

Design and implement Azure ExpressRoute

Introduction

ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection with the help of a connectivity provider. With ExpressRoute, you can establish connections to various Microsoft cloud services, such as Microsoft Azure and Microsoft 365. Connectivity can be from an any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a colocation facility. Since ExpressRoute connections do not go over the public Internet, this approach allows ExpressRoute connections to offer more reliability, faster speeds, consistent latencies, and higher security.

ExpressRoute capabilities

Some key benefits of ExpressRoute are:

- Layer 3 connectivity between your on-premises network and the Microsoft Cloud through a connectivity provider
- Connectivity can be from an any-to-any (IPVPN) network, a point-to-point Ethernet connection, or through a virtual cross-connection via an Ethernet exchange
- Connectivity to Microsoft cloud services across all regions in the geopolitical region
- Global connectivity to Microsoft services across all regions with the ExpressRoute premium add-on
- Built-in redundancy in every peering location for higher reliability

Azure ExpressRoute is used to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. ExpressRoute connections do not go over the public Internet, and they offer more reliability, faster speeds, and lower latencies than typical Internet connections.

Understand use cases for Azure ExpressRoute

Faster and Reliable connection to Azure services - Organizations leveraging Azure services look for reliable connections to Azure services and data centers. Public internet is dependent upon many factors and may not be suitable for a business. Azure ExpressRoute is used to create private connections between Azure data centers and infrastructure on your premises or in a colocation environment. Using ExpressRoute connections to transfer data between on-premises systems and Azure can also give significant cost benefits.

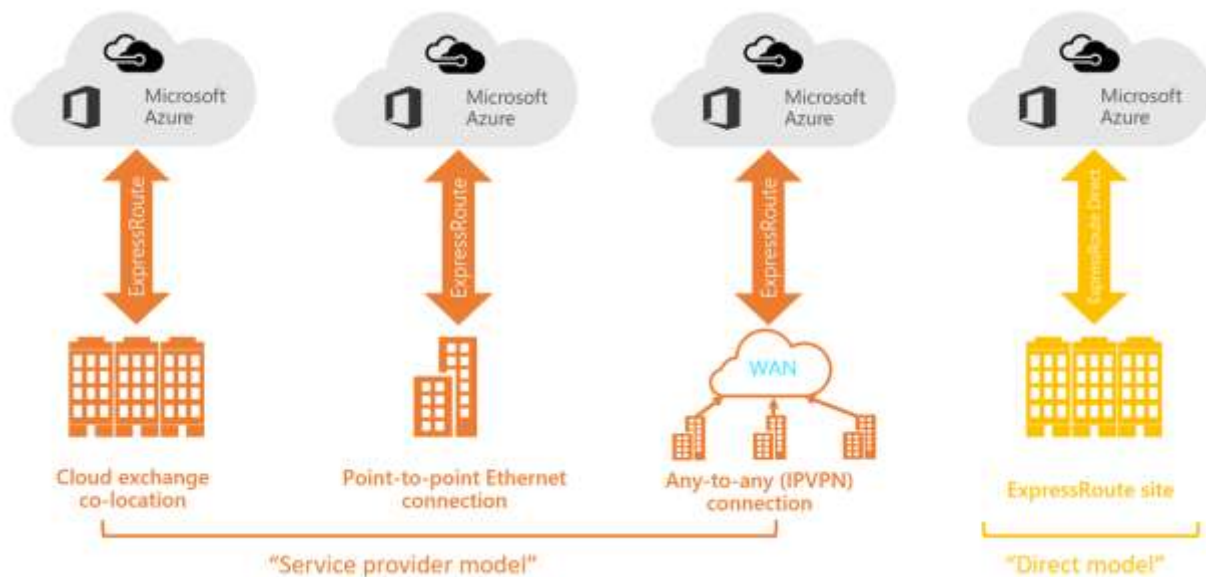
Storage, backup, and Recovery - Backup and Recovery are important for an organization for business continuity and recovering from outages. ExpressRoute gives you a fast and reliable connection to Azure with bandwidths up to 100 Gbps, which makes it excellent for scenarios such as periodic data migration, replication for business continuity, disaster recovery and other high-availability strategies.

Extends Data center capabilities - ExpressRoute can be used to connect and add compute and storage capacity to your existing data centers. With high throughput and fast latencies, Azure will feel like a natural extension to or between your data centers, so you enjoy the scale and economics of the public cloud without having to compromise on network performance.

Predictable, reliable, and high-throughput connections - With predictable, reliable, and high-throughput connections offered by ExpressRoute, enterprises can build applications that span on-premises infrastructure and Azure without compromising privacy or performance. For example, run a corporate intranet application in Azure that authenticates your customers with an on-premises Active Directory service, and serve all your corporate customers without traffic ever routing through the public Internet.

ExpressRoute connectivity models

You can create a connection between your on-premises network and the Microsoft cloud in four different ways, CloudExchange Co-location, Point-to-point Ethernet Connection, Any-to-any (IPVPN) Connection, and ExpressRoute Direct. Connectivity providers may offer one or more connectivity models.



Co-located at a cloud exchange

If you are co-located in a facility with a cloud exchange, you can order virtual cross-connections to the Microsoft cloud through the co-location provider's Ethernet exchange. Co-location providers can offer either Layer 2 cross-connections, or managed Layer 3 cross-connections between your infrastructure in the co-location facility and the Microsoft cloud.

Point-to-point Ethernet connections

You can connect your on-premises datacenters/offices to the Microsoft cloud through point-to-point Ethernet links. Point-to-point Ethernet providers can offer Layer 2 connections, or managed Layer 3 connections between your site and the Microsoft cloud.

Any-to-any (IPVPN) networks

You can integrate your WAN with the Microsoft cloud. IPVPN providers (typically MPLS VPN) offer any-to-any connectivity between your branch offices and datacenters. The Microsoft cloud can be interconnected to your WAN to make it look just like any other branch office. WAN providers typically offer managed Layer 3 connectivity.

Direct from ExpressRoute sites

You can connect directly into the Microsoft's global network at a peering location strategically distributed across the world. ExpressRoute Direct provides dual 100 Gbps or 10-Gbps connectivity, which supports Active/Active connectivity at scale.

Design considerations for ExpressRoute deployments

When planning an ExpressRoute deployment, there are many decisions to make. This section discusses a few key areas that you must consider as you design your deployment.

Choose between provider and direct model (ExpressRoute Direct)

ExpressRoute Direct

ExpressRoute Direct gives you the ability to connect directly into Microsoft's global network at peering locations strategically distributed around the world. ExpressRoute Direct provides dual 100 Gbps or 10-Gbps connectivity, which supports Active/Active connectivity at scale. You can work with any service provider for ExpressRoute Direct.

Key features that ExpressRoute Direct provides includes:

- Massive Data Ingestion into services like Storage and Cosmos DB
- Physical isolation for industries that are regulated and require dedicated and isolated connectivity like: Banking, Government, and Retail
- Granular control of circuit distribution based on business unit

Using ExpressRoute direct vs using a Service Provider

ExpressRoute using a Service Provider	ExpressRoute Direct
Uses service providers to enable fast onboarding and connectivity into existing infrastructure	Requires 100 Gbps/10 Gbps infrastructure and full management of all layers
Integrates with hundreds of providers including Ethernet and MPLS	Direct/Dedicated capacity for regulated industries and massive data ingestion
Circuits SKUs from 50 Mbps to 10 Gbps	Customer may select a combination of the following circuit SKUs on 100-Gbps ExpressRoute Direct: 5 Gbps 10 Gbps 40 Gbps 100 Gbps Customer may select a combination of the following circuit SKUs on 10-Gbps ExpressRoute Direct: 1 Gbps 2 Gbps 5 Gbps 10 Gbps
Optimized for single tenant	Optimized for single tenant with multiple business units and multiple work environments

Route advertisement

When Microsoft peering gets configured on your ExpressRoute circuit, the Microsoft Edge routers establish a pair of Border Gateway Protocol (BGP) sessions with your edge routers through your connectivity provider. No routes are advertised to your network. To enable route advertisements to your network, you must associate a route filter.

In order to associate a route filter:

- You must have an active ExpressRoute circuit that has Microsoft peering provisioned.
- Create an ExpressRoute circuit and have the circuit enabled by your connectivity provider before you continue. The ExpressRoute circuit must be in a provisioned and enabled state.
- Create Microsoft peering if you manage the BGP session directly. Or, have your connectivity provider provision Microsoft peering for your circuit.

Get a list of BGP community values

BGP community values associated with services accessible through Microsoft peering is available in the ExpressRoute routing requirements page.

Make a list of the values that you want to use

Make a list of BGP community values you want to use in the route filter.

Bidirectional Forwarding Detection

ExpressRoute supports Bidirectional Forwarding Detection (BFD) both over private and Microsoft peering. When you enable BFD over ExpressRoute, you can speed up the link failure detection between Microsoft Enterprise edge (MSEE) devices and the routers that your ExpressRoute circuit gets configured (CE/PE). You can configure ExpressRoute over your edge routing devices or your Partner Edge routing devices (if you went with managed Layer 3 connection service). This section walks you through the need for BFD, and how to enable BFD over ExpressRoute.

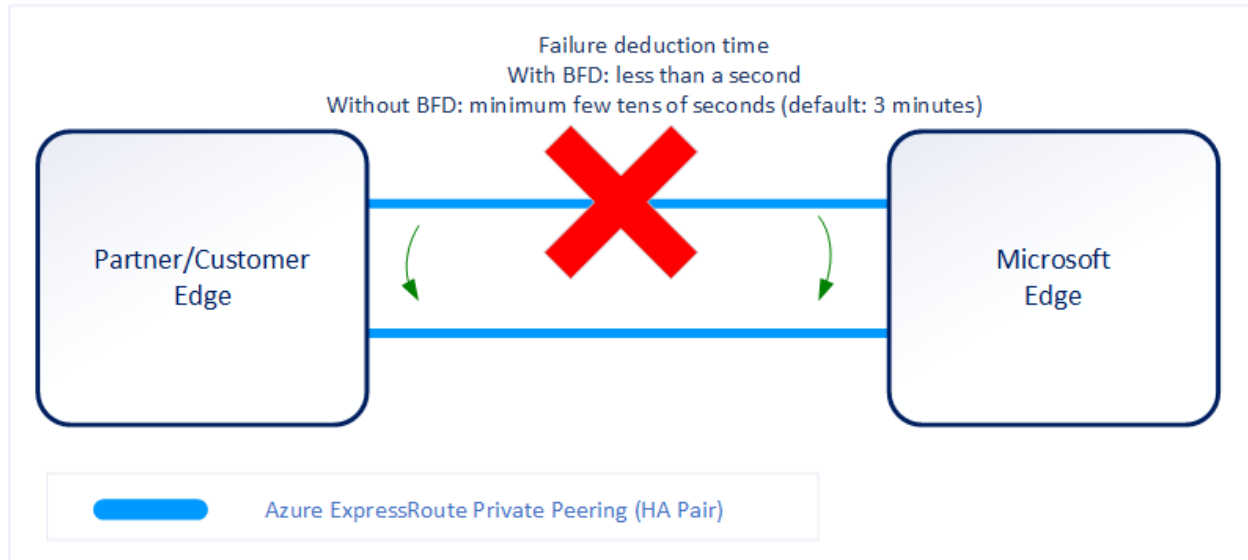
You can enable ExpressRoute circuit either by Layer 2 connections or managed Layer 3 connections. In both cases, if there are more than one Layer-2 devices in the ExpressRoute connection path, the responsibility of detecting any link failures in the path lies with the overlying BGP session.

On the MSEE devices, BGP keep-alive and hold-time are typically configured as 60 and 180 seconds, respectively. For that reason, when a link failure happens it can take up to three minutes to detect any link failure and switch traffic to alternate connection.

You can control the BGP timers by configuring a lower BGP keep-alive and hold-time on your edge peering device. If the BGP timers are not the same between the two peering

devices, the BGP session will establish using the lower time value. The BGP keep-alive can be set as low as three seconds, and the hold-time as low as 10 seconds. However, setting a very aggressive BGP timer isn't recommended because the protocol is process intensive. In this scenario, BFD can help. BFD provides low-overhead link failure detection in a sub second time interval.

The following diagram shows the benefit of enabling BFD over an ExpressRoute circuit:



Enabling BFD

BFD is configured by default under all the newly created ExpressRoute private peering interfaces on the MSEs. As such, to enable BFD, you only need to configure BFD on both your primary and secondary devices. Configuring BFD is two-step process. You configure the BFD on the interface and then link it to the BGP session.

When you disable a peering, the Border Gateway Protocol (BGP) session for both the primary and the secondary connection of your ExpressRoute circuit is shut down. When you enable a peering, the BGP session on both the primary and the secondary connection of your ExpressRoute circuit is restored.

Note

The first time you configure the peering on your ExpressRoute circuit, the Peerings are enabled by default.

Resetting your ExpressRoute Peerings might be helpful in the following scenarios:

You are testing your disaster recovery design and implementation. For example, assume that you have two ExpressRoute circuits. You can disable the Peerings of one circuit and force your network traffic to use the other circuit.

