EdgeConnect and Microsoft Azure Virtual WAN Integration Guide

March 2020
PN: 201670-001
Revision B

Copyright and Trademarks

Silver Peak Systems, Inc.
2860 De La Cruz Boulevard
Santa Clara, CA 95050

1.877.210.7325 (toll-free in USA)
+1.408.935.1850

http://www.silver-peak.com/support

Contents

Additional Resources

If you need assistance or additional information, contact the Silver Peak Technical Support team or review other documentation available on our website.

Support

For product and technical support, contact Silver Peak Systems at either of the following:

1.877.210.7325 (toll-free in USA)
+1.408.935.1850
www.silver-peak.com/support

We're dedicated to continually improving the usability of our products and documentation.

- If you have suggestions or feedback for our documentation, send an e-mail to techpubs@silver-peak.com.
- If you have comments or feedback about the interface, send an e-mail to usability@silver-peak.com.

Related Documentation

- **Release Notes** provide information on new software features, system bugs, and software compatibility.
- All user documentation is available at http://www.silver-peak.com.

About Azure Virtual WAN with EdgeConnect

This guide explains how to integrate Silver Peak EdgeConnect with Microsoft Azure Virtual WAN (VWAN) cloud services. Using Silver Peak Unity Orchestrator, you can build, orchestrate, maintain, and troubleshoot secure connectivity from EdgeConnect appliances to the Azure Cloud.

Benefits

By integrating EdgeConnect with Azure VWAN, you will benefit from optimized routing using the Microsoft global network, automated large-scale connectivity from branches to Azure workloads, and unified network and policy management.

Overview

Before you can start to build the integration in EdgeConnect and Microsoft Azure Virtual WAN, you have to create an Azure AD application and service principal in the Azure portal. In the portal, you will:

- Create a subscription account using Azure AD
- Create a resource group
- Create a VWAN in the resource group
- Create hubs in the VWAN
- Create a storage account

NOTE When the configuration in the Azure portal is complete, you will need the following details when working in EdgeConnect and Microsoft Azure Virtual WAN:

- Subscription ID
- Tenant ID
- Application ID
- Secret Key
- Storage account name, key, and URL

In Orchestrator, you will provide the details of your Azure subscription and AD application (noted above), select interface labels for building tunnels, and associate EdgeConnect appliances to an Azure Virtual WAN.

Azure Prerequisites

There are a few things you'll need to set up in the Azure portal before doing any configuration on the Silver Peak side of the integration.

Create Azure Application and Service Principal

Create and register a new Azure Active Directory (AD) application (Orchestrator) and service principal in the Azure portal. For more information about this step, refer to Create Application and Service Principal.

After you have successfully registered the new application, you will want to note the following application details as you will need to provide them in Orchestrator (see Add Azure Subscription Details).

- Subscription ID
- Tenant ID
- Application ID
- Secret Key (from Certificates and secrets menu)

Create an Azure Storage Account

In the Azure portal, create a storage account and blob container for downloading the VPN configuration file. For more information about this step, refer to Create an Azure Storage Account and Blob Storage Quick Start.

1. Go to Azure Storage Account
2. Create a new storage account
3. Create a new blob container inside the storage account

You need the following details for Orchestrator configuration (see Add Azure Subscription Details).

- Blob URL (blob container properties)
- Storage Access Key (Access Keys menu)

Create an Azure Resource Group, Virtual WANs, Hubs

You will need to create a resource group to contain your Azure Virtual WANs and the storage container that you just created. In the new resource group, create your Azure Virtual WANs and hubs for every virtual WAN.

Before continuing to Silver Peak Prerequisites, verify the Virtual Hub is successfully deployed. This can take from 5 to 30 minutes.

