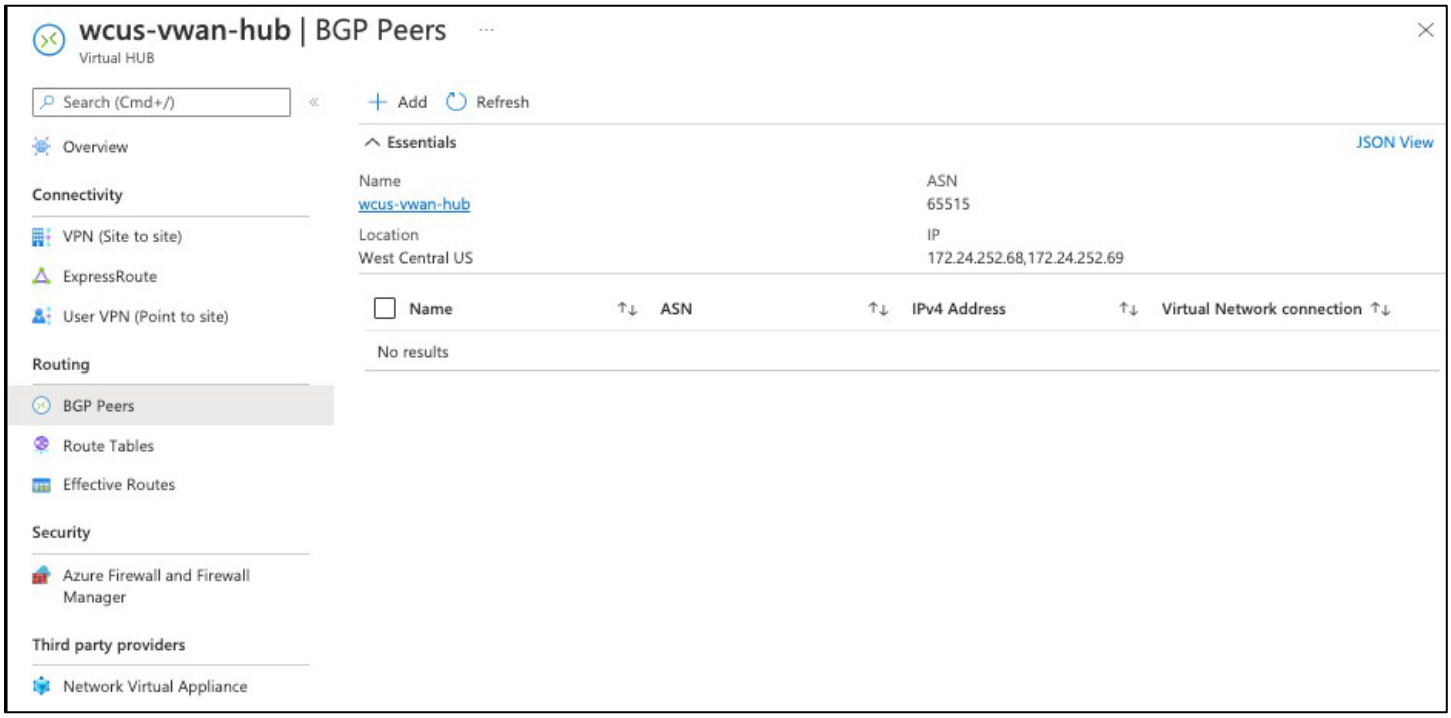

Figure 28. The BGP Peers page in Virtual WAN Hub.

Local BGP route-map configuration steps

If you do not have your route-maps configured as part of your templates the following steps can be used to configure local route-maps on the appliance. This is not best practice, but can be used temporarily if change controls do not allow global template configurations etc.

1. Click the edit icon next to Outbound route map.
2. In the drop-down menu, select **default_rtmap_bgp_outbound_br**.
3. Click **Clone Map**.
4. Give the new map a name (for example, AZURE_PEER-1_OUT).
5. Click **Clone**.
6. Remove lines **65505**, **65525**, and **65535**.
7. Edit lines **65485**, **65495**, and **65515**, and change the Set Action for ASN Prepend Count = 1.
8. Click **Clone Map**.
9. Give the new map a name (for example, AZURE_PEER-2_OUT).
10. Edit lines **65485**, **65495**, and **65515**, and change the Set Action for ASN Prepend Count = 2.

    Refer to Figure 29 for an example of what the result should look like.