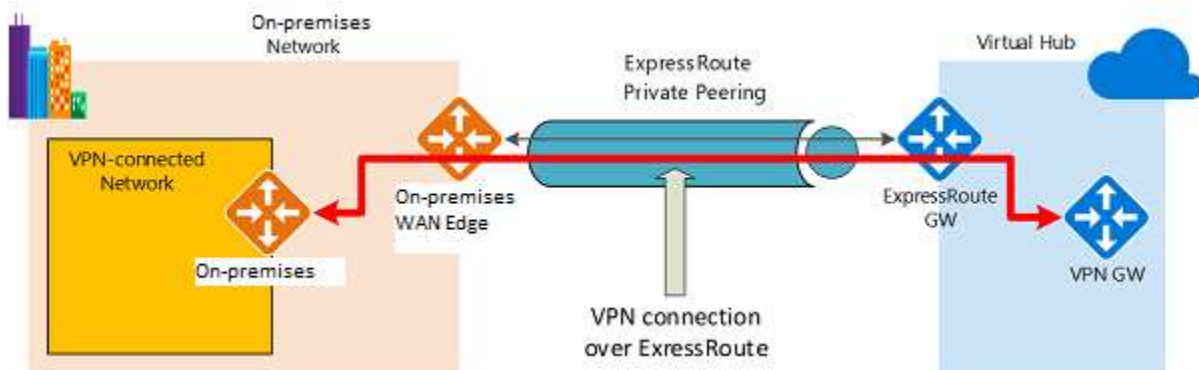
You want to enable Bidirectional Forwarding Detection (BFD) on Azure private peering or Microsoft peering. If your ExpressRoute circuit was created before August 1, 2018, on Azure private peering or before January 10, 2020, on Microsoft peering, BFD was not enabled by default. Reset the peering to enable BFD.

Configure encryption over ExpressRoute

This section shows you how to use Azure Virtual WAN to establish an IPsec/IKE VPN connection from your on-premises network to Azure over the private peering of an Azure ExpressRoute circuit. This technique can provide an encrypted transit between the on-premises networks and Azure virtual networks over ExpressRoute, without going over the public internet or using public IP addresses.

Topology and routing

The following diagram shows an example of VPN connectivity over ExpressRoute private peering:



The diagram shows a network within the on-premises network connected to the Azure hub VPN gateway over ExpressRoute private peering. The connectivity establishment is straightforward:

- Establish ExpressRoute connectivity with an ExpressRoute circuit and private peering.
- Establish the VPN connectivity.

An important aspect of this configuration is routing between the on-premises networks and Azure over both the ExpressRoute and VPN paths.

Traffic from on-premises networks to Azure

For traffic from on-premises networks to Azure, the Azure prefixes (including the virtual hub and all the spoke virtual networks connected to the hub) are advertised via both the ExpressRoute private peering BGP and the VPN BGP. This results in two network routes (paths) toward Azure from the on-premises networks:

- One over the IPsec-protected path
- One directly over ExpressRoute without IPsec protection

To apply encryption to the communication, you must make sure that for the VPN-connected network in the diagram, the Azure routes via on-premises VPN gateway are preferred over the direct ExpressRoute path.

Traffic from Azure to on-premises networks

The same requirement applies to the traffic from Azure to on-premises networks. To ensure that the IPsec path is preferred over the direct ExpressRoute path (without IPsec), you have two options:

- Advertise more specific prefixes on the VPN BGP session for the VPN-connected network. You can advertise a larger range that encompasses the VPN-connected network over ExpressRoute private peering, then more specific ranges in the VPN BGP session. For example, advertise 10.0.0.0/16 over ExpressRoute, and 10.0.1.0/24 over VPN.
- Advertise disjoint prefixes for VPN and ExpressRoute. If the VPN-connected network ranges are disjoint from other ExpressRoute connected networks, you can advertise the prefixes in the VPN and ExpressRoute BGP sessions, respectively. For example, advertise 10.0.0.0/24 over ExpressRoute, and 10.0.1.0/24 over VPN.

In both examples, Azure will send traffic to 10.0.1.0/24 over the VPN connection rather than directly over ExpressRoute without VPN protection.

[!WARNING]

If you advertise the same prefixes over both ExpressRoute and VPN connections, Azure will use the ExpressRoute path directly without VPN protection.

Design redundancy for an ExpressRoute deployment

There are 2 ways in which redundancy can be planned for an ExpressRoute deployment.

- Configure ExpressRoute and site to site coexisting connections

- Create a zone redundant VNET gateway in Azure Availability zones

Configure ExpressRoute and site to site coexisting connections

This section helps you configure ExpressRoute and Site-to-Site VPN connections that coexist. Having the ability to configure Site-to-Site VPN and ExpressRoute has several advantages. You can configure Site-to-Site VPN as a secure failover path for ExpressRoute or use Site-to-Site VPNs to connect to sites that are not connected through ExpressRoute. Configuring Site-to-Site VPN and ExpressRoute coexisting connections has several advantages:

- You can configure a Site-to-Site VPN as a secure failover path for ExpressRoute.
- Alternatively, you can use Site-to-Site VPNs to connect to sites that are not connected through ExpressRoute.

You can configure either gateway first. Typically, you will incur no downtime when adding a new gateway or gateway connection.

Network Limits and limitations

- **Only route-based VPN gateway is supported.** You must use a route-based VPN gateway. You also can use a route-based VPN gateway with a VPN connection configured for 'policy-based traffic selectors'.
- **The ASN of Azure VPN Gateway must be set to 65515.** Azure VPN Gateway supports the BGP routing protocol. For ExpressRoute and Azure VPN to work together, you must keep the Autonomous System Number of your Azure VPN gateway at its default value, 65515. If you previously selected an ASN other than 65515 and you change the setting to 65515, you must reset the VPN gateway for the setting to take effect.
- **The gateway subnet must be /27 or a shorter prefix,** (such as /26, /25), or you will receive an error message when you add the ExpressRoute virtual network gateway.
- **Coexistence in a dual stack VNet is not supported.** If you are using ExpressRoute IPv6 support and a dual-stack ExpressRoute gateway, coexistence with VPN Gateway will not be possible.

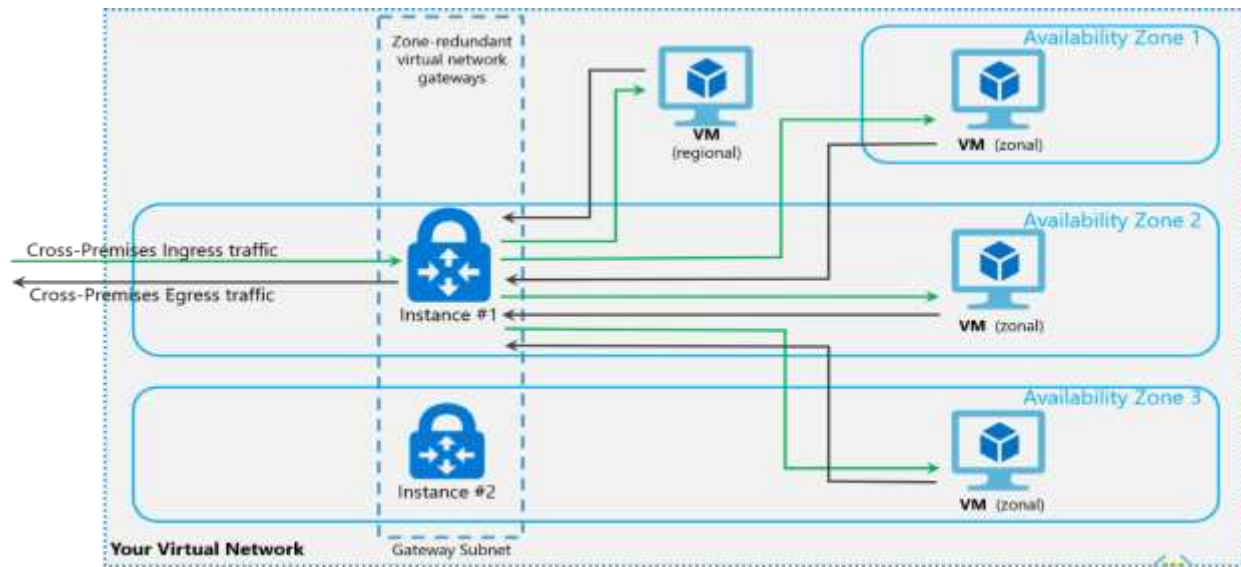
Create a zone redundant VNet gateway in Azure availability zones

You can deploy VPN and ExpressRoute gateways in Azure Availability Zones. This brings resiliency, scalability, and higher availability to virtual network gateways. Deploying

gateways in Azure Availability Zones physically and logically separates gateways within a region, while protecting your on-premises network connectivity to Azure from zone-level failures.

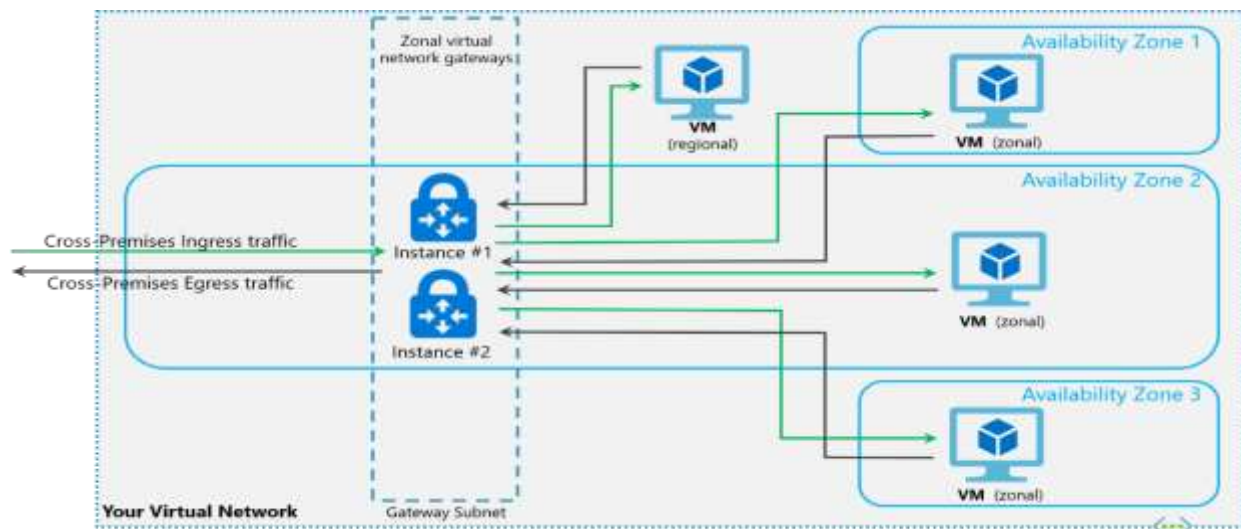
Zone-redundant gateways

To automatically deploy your virtual network gateways across availability zones, you can use zone-redundant virtual network gateways. With zone-redundant gateways, you can benefit from zone-resiliency to access your mission-critical, scalable services on Azure.



Zonal gateways

To deploy gateways in a specific zone, you can use zonal gateways. When you deploy a zonal gateway, all instances of the gateway are deployed in the same Availability Zone.



Gateway SKUs

Zone-redundant and zonal gateways are available as gateway SKUs. There is a new virtual network gateway SKUs in Azure AZ regions. These SKUs are like the corresponding existing SKUs for ExpressRoute and VPN Gateway, except that they are specific to zone-redundant and zonal gateways. You can identify these SKUs by the "AZ" in the SKU name.

Public IP SKUs

Zone-redundant gateways and zonal gateways both rely on the Azure public IP resource Standard SKU. The configuration of the Azure public IP resource determines whether the gateway that you deploy is zone-redundant, or zonal. If you create a public IP resource with a Basic SKU, the gateway will not have any zone redundancy, and the gateway resources will be regional.

- Zone-redundant gateways
 - When you create a public IP address using the **Standard** public IP SKU without specifying a zone, the behavior differs depending on whether the gateway is a VPN gateway, or an ExpressRoute gateway.
 - For a VPN gateway, the two gateway instances will be deployed in any 2 out of these three zones to provide zone-redundancy.
 - For an ExpressRoute gateway, since there can be more than two instances, the gateway can span across all the three zones.
- Zonal gateways
 - When you create a public IP address using the **Standard** public IP SKU and specify the Zone (1, 2, or 3), all the gateway instances will be deployed in the same zone.
- Regional gateways
 - When you create a public IP address using the **Basic** public IP SKU, the gateway is deployed as a regional gateway and does not have any zone-redundancy built into the gateway.

Configure a Site-to-Site VPN as a failover path for ExpressRoute

You can configure a Site-to-Site VPN connection as a backup for ExpressRoute. This connection applies only to virtual networks linked to the Azure private peering path. There is no VPN-based failover solution for services accessible through Azure Microsoft peering. The ExpressRoute circuit is always the primary link. Data flows through the Site-to-Site VPN path only if the ExpressRoute circuit fails. To avoid asymmetrical routing, your local network configuration should also prefer the ExpressRoute circuit over the Site-to-Site

VPN. You can prefer the ExpressRoute path by setting higher local preference for the routes received the ExpressRoute.

Note

If you have ExpressRoute Microsoft Peering enabled, you can receive the public IP address of your Azure VPN gateway on the ExpressRoute connection. To set up your site-to-site VPN connection as a backup, you must configure your on-premises network so that the VPN connection is routed to the Internet.

Note

While ExpressRoute circuit is preferred over Site-to-Site VPN when both routes are the same, Azure will use the longest prefix match to choose the route towards the packet's destination.

Design an ExpressRoute deployment

ExpressRoute enables us to connect on Premises to Azure services seamlessly. lets review some design decisions you will make before deploying an ExpressRoute circuit.

ExpressRoute circuit SKUs

Azure ExpressRoute has three different circuit SKUs: Local, Standard, and Premium. The way you are charged for your ExpressRoute usage varies between these three SKU types.

- **Local SKU** - With Local SKU, you are automatically charged with an Unlimited data plan.
- **Standard and Premium SKU** - You can select between a Metered or an Unlimited data plan. All ingress data are free of charge except when using the Global Reach add-on.

Important

Based on requirements of workloads and data plan, selection of SKU types can help optimize cost and budget.

Explore pricing based on ExpressRoute SKU

SKU models have been discussed previously as Local, Standard and Premium. It is a good practice to estimate costs before using Azure ExpressRoute as the price might affect your design decisions.