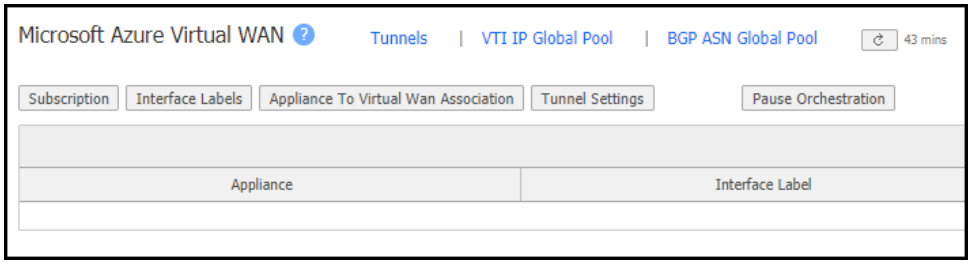
For more information about this step, refer to Azure Resource Manager and Virtual WAN and Hub Tutorial.

Silver Peak Prerequisites

After completing the Azure configuration requirements in the Azure portal, you should configure global pools for Virtual Tunnel Interface (VTI) IP addresses and BGP ASNs.

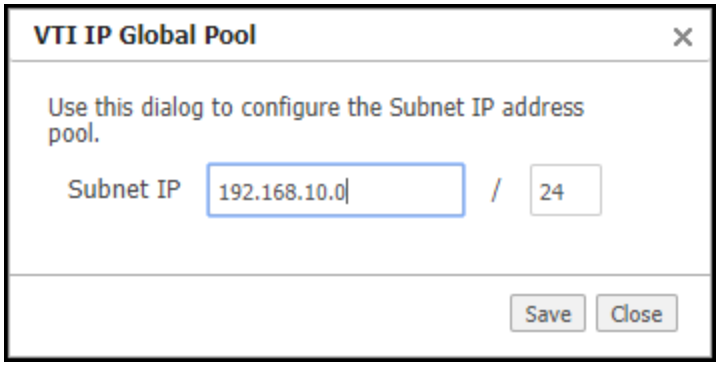
1. Log in to Orchestrator as a user with read-write privileges.
2. Open the Microsoft Azure Virtual WAN tab (click **Configuration**, **Cloud Services**, **Microsoft Azure Virtual WAN**).

   The Microsoft Azure Virtual WAN tab appears.



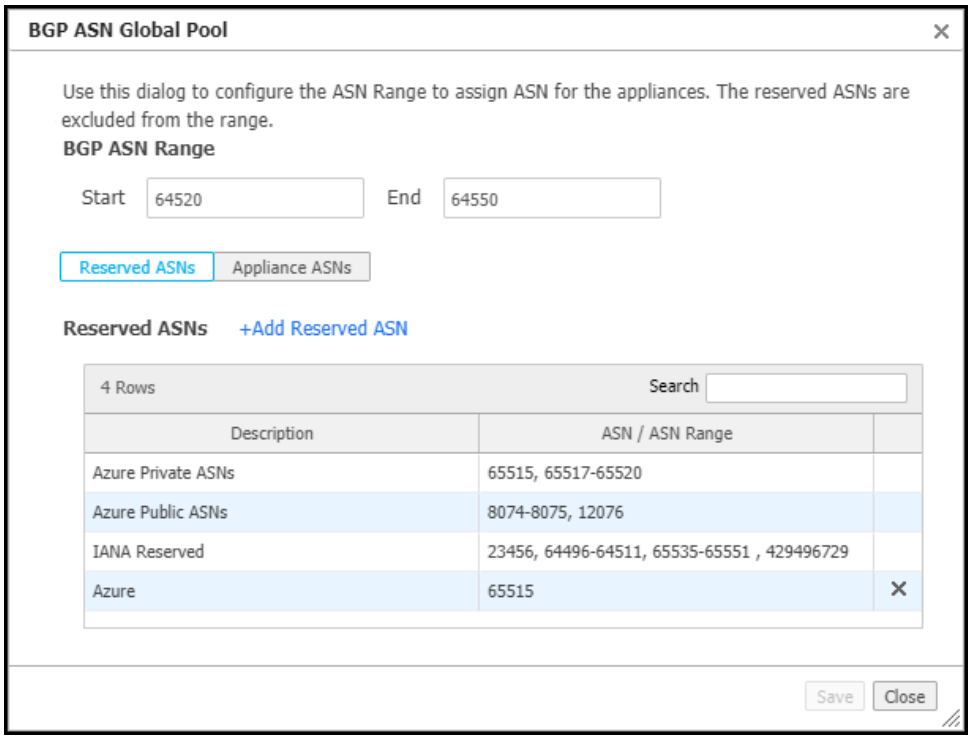
3. Click the **VTI IP Global Pool** link.