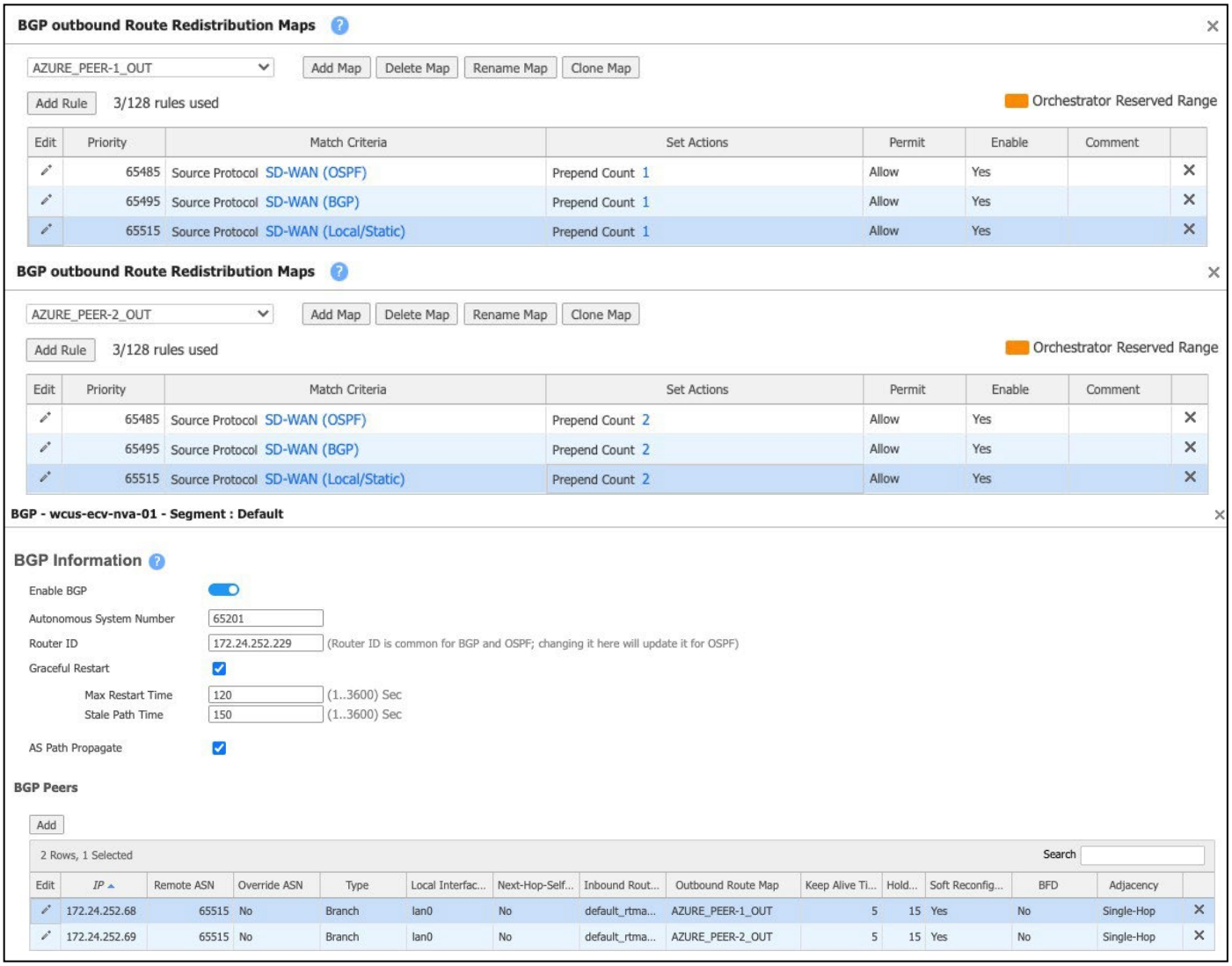

Figure 29. Local BGP route map configurations.

Where to find configuration items

If you do not have the EdgeConnect ASN that was configured in the NVA deployment steps, you can find it by going to **Subscriptions > Resources > Filter "Type = Managed Applications" >** click the Managed Application.

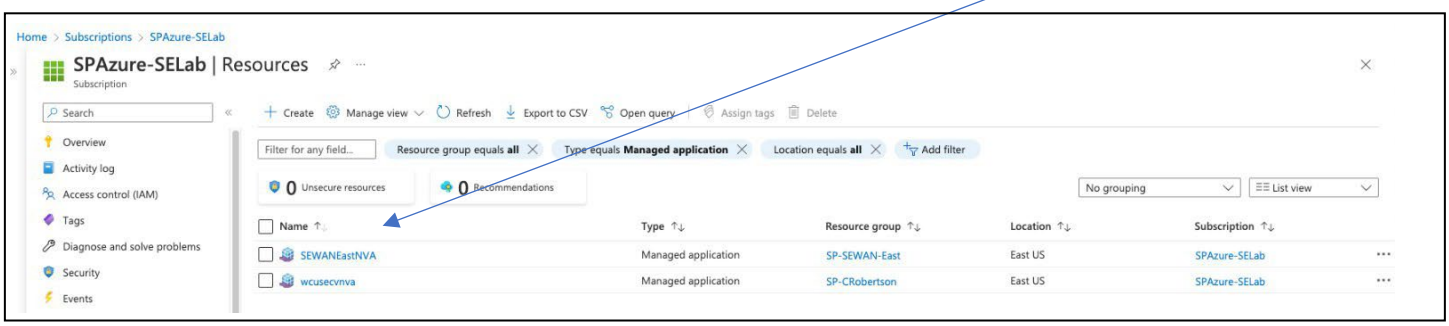

Figure 30. The NVA Resources page.

Under the managed application screen, click **Parameters and Outputs**.

Figure 31. The NVA Parameters and Outputs page.

If you do not have the Virtual WAN Hub ASN or BGP Peer IPs you can find them by going to **Virtual WANs > Select your Virtual WAN > Hubs > Select your Hub**, and under Routing, select **BGP Peers**.

The peer IPs and ASN can be found in the upper-right corner of the screen.

Figure 32. The NVA BGP Peers page.

Learn more at

hpe.com

Chat now (sales)

Hewlett Packard Enterprise