Use the Azure pricing calculator to estimate costs before you create an Azure ExpressRoute circuit.

1. On the left, select **Networking**, then select **Azure ExpressRoute** to begin.
2. Select the appropriate Zone depending on your peering location.
3. Then select the SKU, Circuit Speed, and the Data Plan you would like an estimate for.
4. In the Additional outbound data transfer, enter an estimate in GB of how much outbound data you might use over the course of a month.
5. Lastly, you can add the Global Reach Add-on to the estimate.

Choose a peering location

Peering location is of importance when working with ExpressRoute.

Note

Azure regions and ExpressRoute locations are two distinct and different concepts, understanding the difference between the two is critical to exploring Azure hybrid networking connectivity.

Azure regions

Azure regions are global datacenters where Azure compute, networking and storage resources are located. When creating an Azure resource, a customer needs to select a resource location. The resource location determines which Azure datacenter (or availability zone) the resource is created in.

ExpressRoute locations (Peering locations)

ExpressRoute locations (sometimes referred to as peering locations or meet-me-locations) are co-location facilities where Microsoft Enterprise Edge (MSEE) devices are located. ExpressRoute locations are the entry point to Microsoft's network – and are globally distributed, providing customers the opportunity to connect to Microsoft's network around the world. These locations are where ExpressRoute partners and ExpressRoute Direct customers issue cross connections to Microsoft's network. You would

have access to Azure services across all regions within a geopolitical region if you connected to at least one ExpressRoute location within the geopolitical region.

Azure regions to ExpressRoute locations within a geopolitical region.

The following link provides a list of Azure regions to ExpressRoute locations within a geopolitical region. This page is kept up to date with the latest ExpressRoute locations and providers.

ExpressRoute connectivity providers

The following link list's locations by service provider. This page is kept up to date with the latest available providers by location, see Service providers by location.

Connectivity through Exchange providers

If your connectivity provider is not listed in previous sections, you can still create a connection. Several connectivity providers are already connected to Ethernet exchanges.

Connectivity through satellite operators

If you are remote and do not have fiber connectivity or want to explore other connectivity options, you can check the following satellite operators.

Additional Connectivity options:

- Through additional service providers
- Datacenter providers
- National Research and Education networks (NERN)
- System integrators

Choose the right ExpressRoute circuit and billing model

Microsoft offers various Express Route options depending on the desired bandwidth of this private connection between the customer on premises network and the selected Azure region. Typically, enterprises need to evaluate their current usage and determine how much data they use monthly to start with.

The next step is to figure out which of the available ExpressRoute is the best choice depending upon the requirements of the Enterprise keeping in mind the budget and SLA requirements.

When you deploy ExpressRoute, you must choose between the Local, Standard and Premium SKUs. The Standard and Premium SKU are available in a metered version, where you pay per used GB and an unlimited option.

The other option is the ExpressRoute Direct, connecting your network to the closest Microsoft Edge node which then connects to the Microsoft Global Network, to connect

to other customers offices or factories and any Azure Region. The usage of the Microsoft Global Network is charged on top of the ExpressRoute Direct.

Please refer to the Express Route pricing for details on metered and unlimited data plan based on the bandwidth.

You can purchase ExpressRoute circuits for a wide range of bandwidths. The supported bandwidths are listed as follows. Be sure to check with your connectivity provider to determine the bandwidths they support.

50 Mbps
100 Mbps
200 Mbps
500 Mbps
1 Gbps
2 Gbps
5 Gbps
10 Gbps

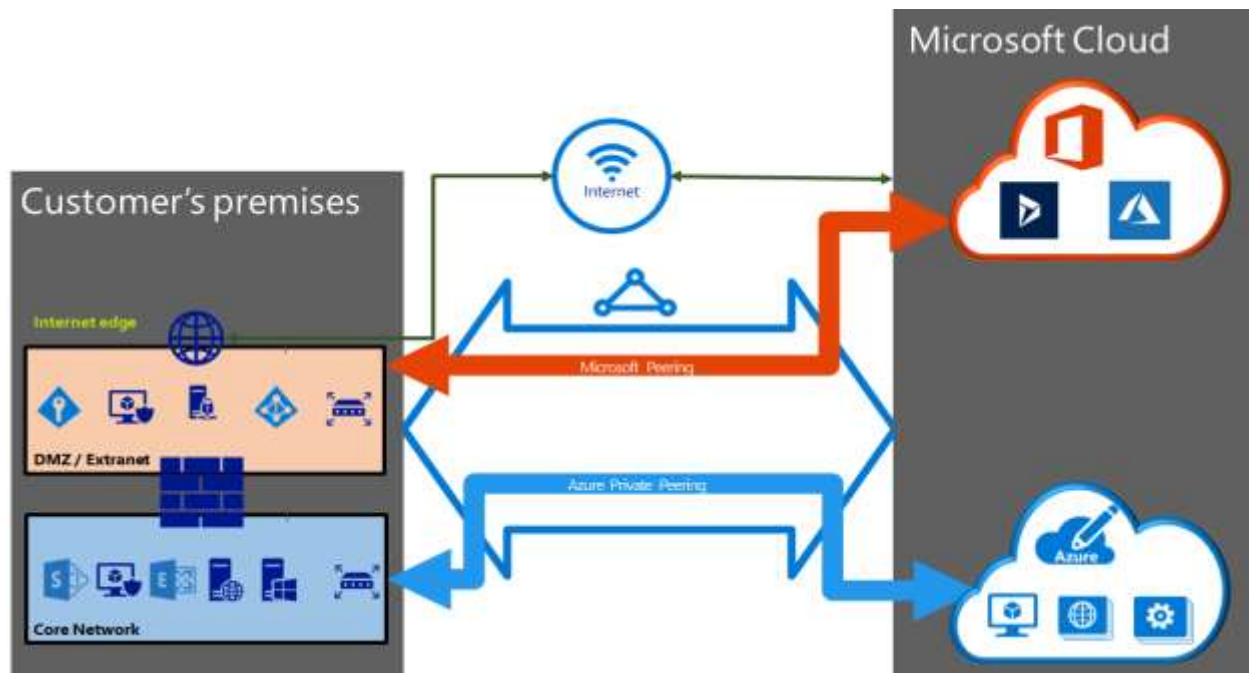
Choose a billing model

You can pick a billing model that works best for you. Choose between the billing models listed as followed.

- **Unlimited data.** Billing is based on a monthly fee; all inbound and outbound data transfer is included free of charge.
- **Metered data.** Billing is based on a monthly fee; all inbound data transfer is free of charge. Outbound data transfer is charged per GB of data transfer. Data transfer rates vary by region.
- **ExpressRoute premium add-on.** ExpressRoute premium is an add-on to the ExpressRoute circuit. The ExpressRoute premium add-on provides the following capabilities:
 - Increased route limits for Azure public and Azure private peering from 4,000 routes to 10,000 routes.
 - Global connectivity for services. An ExpressRoute circuit created in any region (excluding national clouds) will have access to resources across every other region in the world. For example, a virtual network created in West Europe can be accessed through an ExpressRoute circuit provisioned in Silicon Valley.
 - Increased number of VNet links per ExpressRoute circuit from 10 to a larger limit, depending on the bandwidth of the circuit.

Configure peering for an ExpressRoute deployment

An ExpressRoute circuit has two peering options associated with it: Azure private, and Microsoft. Each peering is configured identically on a pair of routers (in active-active or load sharing configuration) for high availability. Azure services are categorized as Azure public and Azure private to represent the IP addressing schemes.



Create Peering configuration

- You can configure private peering and Microsoft peering for an ExpressRoute circuit. Peering's can be configured in any order you choose. However, you must make sure that you complete the configuration of each peering one at a time.
- You must have an active ExpressRoute circuit. Have the circuit enabled by your connectivity provider before you continue. To configure peering(s), the ExpressRoute circuit must be in a provisioned and enabled state.
- If you plan to use a shared key/MD5 hash, be sure to use the key on both sides of the tunnel. The limit is a maximum of 25 alphanumeric characters. Special characters are not supported.

- This only applies to circuits created with service providers offering Layer 2 connectivity services. If you are using a service provider that offers managed Layer 3 services (typically an IPVPN, like MPLS), your connectivity provider configures and manages the routing for you.

Choose between private peering only, Microsoft peering only, or both

The following table compares the two peering. Public peering is deprecated for new peering.

Features	Private Peering	Microsoft Peering
Max. # prefixes supported per peering	4000 by default, 10,000 with ExpressRoute Premium	200
IP address ranges supported	Any valid IP address within your WAN.	Public IP addresses owned by you or your connectivity provider.
AS Number requirements	Private and public AS numbers. You must own the public AS number if you choose to use one.	Private and public AS numbers. However, you must prove ownership of public IP addresses.
IP protocols supported	IPv4, IPv6 (preview)	IPv4, IPv6
Routing Interface IP addresses	RFC1918 and public IP addresses	Public IP addresses registered to you in routing registries.
MD5 Hash support	Yes	Yes

You may enable one or more of the routing domains as part of your ExpressRoute circuit. You can choose to have all the routing domains put on the same VPN if you want to combine them into a single routing domain. The recommended configuration is that private peering is connected directly to the core network, and the public and Microsoft peering links are connected to your DMZ.

Each peering requires separate BGP sessions (one pair for each peering type). The BGP session pairs provide a highly available link. If you are connecting through layer 2 connectivity providers, you are responsible for configuring and managing routing.

Important

IPv6 support for private peering is currently in Public Preview. If you would like to connect your virtual network to an ExpressRoute circuit with IPv6-based private peering

configured, please make sure that your virtual network is dual stack and follows the guidelines for **IPv6 for Azure VNet**.

Configure private peering

Azure compute services, namely virtual machines (IaaS) and cloud services (PaaS), that are deployed within a virtual network can be connected through the private peering domain. The private peering domain is a trusted extension of your core network into Microsoft Azure. You can set up bi-directional connectivity between your core network and Azure virtual networks (VNets). This peering lets you connect to virtual machines and cloud services directly on their private IP addresses.

You can connect more than one virtual network to the private peering domain. You can visit the [Azure Subscription and Service Limits, Quotas, and Constraints](#) page for up-to-date information on limits.

Configure Microsoft peering

Microsoft 365 was created to be accessed securely and reliably via the Internet. Because of this, it is recommended to use ExpressRoute for specific scenarios.

Connectivity to Microsoft online services (Microsoft 365 and Azure PaaS services) occurs through Microsoft peering. You can enable bidirectional connectivity between your WAN and Microsoft cloud services through the Microsoft peering routing domain. You must connect to Microsoft cloud services only over public IP addresses that are owned by you or your connectivity provider and you must adhere to all the defined rules.

Configure route filters for Microsoft Peering

Route filters are a way to consume a subset of supported services through Microsoft peering.

Microsoft 365 services such as Exchange Online, SharePoint Online, and Skype for Business, are accessible through the Microsoft peering. When Microsoft peering gets configured in an ExpressRoute circuit, all prefixes related to these services gets advertised through the BGP sessions that are established. A BGP community value is attached to every prefix to identify the service that is offered through the prefix.

Connectivity to all Azure and Microsoft 365 services causes many prefixes to get advertised through BGP. The large number of prefixes significantly increases the size of the route tables maintained by routers within your network. If you plan to consume only

a subset of services offered through Microsoft peering, you can reduce the size of your route tables in two ways. You can:

- Filter out unwanted prefixes by applying route filters on BGP communities. Route filtering is a standard networking practice and is used commonly within many networks.
- Define route filters and apply them to your ExpressRoute circuit. A route filter is a new resource that lets you select the list of services you plan to consume through Microsoft peering. ExpressRoute routers only send the list of prefixes that belong to the services identified in the route filter.

About route filters

When Microsoft peering gets configured on your ExpressRoute circuit, the Microsoft Edge routers establish a pair of BGP sessions with your edge routers through your connectivity provider. No routes are advertised to your network. To enable route advertisements to your network, you must associate a route filter.

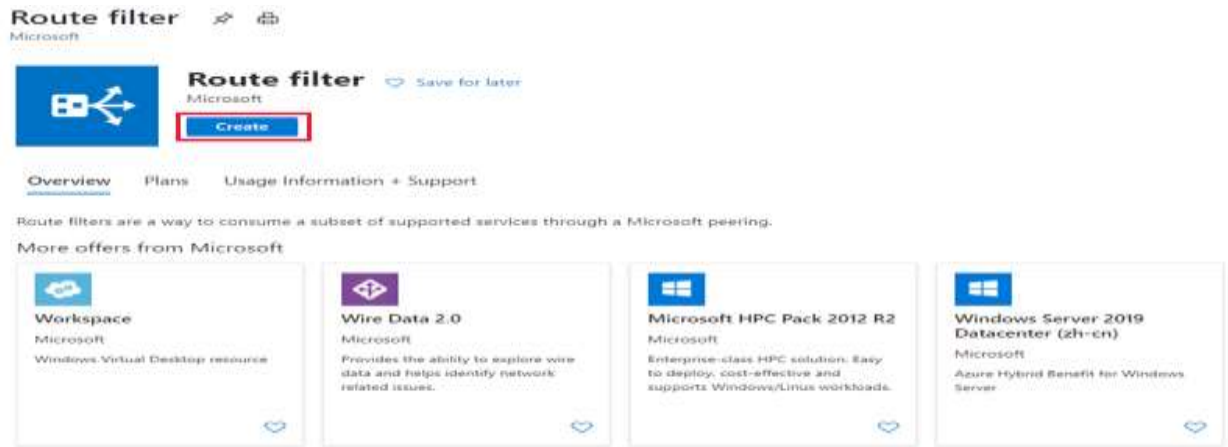
A route filter lets you identify services you want to consume through your ExpressRoute circuit's Microsoft peering. It is essentially an allowed list of all the BGP community values. Once a route filter resource gets defined and attached to an ExpressRoute circuit, all prefixes that map to the BGP community values gets advertised to your network.