   The VTI IP Global Pool dialog appears.



4. Enter the IP address and subnet mask to use for the VTI pool for Azure VWAN.
5. Click **Save**.
6. Click the **BGP ASN Global Pool** link.

The BGP ASN Global Pool dialog appears.



7. Enter the start and end values for BGP ASN range to use for Azure VWAN.
8. If you want to add a reserved ASN or ASN range, click **+Add Reserved ASN** and provide a description and the ASN/ASN Range in the new table row.
9. Click **Save**.

Configure the Silver Peak and Azure Virtual WAN Integration

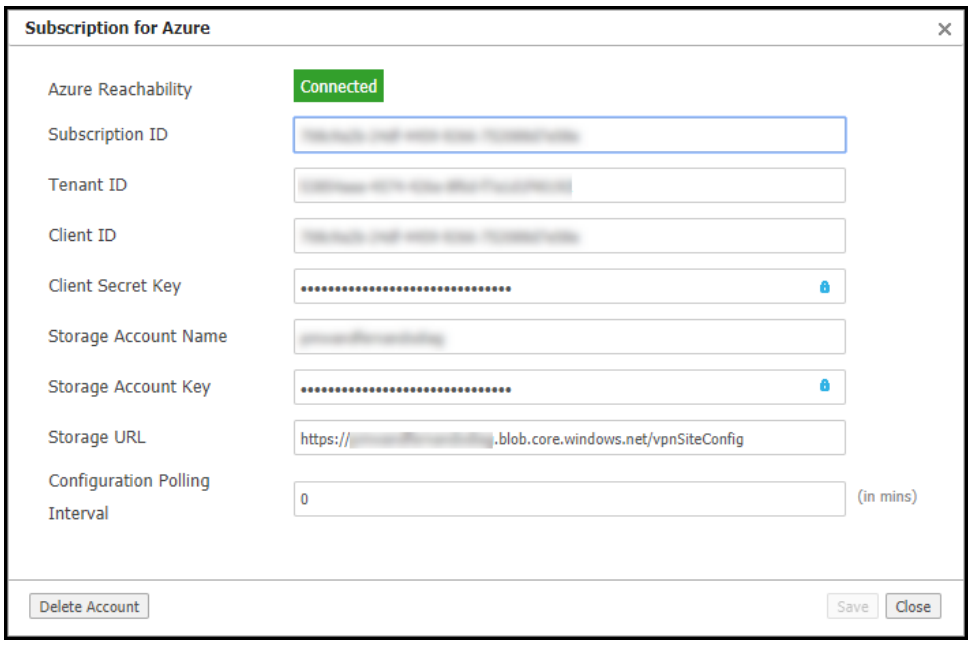
After completing the prerequisite configuration steps in the Azure portal and in Orchestrator, finish the integrations steps using Orchestrator's Microsoft Azure Virtual WAN tab.

There are four buttons at the top of the tab — Subscription, Interface Labels, Appliance To Virtual Wan Association, and Tunnel Settings — that you will use to complete the configuration.

Add Azure Subscription Details

1. Click the **Subscription** button.

   The Subscription for Azure dialog appears.



   The status of the connection between Silver Peak and your Azure subscription is displayed next to Azure Reachability.

2. Enter the subscription, application, and storage account details from your Azure configuration in the following fields: Subscription ID, Tenant ID, Client ID, Client Secret Key, Storage Account Name, Storage Account Key, and Storage URL.

   TIP The Storage URL can be found in the Storage Accounts tab of the Azure portal. After creating the storage account, create a blob container and note the container URL. Add the URL in the Storage URL field, add a forward slash, then add a file name

3. In the Configuration Polling Interval field, specify how frequently (in minutes) Orchestrator should check for configuration changes in Azure. For example, if you enter 60, Orchestrator will check for configuration changes once every 60 minutes.

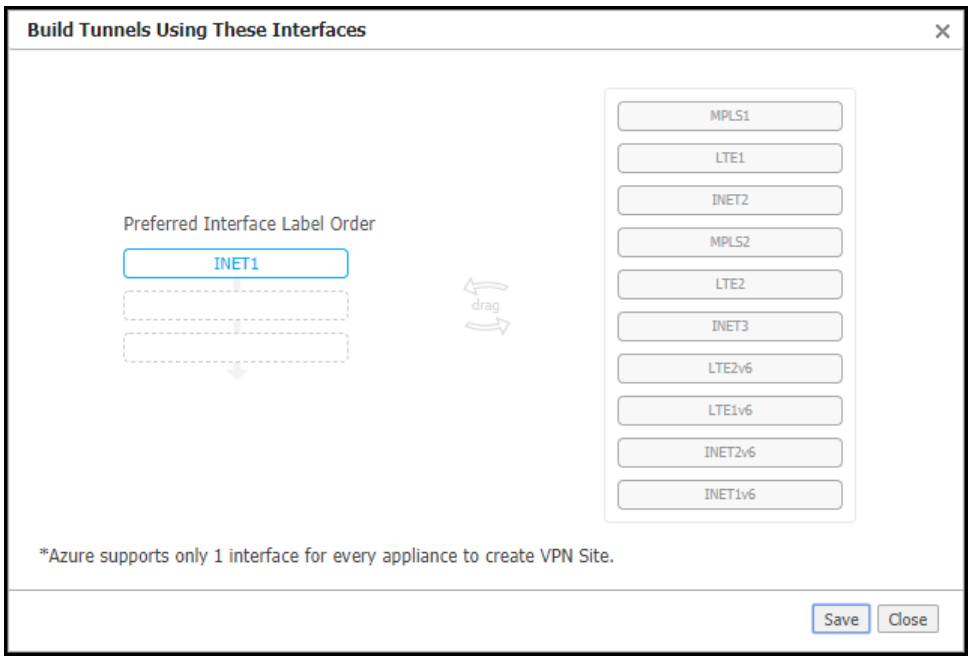
4. When you are finished, click **Save**.

   NOTE If you want to delete the current subscription configuration, click **Delete Account**.

Configure Interface Labels

1. Click the **Interface Labels** button.

   The Build Tunnels Using These Interfaces dialog appears.



2. Drag an interface label from the list on the right to the preferred order list on the left.

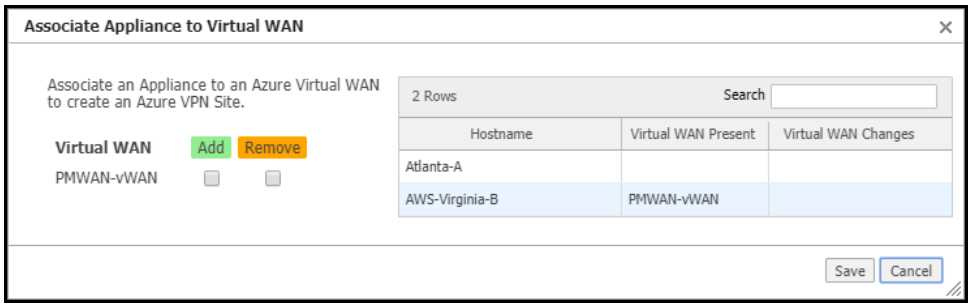
   NOTE Only one interface label is supported for building tunnels. If you add more than one interface, only the top interface will be used.