To attach route filters with Microsoft 365 services, you must have authorization to consume Microsoft 365 services through ExpressRoute. If you are not authorized to consume Microsoft 365 services through ExpressRoute, the operation to attach route filters fails.

Create a route filter and a filter rule

A route filter can have only one rule, and the rule must be of type 'Allow'. This rule can have a list of BGP community values associated with it.

- Select **Create a resource** then search for Route filter as shown in the following image:



- Place the route filter in a resource group. Ensure the location is the same as the ExpressRoute circuit. Select **Review + create** and then **Create**.

Create route filter

Basics | Tags | Review + create

Route filters help you filter the traffic going through your ExpressRoute. Essentially a white list of all the BGP community values, a route filter lets you identify services you want to consume through your ExpressRoute circuit's Microsoft peering. Once a route filter resource is defined and attached to an ExpressRoute circuit, all prefixes that map to the BGP community values are advertised to your network. [Learn more about route filters](#)

Project details

Subscription * ⓘ Azure Subscription

Resource group * ⓘ ExpressRouteResourceGroup
[Create new](#)

Instance details

Name * MyRouteFilter ✓

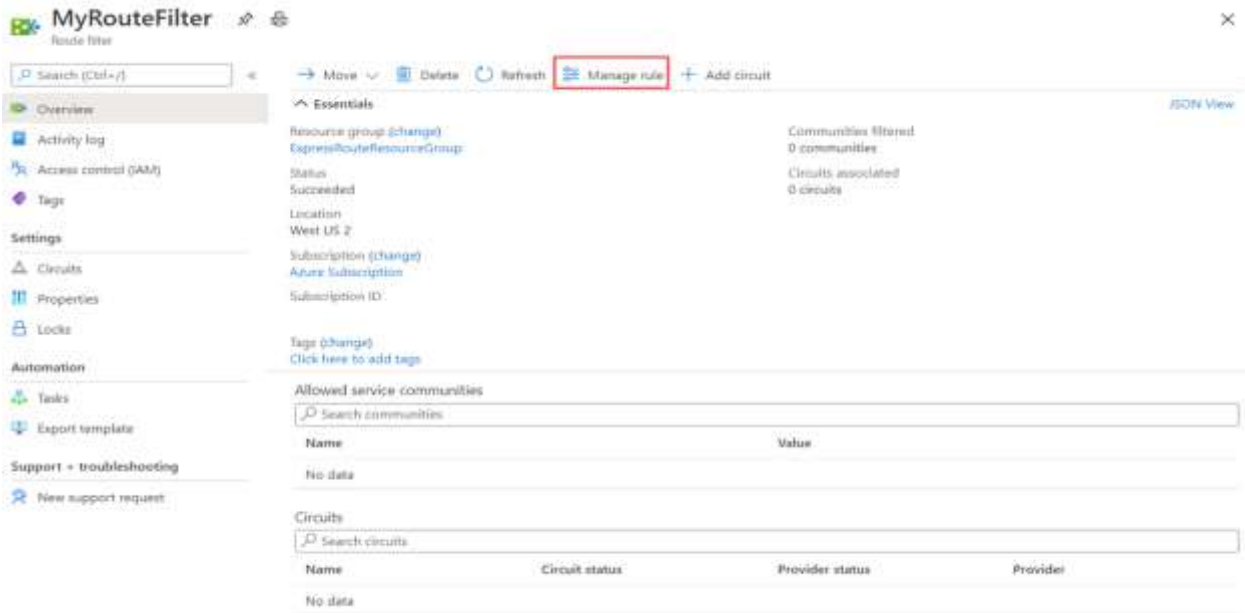
Region * (US) West US 2 ✓

Route filter must be created in the same location as the ExpressRoutes it will be associated with.


Review + create < Previous Next : Tags > [Download a template for automation](#)



Create a filter rule

To add and update rules, select the manage rule tab for your route filter.



- Select the services you want to connect to from the drop-down list and save the rule when done.

 **Manage rule** ×
MyRouteFilter

 Save  Discard

Rule name *

Rule1 ✓

Allowed service communities *

2 selected ^

☒ Select all

☐ Exchange (12076:5010)

☒ Other Office 365 Services (12076:510)

☒ SharePoint Online (12076:5020)

☐ Skype For Business (12076:5030)

☐ CRM Online (12076:5040)

☐ Azure Active Directory (12076:5060)

☐ Azure Australia Central (12076:51032)

☐ Azure Australia Central 2 (12076:510)

☐ Azure Australia East (12076:51015)

☐ Azure Australia Southeast (12076:51016)

☐ Azure Brazil South (12076:51014)

☐ Azure Canada Central (12076:51020)

☐ Azure Canada East (12076:51021)

☐ Azure Central India (12076:51017)

☐ Azure Central US (12076:51009)

☐ Azure Central US EUAP (12076:51009)

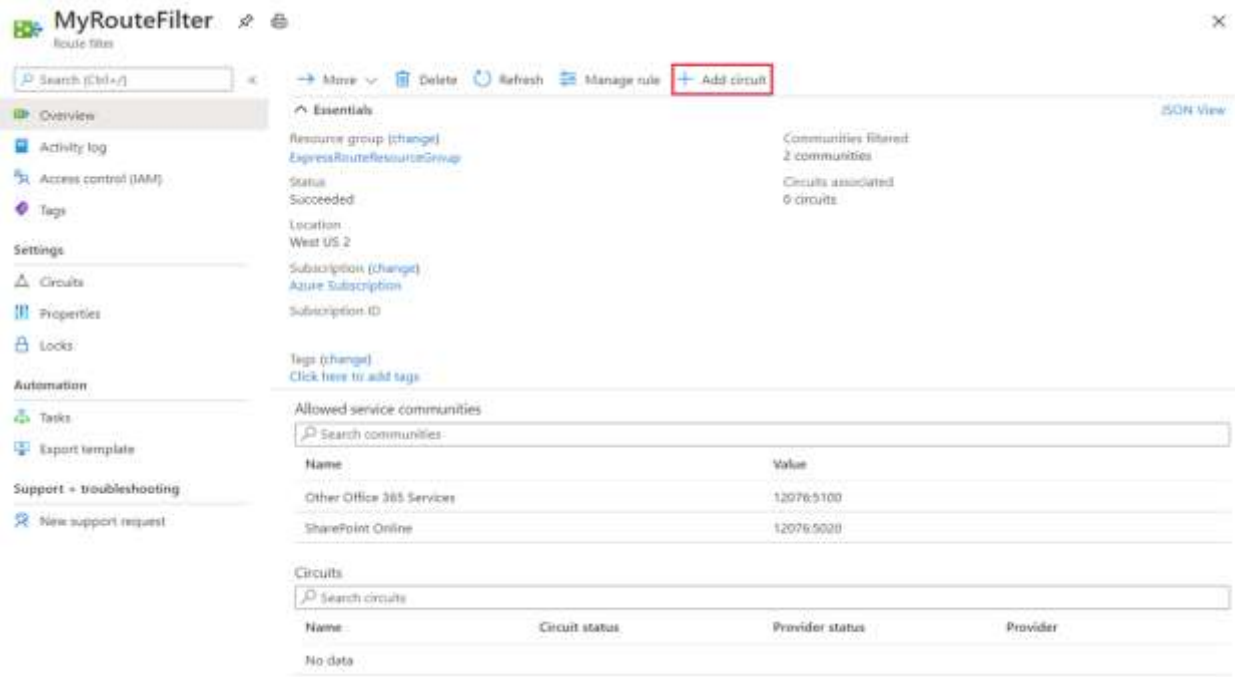
☐ Azure East Asia (12076:51010)

☐ Azure East US (12076:51004)

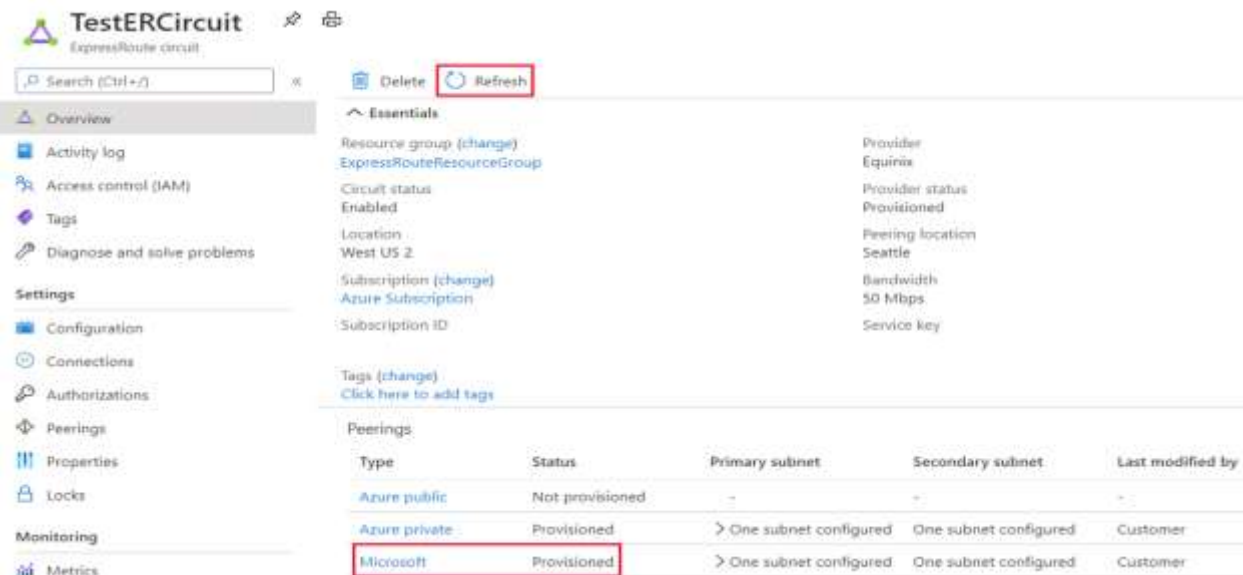
☐ Azure East US 2 (12076:51005)

Attach the route filter to an ExpressRoute circuit

- Attach the route filter to a circuit by selecting the **+ Add Circuit** button and selecting the ExpressRoute circuit from the drop-down list.



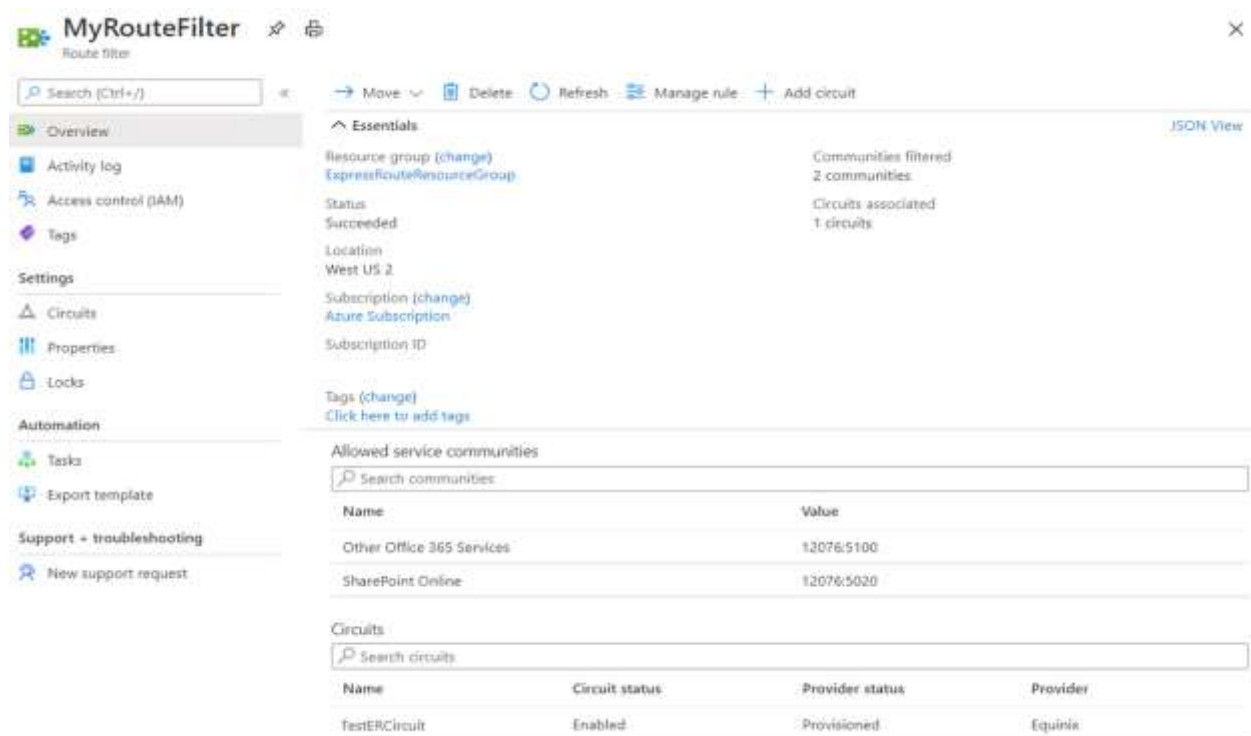
- If the connectivity provider configures peering for your ExpressRoute circuit, refresh the circuit from the ExpressRoute circuit page before you select the **+ Add Circuit** button.



Common tasks

To get the properties of a route filter

- You can view properties of a route filter when you open the resource in the portal.