3. Click **Save**.

Associate Appliances to an Azure Virtual WAN

1. In the device tree, select one or more appliances that you want to associate to an Azure Virtual WAN.
2. Click the **Appliance to Virtual WAN Association** button.

   The Associate Appliance to Virtual WAN dialog appears, and the selected appliances are displayed in the table. If any of the listed appliances are already associated with an Azure Virtual WAN, the name of the associated WAN is listed in the Virtual WAN Present column.



   NOTE Each appliance can be associated with only one Azure Virtual WAN.

3. To associate the selected appliances to an existing Azure Virtual WAN, select the Add checkbox next to the name of the Virtual WAN.
4. To remove an existing association for the selected appliances, select the Remove checkbox next to the name of the Virtual WAN.

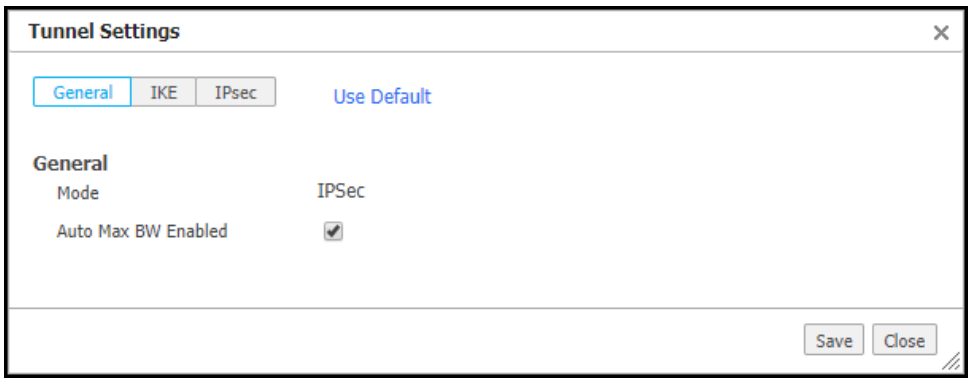
   The configured changes will be displayed (add or remove) in the Virtual WAN Changes for each appliance.

5. Click **Save**.
6. Verify the appliances are associated to at least one overlay: open the **Apply Overlays** tab by navigating to (*Configuration -> Overlays -> Apply Overlays*).

View or Modify Tunnel Settings

1. Click the **Tunnel Settings** button.

   The Tunnel Settings dialog appears.

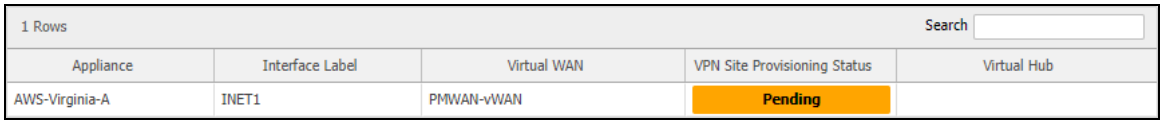


   NOTE Default tunnel settings are defined using the default VPN configuration parameters received from virtual WAN APIs in your Azure portal account.

2. If you want to modify the current settings, make changes under General, IKE, and IPsec.
3. Click **Save**.

Review Azure VPN Site Status

When you have finished configuring all of the settings in the Microsoft Azure Virtual WAN tab, review the configuration table to see the VPN site provisioning status for each appliance.