MyRouteFilter Route filter

Search (Ctrl+/) Move Delete Refresh Manage rule Add circuit

Overview

Activity log Access control (IAM) Tags

Settings

Circuits Properties Locks

Automation

Tasks Export template

Support + troubleshooting

New support request

Essentials

Resource group (change) ExpressRouteResourceGroup

Status Succeeded

Location West US 2

Subscription (change) Azure Subscription

Subscription ID

Tags (change) Click here to add tags

Communities filtered 2 communities

Circuits associated 1 circuits

Allowed service communities

Search communities

Name	Value
Other Office 365 Services	12076:5100
SharePoint Online	12076:5020

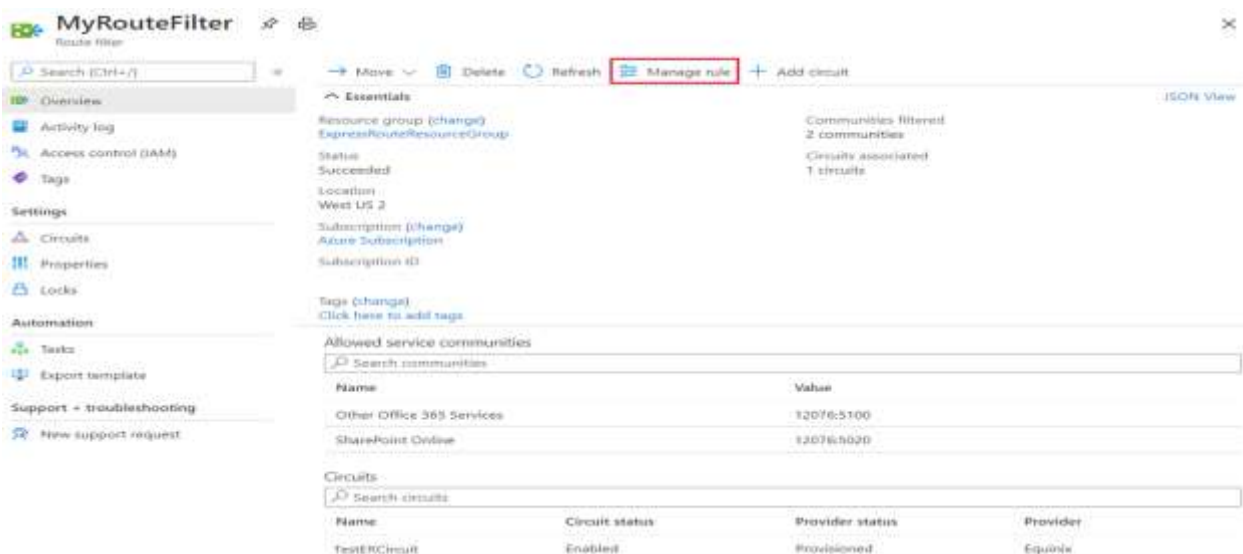
Circuits

Search circuits

Name	Circuit status	Provider status	Provider
TestERCircuit	Enabled	Provisioned	Equinix

To update the properties of a route filter

You can update the list of BGP community values attached to a circuit by selecting the **Manage rule** button.



MyRouteFilter Route filter

Search (Ctrl+/) Move Delete Refresh Manage rule Add circuit

Overview

Activity log Access control (IAM) Tags

Settings

Circuits Properties Locks

Automation

Tasks Export template

Support + troubleshooting

New support request

Essentials

Resource group (change) ExpressRouteResourceGroup

Status Succeeded

Location West US 2

Subscription (change) Azure Subscription

Subscription ID

Tags (change) Click here to add tags

Communities filtered 2 communities

Circuits associated 1 circuits

Allowed service communities

Search communities

Name	Value
Other Office 365 Services	12076:5100
SharePoint Online	12076:5020

Circuits

Search circuits

Name	Circuit status	Provider status	Provider
TestERCircuit	Enabled	Provisioned	Equinix

- Select the service communities you want and then select **Save**.

Manage rule ×

MyRouteFilter

 Save  Discard

Rule name *

Rule1 

Allowed service communities *

2 selected 

-
- ☒ Select all
 - ☐ Exchange (12076:5010)
 - ☒ Other Office 365 Services (12076:510)
 - ☒ SharePoint Online (12076:5020)
 - ☐ Skype For Business (12076:5030)
 - ☐ CRM Online (12076:5040)
 - ☐ Azure Active Directory (12076:5060)
 - ☐ Azure Australia Central (12076:51032)
 - ☐ Azure Australia Central 2 (12076:510)
 - ☐ Azure Australia East (12076:51015)
 - ☐ Azure Australia Southeast (12076:51016)
 - ☐ Azure Brazil South (12076:51014)
 - ☐ Azure Canada Central (12076:51020)
 - ☐ Azure Canada East (12076:51021)
 - ☐ Azure Central India (12076:51017)
 - ☐ Azure Central US (12076:51009)
 - ☐ Azure Central US EUAP (12076:51009)
 - ☐ Azure East Asia (12076:51010)
 - ☐ Azure East US (12076:51004)
 - ☐ Azure East US 2 (12076:51005)

To detach a route filter from an ExpressRoute circuit

- To detach a circuit from the route filter, right-click on the circuit and select **Disassociate**.

The screenshot shows the 'MyRouteFilter' page in the Azure portal. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Settings (Circuits, Properties, Locks), Automation (Tasks, Export template), and Support + troubleshooting. The main content area displays the 'Essentials' section for the route filter, including Resource group (ExpressRouteResourceGroup), Status (Succeeded), Location (West US 2), Subscription (Azure Subscription), and Subscription ID. It also shows 'Allowed service communities' with a table listing 'Other Office 365 Services' and 'SharePoint Online'. Below this, the 'Circuits' section shows a table with one circuit: 'Test@Circuit' with status 'Enabled' and provider 'Equinix'. A red box highlights the 'Disassociate' button next to this circuit.

Name	Circuit status	Provider status	Provider
Test@Circuit	Enabled	Provisioned	Equinix

Clean up resources

- You can delete a route filter by selecting the **Delete** button. Ensure the Route filter is not associate to any circuits before doing so.

This screenshot shows the 'MyRouteFilter' page after the circuit has been disassociated. The 'Delete' button in the top toolbar is highlighted with a red box. In the 'Circuits' section, the table now shows 'No data'. Additionally, the 'Circuits associated' count in the 'Essentials' summary has changed from 1 to 0, also highlighted with a red box.

Name	Circuit status	Provider status	Provider
No data			

Reset peering

Sign into the Azure portal

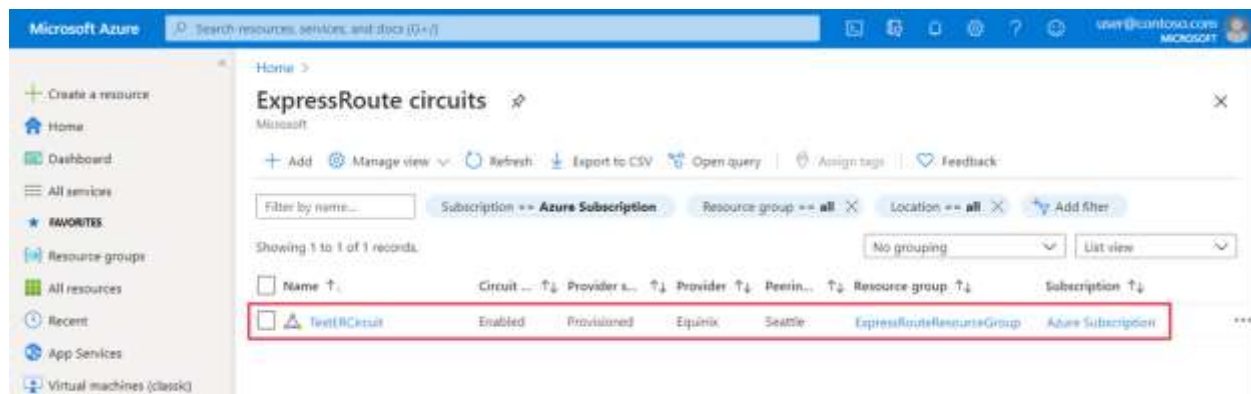
From a browser, go to the Azure portal, and then sign in with your Azure account.

Reset a peering

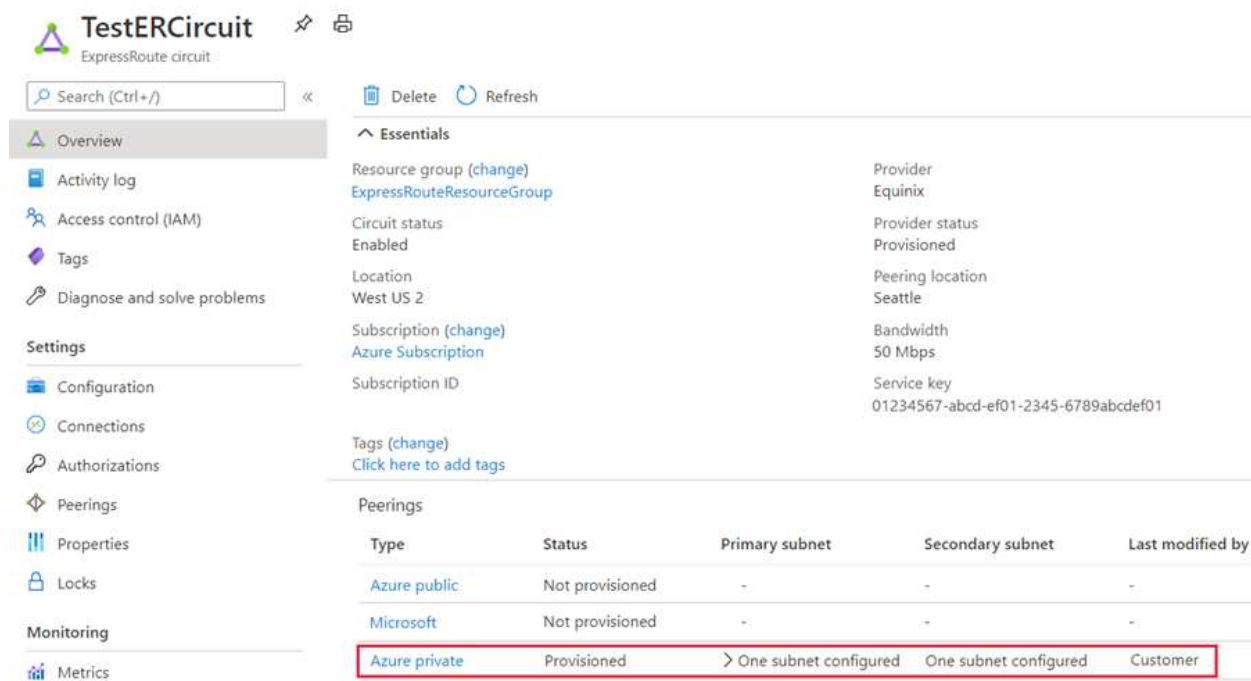
You can reset the Microsoft peering and the Azure private peering on an ExpressRoute circuit independently.

- Choose the circuit that you want to change.

-



- Choose the peering configuration that you want to reset.



- Clear the **Enable Peering** check box, and then select **Save** to disable the peering configuration.

Private peering TestERCircuit

☐ Enable Peering ⓘ

Peer ASN ⓘ
65020

Subnets
☐ Both
☒ IPv4
☐ IPv6

IPv4 Primary subnet ⓘ
192.168.11.16/30

IPv4 Secondary subnet ⓘ
192.168.11.20/30

VLAN ID ⓘ
110

Shared key

☐ Enable Global Reach ⓘ

Save Cancel

- Select the **Enable Peering** check box, and then select **Save** to re-enable the peering configuration.

Connect an ExpressRoute circuit to a virtual network

An ExpressRoute circuit represents a logical connection between your on-premises infrastructure and Microsoft cloud services through a connectivity provider. You can order multiple ExpressRoute circuits. Each circuit can be in the same or different regions and can be connected to your premises through different connectivity providers. ExpressRoute circuits do not map to any physical entities. A circuit is uniquely identified by a standard GUID called as a service key (s-key).

In the previous exercises you created an ExpressRoute Gateway and an ExpressRoute circuit. You then learned how to configure peering for an express route circuit. You will

now learn how to create a connection between your ExpressRoute circuit and Azure virtual network.

Connect a virtual network to an ExpressRoute circuit

- You must have an active ExpressRoute circuit.
- Ensure that you have Azure private peering configured for your circuit.
- Ensure that Azure private peering gets configured and establishes BGP peering between your network and Microsoft for end-to-end connectivity.
- Ensure that you have a virtual network and a virtual network gateway created and fully provisioned. A virtual network gateway for ExpressRoute uses the GatewayType 'ExpressRoute', not VPN.
- You can link up to 10 virtual networks to a standard ExpressRoute circuit. All virtual networks must be in the same geopolitical region when using a standard ExpressRoute circuit.
- A single VNet can be linked to up to 16 ExpressRoute circuits. Use the following process to create a new connection object for each ExpressRoute circuit you are connecting to. The ExpressRoute circuits can be in the same subscription, different subscriptions, or a mix of both.
- If you enable the ExpressRoute premium add-on, you can link virtual networks outside of the geopolitical region of the ExpressRoute circuit. The premium add-on will also allow you to connect more than 10 virtual networks to your ExpressRoute circuit depending on the bandwidth chosen.
- To create the connection from the ExpressRoute circuit to the target ExpressRoute virtual network gateway, the number of address spaces advertised from the local or peered virtual networks needs to be equal to or less than **200**. Once the connection has been successfully created, you can add additional address spaces, up to 1,000, to the local or peered virtual networks.

Add a VPN to an ExpressRoute deployment

This section helps you configure secure encrypted connectivity between your on-premises network and your Azure virtual networks (VNets) over an ExpressRoute private connection. You can use Microsoft peering to establish a site-to-site IPsec/IKE VPN tunnel between your selected on-premises networks and Azure VNets. Configuring a secure tunnel over ExpressRoute allows for data exchange with confidentiality, anti-replay, authenticity, and integrity.