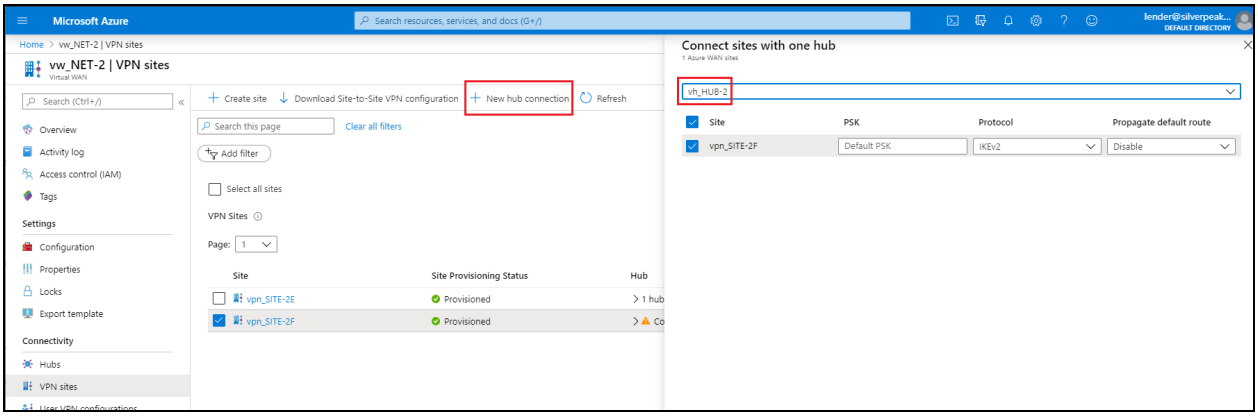


The table shows the Virtual WAN to which each appliance is associated and the VPN site provisioning status.

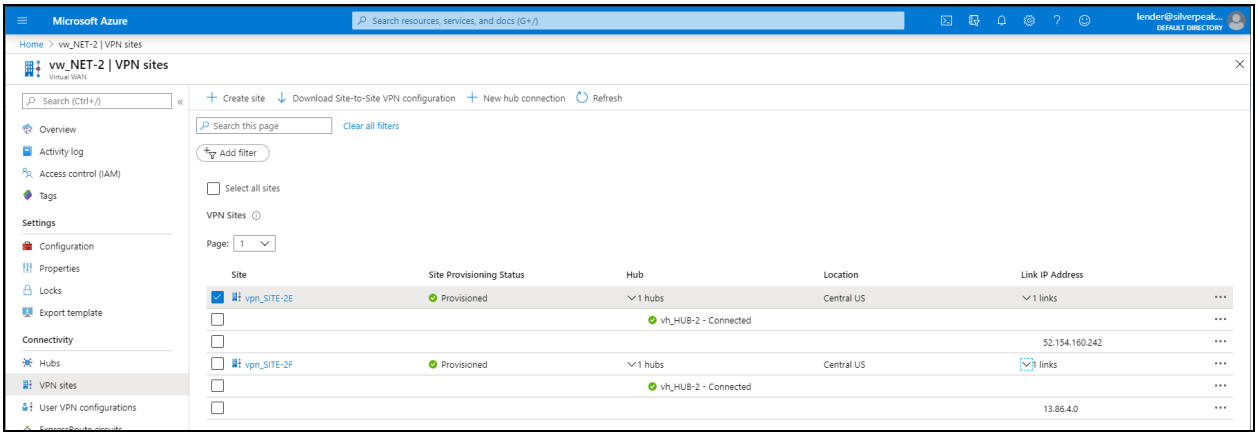
NOTE VPN site provisioning status must be green to before you can proceed to the next step and associate a VPN site to one or more Azure hubs in the Azure portal.

Associate a VPN Site to Azure Hubs

When VPN site provisioning status is green in Orchestrator, you can return to the Azure portal and associate each VPN site to one or more Azure hubs.



NOTE It can take five to 30 minutes for the association between a VPN site and a hub to complete.



Monitor Integration Status

When you have successfully finished with all of the previous steps, Orchestrator will now automate the creation of IPSec tunnels for Azure VPN site connections. By default, EdgeConnect creates two active-active IPSec tunnels for each VPN site.

You can use the Tunnel tab in Orchestrator to check the status of the IPSec tunnels created for Azure.

NOTE Use the keyword “ThirdParty_Azure” to filter all the Azure tunnels for the appliances.

Additionally, Orchestrator will now automate dynamic routes via BGP using Azure BGP endpoints.

For overall monitoring in Orchestrator, use the Dashboard, Tunnels, and Flow tabs.