Note

When you set up site-to-site VPN over Microsoft peering, you are charged for the VPN gateway and VPN egress.

For high availability and redundancy, you can configure multiple tunnels over the two MSEE-PE pairs of an ExpressRoute circuit and enable load balancing between the tunnels. VPN tunnels over Microsoft peering can be terminated either using VPN gateway or using an appropriate Network Virtual Appliance (NVA) available through Azure Marketplace. You can exchange routes statically or dynamically over the encrypted tunnels without exposing the route exchange to the underlying Microsoft peering. In this section, BGP (different from the BGP session used to create the Microsoft peering) is used to dynamically exchange prefixes over the encrypted tunnels.

Important

For the on-premises side, typically Microsoft peering is terminated on the DMZ and private peering is terminated on the core network zone. The two zones would be segregated using firewalls. If you are configuring Microsoft peering exclusively for enabling secure tunneling over ExpressRoute, remember to filter through only the public IPs of interest that are getting advertised via Microsoft peering.

Steps

- Configure Microsoft peering for your ExpressRoute circuit.
- Advertise selected Azure regional public prefixes to your on-premises network via Microsoft peering.
- Configure a VPN gateway and establish IPsec tunnels
- Configure the on-premises VPN device.
- Create the site-to-site IPsec/IKE connection.
- (Optional) Configure firewalls/filtering on the on-premises VPN device.
- Test and validate the IPsec communication over the ExpressRoute circuit.
-

Connect geographically dispersed networks with ExpressRoute global reach

Use cross-region connectivity to link multiple ExpressRoute locations

There are various ways of designing and implementing ExpressRoute based on specific organizational requirements.

ExpressRoute connections enable access to the following services:

- Microsoft Azure services
- Microsoft 365 services

Connectivity to all regions within a geopolitical region

You can connect to Microsoft in one of the peering locations and access regions within the geopolitical region.

For example, if you connect to Microsoft in Amsterdam through ExpressRoute, you will have access to all Microsoft cloud services hosted in Northern and Western Europe.

Global connectivity with ExpressRoute Premium

You can enable ExpressRoute Premium to extend connectivity across geopolitical boundaries. For example, if you connect to Microsoft in Amsterdam through ExpressRoute, you will have access to all Microsoft cloud services hosted in all regions across the world. You can also access services deployed in South America or Australia the same way you access North and West Europe regions. National clouds are excluded.

Local connectivity with ExpressRoute Local

You can transfer data cost-effectively by enabling the Local SKU. With Local SKU, you can bring your data to an ExpressRoute location near the Azure region you want. With Local, Data transfer is included in the ExpressRoute port charge.

Across on-premises connectivity with ExpressRoute Global Reach

You can enable ExpressRoute Global Reach to exchange data across your on-premises sites by connecting your ExpressRoute circuits. For example, if you have a private data center in California connected to an ExpressRoute circuit in Silicon Valley and another private data center in Texas connected to an ExpressRoute circuit in Dallas. With ExpressRoute Global Reach, you can connect your private data centers together through these two ExpressRoute circuits. Your cross-data-center traffic will traverse through Microsoft's network.

Rich connectivity partner ecosystem

ExpressRoute has a constantly growing ecosystem of connectivity providers and systems integrator partners. You can refer to ExpressRoute partners and peering locations.

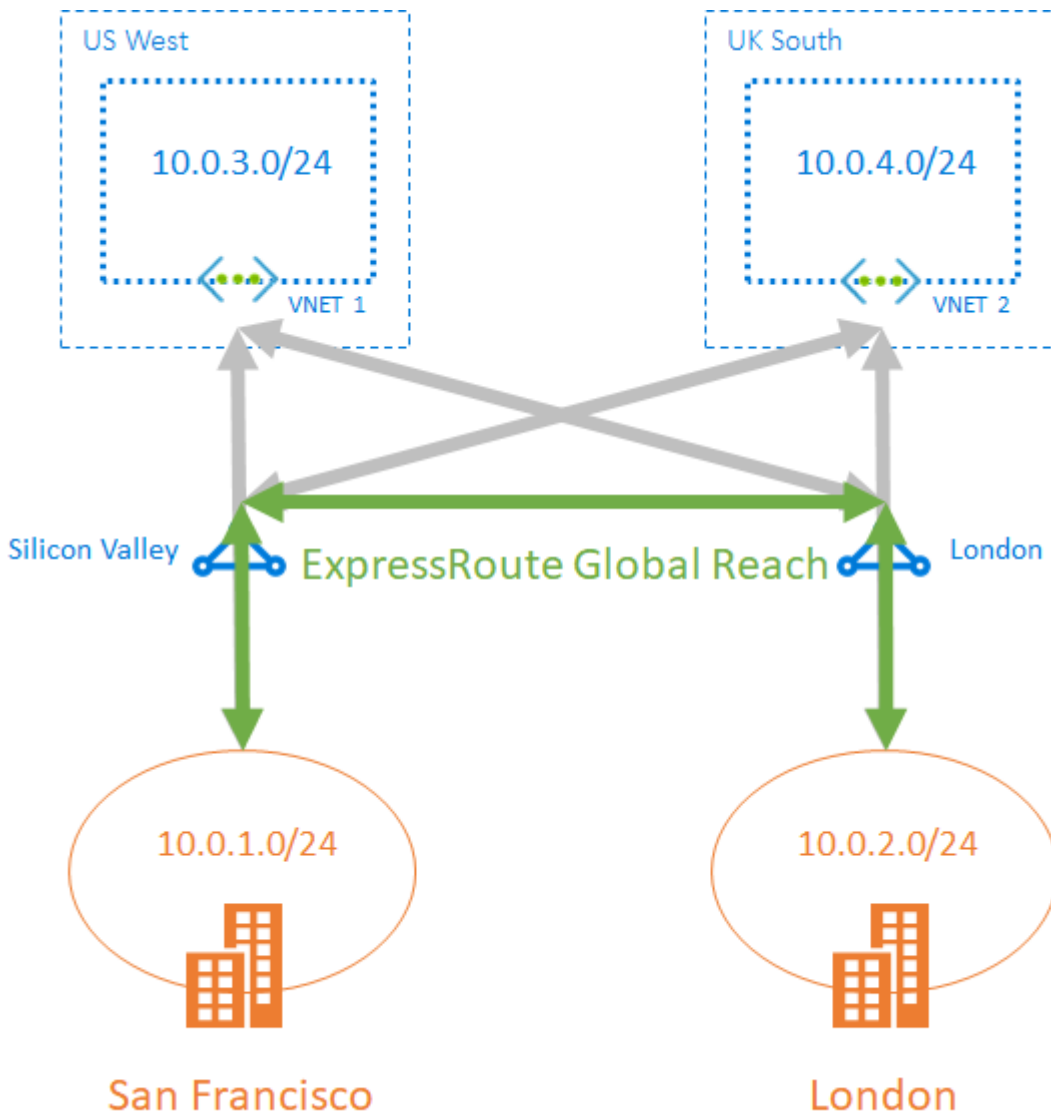
Connectivity to national clouds

Microsoft operates isolated cloud environments for special geopolitical regions and customer segments.

ExpressRoute Direct

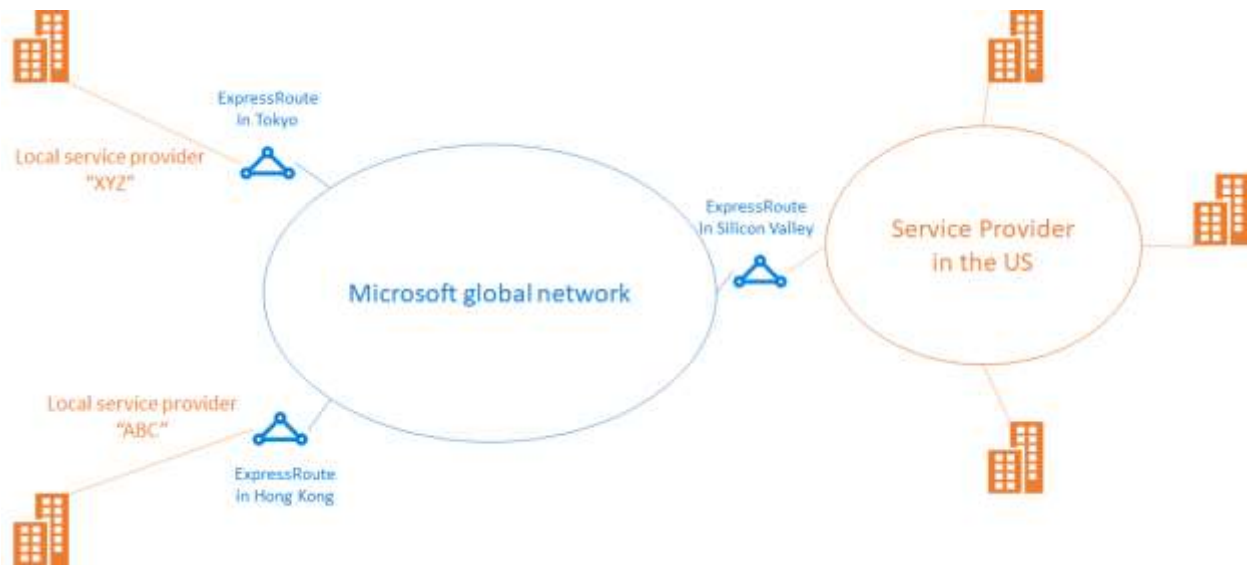
ExpressRoute Direct provides customers the opportunity to connect directly into Microsoft's global network at peering locations strategically distributed across the world. ExpressRoute Direct provides dual 100-Gbps connectivity, which supports Active/Active connectivity at scale.

ExpressRoute is a private and resilient way to connect your on-premises networks to the Microsoft Cloud. You can access many Microsoft cloud services such as Azure and Microsoft 365 from your private data center or your corporate network. For example, you may have a branch office in San Francisco with an ExpressRoute circuit in Silicon Valley and another branch office in London with an ExpressRoute circuit in the same city. Both branch offices have high-speed connectivity to Azure resources in US West and UK South. However, the branch offices cannot connect and send data directly with one another. In other words, 10.0.1.0/24 can send data to 10.0.3.0/24 and 10.0.4.0/24 network, but NOT to 10.0.2.0/24 network.



Choose when to use ExpressRoute global reach

ExpressRoute Global Reach is designed to complement your service provider's WAN implementation and connect your branch offices across the world. For example, if your service provider primarily operates in the United States and has linked all your branches in the U.S., but the service provider does not operate in Japan and Hong Kong SAR, with ExpressRoute Global Reach you can work with a local service provider and Microsoft will connect your branches there to the ones in the U.S. using ExpressRoute and the Microsoft global network.



Configure ExpressRoute global reach

These steps show you how to configure ExpressRoute Global Reach using Azure portal.

Before you begin

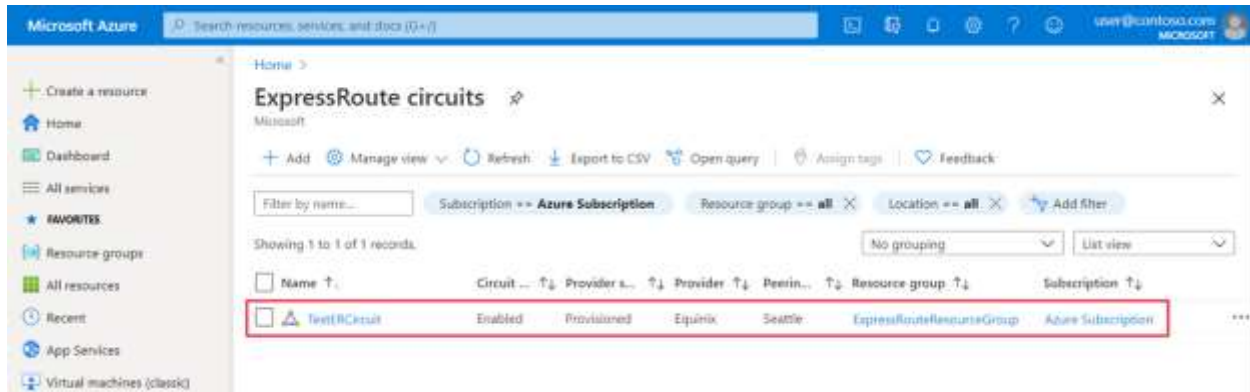
Before you start configuration, confirm the following criteria:

- You understand ExpressRoute circuit provisioning workflows.
- Your ExpressRoute circuits are in a provisioned state.
- Azure private peering is configured on your ExpressRoute circuits.
- If you want to run PowerShell locally, verify that the latest version of Azure PowerShell is installed on your computer.

Identify circuits

Identify the ExpressRoute circuits that you want use. You can enable ExpressRoute Global Reach between the private peering of any two ExpressRoute circuits, if they are in the supported countries/regions. The circuits are required to be created at different peering locations.

- If your subscription owns both circuits, you can choose either circuit to run the configuration in the following sections.
- If the two circuits are in different Azure subscriptions, you need authorization from one Azure subscription. Then you pass in the authorization key when you run the configuration command in the other Azure subscription.

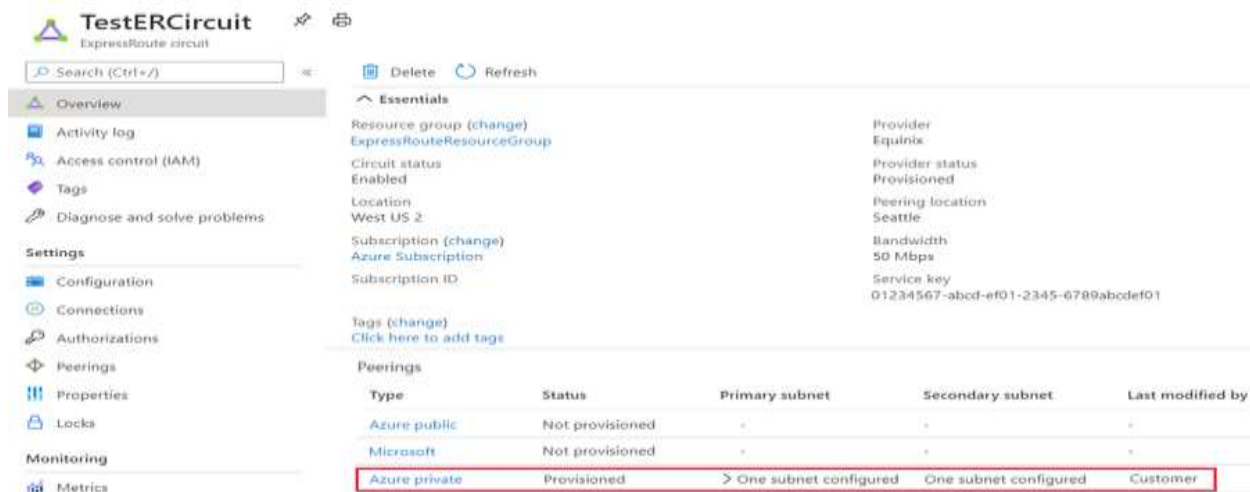


Enable connectivity

Enable connectivity between your on-premises networks. There are separate sets of instructions for circuits that are in the same Azure subscription, and circuits that are different subscriptions.

ExpressRoute circuits in the same Azure subscription

1. Select the **Azure private** peering configuration.



2. Select **Add Global Reach** to open the Add Global Reach configuration page.

Private peering

☒ Enable Peering ⓘ

Peer ASN * ⓘ

65020 ✓

IPv4 Primary subnet * ⓘ

192.168.11.16/30

IPv4 Secondary subnet * ⓘ

192.168.11.20/30

VLAN ID * ⓘ

110 ✓

Shared key

Add Global Reach

Global Reach name

ExpressRoute Circuit name ⓘ

Global Reach subnet ⓘ

Save

Cancel

- On the Add Global Reach configuration page, give a name to this configuration. Select the ExpressRoute circuit you want to connect this circuit to and enter in a **/29 IPv4** for the Global Reach subnet. Azure uses IP addresses in this subnet to establish connectivity between the two ExpressRoute circuits. Do not use the addresses in this subnet in your Azure virtual networks, or in your on-premises network. Select **Add** to add the circuit to the private peering configuration.

Add Global Reach



TestERCircuit

Global Reach name *

TestERCircuit1-TestERCircuit2



☐ Redeem authorization ⓘ

ExpressRoute circuit * ⓘ

TestERCircuit2

resourceGroup: ExpressRouteResourceGroup2, location: eastus



Global Reach subnet * ⓘ

192.168.11.24/29



Add

Cancel

4. Select **Save** to complete the Global Reach configuration. When the operation completes, you will have connectivity between your two on-premises networks through both ExpressRoute circuits.



Private peering



TestERCircuit

☒ Enable Peering ⓘ

Peer ASN * ⓘ

65020



IPv4 Primary subnet * ⓘ

192.168.11.16/30

IPv4 Secondary subnet * ⓘ

192.168.11.20/30

VLAN ID * ⓘ

110



Shared key

Add Global Reach

Global Reach name

ExpressRoute Circuit name ⓘ

Global Reach subnet ⓘ

TestERCircuit1-TestERCirc...

TestERCircuit2

192.168.11.24/29







Save

Cancel

Verify the configuration

Verify the Global Reach configuration by selecting Private peering under the ExpressRoute circuit configuration. When configured correctly your configuration should look as followed:

 **Private peering**   

TestERCircuit

Peer ASN * ⓘ
65020 ✓

IPv4 Primary subnet * ⓘ
192.168.20.16/30 ✓


IPv4 Secondary subnet * ⓘ
192.168.20.20/30 ✓

☒ Enable IPv4 Peering ⓘ

VLAN ID * ⓘ
200 ✓

Shared key


Add Global Reach

Global Reach name	ExpressRoute Circuit name ⓘ	IPv4 Subnet ⓘ	IPv6 Subnet ⓘ	
TestERCircuit1-TestE...	TestERCircuit2 (ER...	192.168.11.24/29		

Save Cancel

Disable connectivity

To disable connectivity between an individual circuit, select the delete button next to the Global Reach name to remove connectivity between them. Then select **Save** to complete the operation.


Private peering
TestERCircuit
✎
🖨
✕

Peer ASN * ⓘ
✓

Subnets

☐ Both
☒ IPv4
☐ IPv6

IPv4 Primary subnet * ⓘ
✓


IPv4 Secondary subnet * ⓘ
✓

☒ Enable IPv4 Peering ⓘ

VLAN ID * ⓘ
✓

Shared key

Add Global Reach

Global Reach name	ExpressRoute Circuit name ⓘ	IPv4 Subnet ⓘ	IPv6 Subnet ⓘ
TestERCircuit1-TestE...	ASH-Cust20-ER (AS...	192.168.11.24/29	

Save

Cancel

Improve data path performance between networks with ExpressRoute FastPath

ExpressRoute virtual network gateway is designed to exchange network routes and route network traffic. FastPath is designed to improve the data path performance between your on-premises network and your virtual network. When enabled, FastPath sends network traffic directly to virtual machines in the virtual network, bypassing the gateway.

Circuits

FastPath is available on all ExpressRoute circuits.

Gateways

FastPath still requires a virtual network gateway to be created to exchange routes between virtual network and on-premises network.

Gateway requirements for ExpressRoute FastPath

To configure FastPath, the virtual network gateway must be either:

- Ultra-Performance
- ErGw3AZ

Important

If you plan to use FastPath with IPv6-based private peering over ExpressRoute, make sure to select ErGw3AZ for SKU. Note that this is only available for circuits using ExpressRoute Direct.

Limitations

While FastPath supports most configurations, it does not support the following features:

- UDR on the gateway subnet: This UDR has no impact on the network traffic that FastPath sends directly from your on-premises network to the virtual machines in Azure virtual network.
- VNet Peering: If you have other virtual networks peered with the one that is connected to ExpressRoute, the network traffic from your on-premises network to the other virtual networks (i.e., the so-called "Spoke" VNets) will continue to be sent to the virtual network gateway. The workaround is to connect all the virtual networks to the ExpressRoute circuit directly.
- Basic Load Balancer: If you deploy a Basic internal load balancer in your virtual network or the Azure PaaS service you deploy in your virtual network uses a Basic internal load balancer, the network traffic from your on-premises network to the virtual IPs hosted on the Basic load balancer will be sent to the virtual network gateway. The solution is to upgrade the Basic load balancer to a Standard load balancer.
- Private Link: If you connect to a private endpoint in your virtual network from your on-premises network, the connection will go through the virtual network gateway.

Configure ExpressRoute FastPath

To enable FastPath, connect a virtual network to an ExpressRoute circuit using the Azure portal.

This section shows you how to create a connection to link a virtual network to an Azure ExpressRoute circuit using the Azure portal. The virtual networks that you connect to your Azure ExpressRoute circuit can either be in the same subscription or be part of another subscription.

Prerequisites

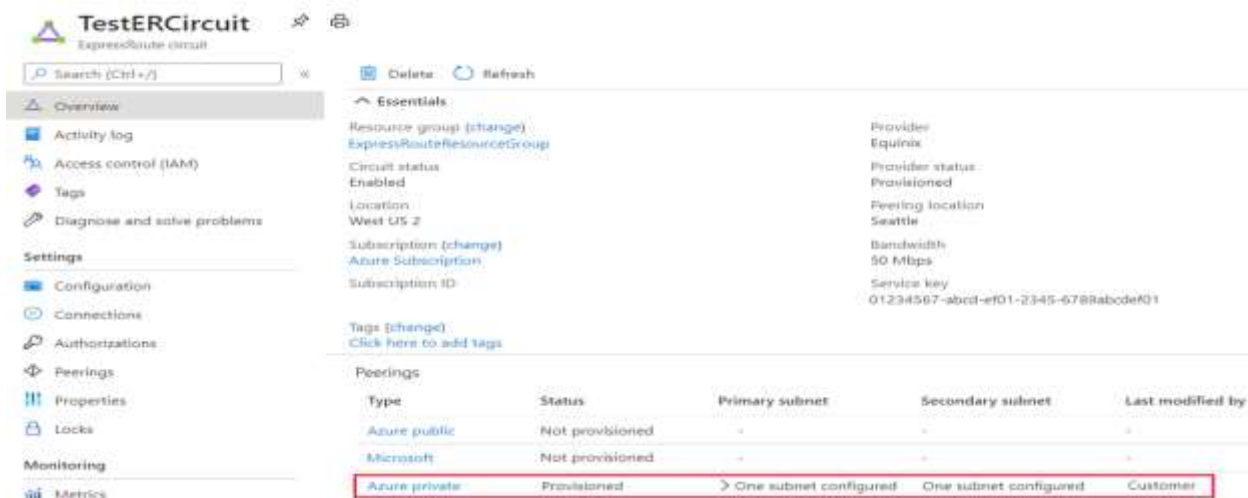
- Review the routing requirements, and workflows before you begin configuration.
- You must have an active ExpressRoute circuit.
- Follow the instructions to create an ExpressRoute circuit and have the circuit enabled by your connectivity provider.
- Ensure that you have Azure private peering configured for your circuit.
- Ensure that Azure private peering gets configured and establishes BGP peering between your network and Microsoft for end-to-end connectivity.
- Ensure that you have a virtual network and a virtual network gateway created and fully provisioned. A virtual network gateway for ExpressRoute uses the GatewayType 'ExpressRoute', not VPN.
- You can link up to 10 virtual networks to a standard ExpressRoute circuit. All virtual networks must be in the same geopolitical region when using a standard ExpressRoute circuit.
- A single VNet can be linked to up to 16 ExpressRoute circuits. Use the following process to create a new connection object for each ExpressRoute circuit you are connecting to. The ExpressRoute circuits can be in the same subscription, different subscriptions, or a mix of both.
- If you enable the ExpressRoute premium add-on, you can link virtual networks outside of the geopolitical region of the ExpressRoute circuit. The premium add-on will also allow you to connect more than 10 virtual networks to your ExpressRoute circuit depending on the bandwidth chosen.
- To create the connection from the ExpressRoute circuit to the target ExpressRoute virtual network gateway, the number of address spaces advertised from the local or peered virtual networks needs to be equal to or less than **200**. Once the connection has been successfully created, you can add additional address spaces, up to 1,000, to the local or peered virtual networks.

Connect a VNet to a circuit - same subscription

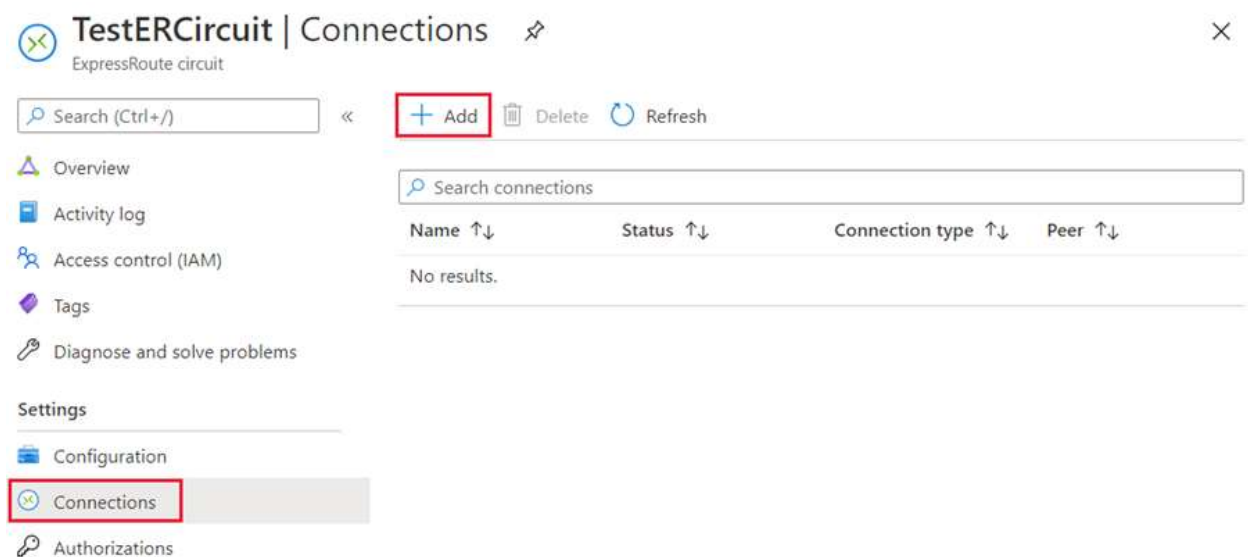
Note

BGP configuration information will not appear if the layer 3 provider configured your peering. If your circuit is in a provisioned state, you should be able to create connections.

1. To create a connection Ensure that your ExpressRoute circuit and Azure private peering have been configured successfully. Your ExpressRoute circuit should look like the following image:



2. You can now start provisioning a connection to link your virtual network gateway to your ExpressRoute circuit. Select **Connection** > **Add** to open the **Add connection** page.



3. Enter a name for the connection and then select **Next: Settings >**.

Create connection

Basics Settings Tags Review + create

Create a secure connection to your virtual network by using VPN Gateway or ExpressRoute. [Learn more about VPN Gateway](#) 
[Learn more about ExpressRoute](#) 

Project details

Subscription

Azure Subscription

Resource group

ExpressRouteResourceGroup

[Create new](#)

Instance details

Connection type 

ExpressRoute

Name *

ER-VNet-Connection

Region

(US) West US 2

Review + create

< Previous

Next : Settings >

[Download a template for automation](#)

4. Select the gateway that belongs to the virtual network that you want to link to the circuit and select **Review + create**. Then select **Create** after validation completes.
- 5.

Create connection

Basics Settings Tags Review + create

Virtual network gateway

To use a virtual network with a connection, it must be associated to a virtual network gateway.

Virtual network gateway *	<input type="text" value="ERGW"/>
ExpressRoute circuit	<input type="text" value="TestERCircuit"/>
Redeem authorization	<input type="checkbox"/>
Routing weight *	<input type="text" value="0"/>



Review + create

< Previous




Next : Tags >


[Download a template for automation](#)


6. After your connection has been successfully configured, your connection object will show the information for the connection.


 **TestERCircuit | Connections** 


ExpressRoute circuit


<<  Add  Delete  Refresh

 Overview


 Activity log


 Access control (IAM)


 Tags

 Diagnose and solve problems

Settings

 Configuration

 **Connections**

 Authorizations

Name ↑↓	Status ↑↓	Connection type ↑↓	Peer ↑↓
ER-VNet-Connection	Succeeded	ExpressRoute	ERGW

Administration - About circuit owners and circuit users

The 'circuit owner' is an authorized Power User of the ExpressRoute circuit resource. The circuit owner can create authorizations that can be redeemed by 'circuit users'. Circuit users are owners of virtual network gateways that are not within the same subscription as the ExpressRoute circuit. Circuit users can redeem authorizations (one authorization per virtual network).

The circuit owner has the power to modify and revoke authorizations at any time. Revoking an authorization results in all link connections being deleted from the subscription whose access was revoked.

Circuit owner operations

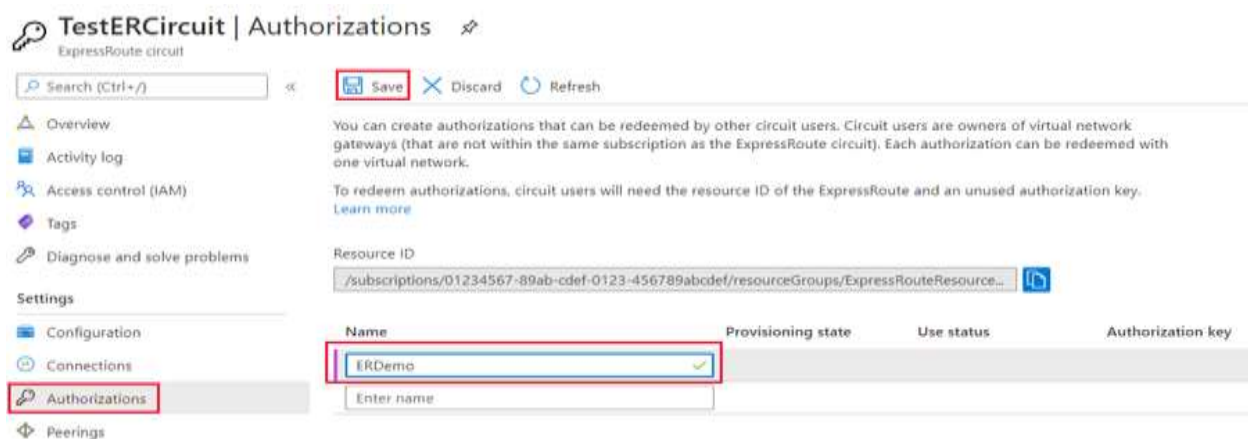
To create a connection authorization

The circuit owner creates an authorization, which creates an authorization key to be used by a circuit user to connect their virtual network gateways to the ExpressRoute circuit. An authorization is valid for only one connection.

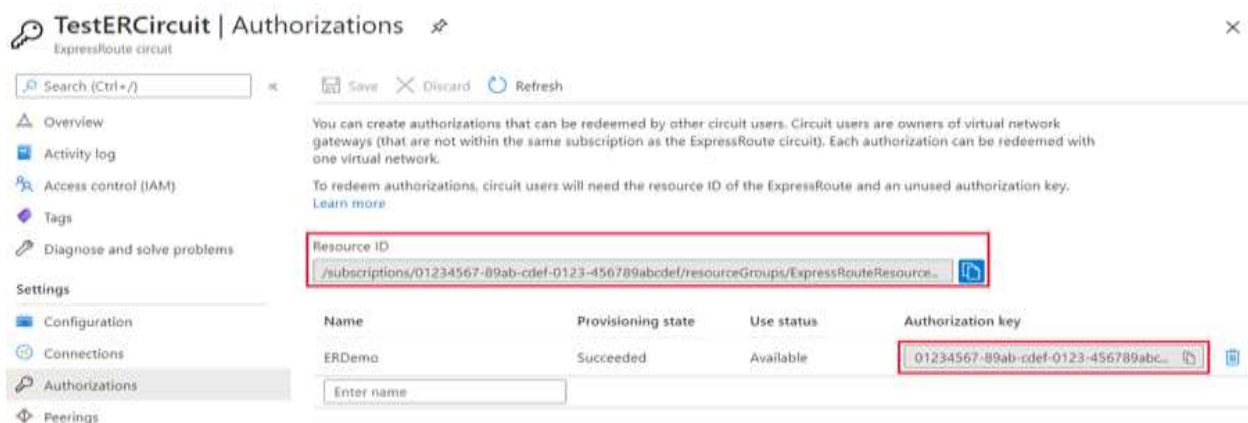
Note

Each connection requires a separate authorization.

1. In the ExpressRoute page, select **Authorizations** and then type a **name** for the authorization and select **Save**.



2. Once the configuration is saved, copy the **Resource ID** and the **Authorization Key**.



3. To delete a connection authorization

You can delete a connection by selecting the Delete icon for the authorization key for your connection.

TestERCircuit | Authorizations

Search (Ctrl+/) Save Discard Refresh


Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings
Configuration
Connections
Authorizations
Peerings

You can create authorizations that can be redeemed by other circuit users. Circuit users are owners of virtual network gateways (that are not within the same subscription as the ExpressRoute circuit). Each authorization can be redeemed with one virtual network.

To redeem authorizations, circuit users will need the resource ID of the ExpressRoute and an unused authorization key.
[Learn more](#)

Resource ID
/subscriptions/01234567-89ab-cdef-0123-456789abcdef/resourceGroups/ExpressRouteResource...

Name	Provisioning state	Use status	Authorization key
ERDemo	Succeeded	Available	01234567-89ab-cdef-0123-456789abc... 
<input type="text" value="Enter name"/>			

If you want to delete the connection but retain the authorization key, you can delete the connection from the connection page of the circuit.

TestERCircuit | Connections

Search (Ctrl+/) Add Delete Refresh

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings
Configuration
Connections
Authorizations

Search connections

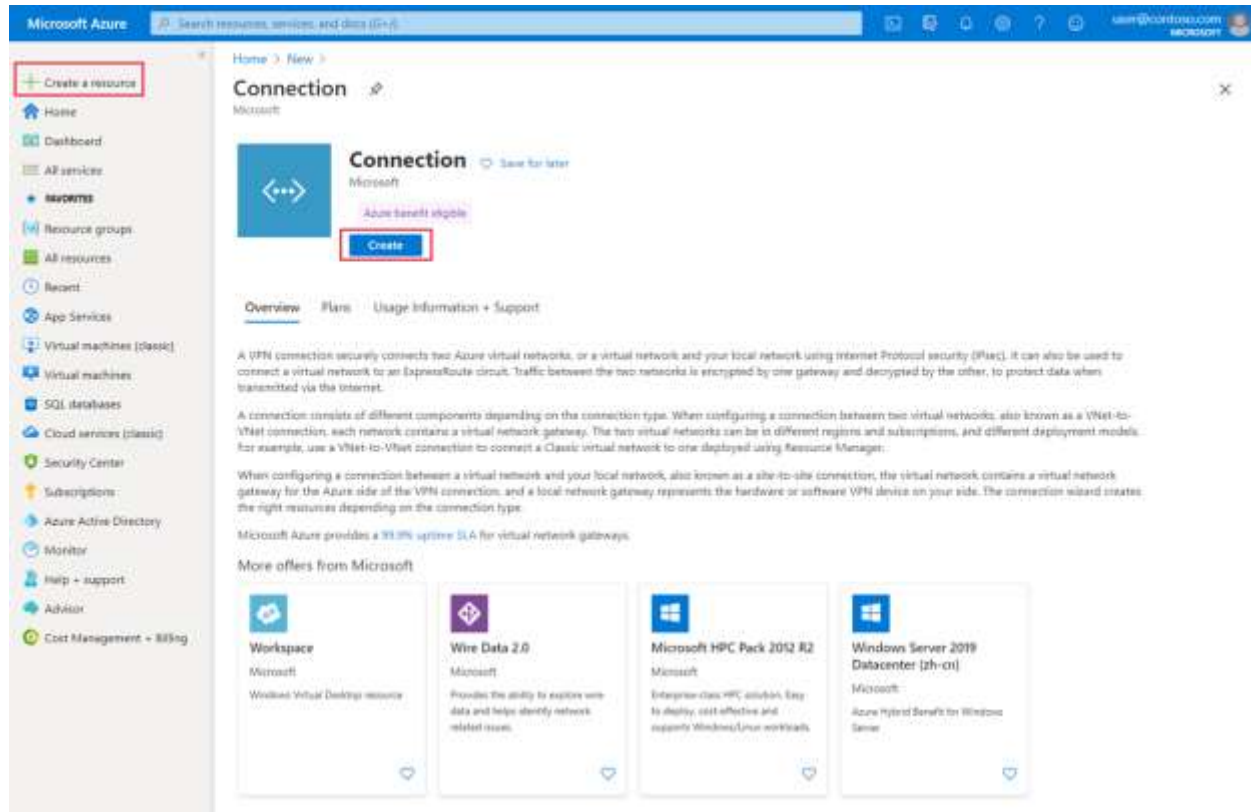
Name ↑↓	Status ↑↓	Connection type ↑↓	Peer ↑↓
ER-VNet-Connection	Succeeded	ExpressRoute	ERGW

Circuit user operations

The circuit user needs the resource ID and an authorization key from the circuit owner.

To redeem a connection authorization

1. Select the + Create a resource button. Search for Connection and select Create.



2. Make sure the Connection type is set to **ExpressRoute**. Select the Resource group and Location, then select **OK** in the Basics page.

Note

The location must match the virtual network gateway location you are creating the connection for.

Basics

Connection type * ⓘ

ExpressRoute

Subscription *

Azure Subscription

Resource group * ⓘ

ExpressRouteResourceGroup

[Create new](#)

Location *

West US 2

OK

3. In the **Settings** page, Select the Virtual network gateway and check the **Redeem authorization** check box. Enter the Authorization key and the Peer circuit URI and give the connection a name. Select **OK**.

Note

The Peer Circuit URI is the Resource ID of the ExpressRoute circuit (which you can find under the Properties Setting pane of the ExpressRoute Circuit).

Settings

*Virtual network gateway ⓘ >

ERGW

☒ Redeem authorization ⓘ

Authorization key *

01234567-89ab-cdef-0123-456789abcdef ✓

Peer circuit URI *

/subscriptions/01234567-89ab-cdef-012... ✓

Connection name *

ER-VNet-Connection ✓

Routing weight *

0

OK

4. Review the information in the **Summary** page and select **OK**.

Summary

Basics

Connection type	ExpressRoute
Subscription	Azure Subscription
Resource Group	ExpressRouteResourceGroup
Location	East US

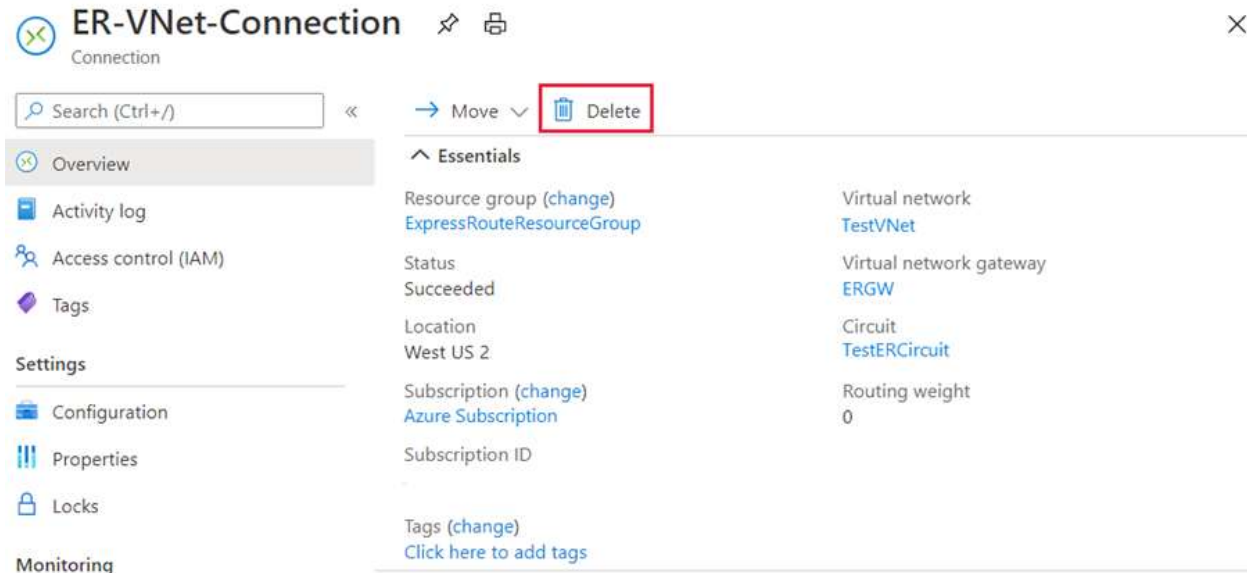
Settings

Virtual network gateway	ERGW
Redeem ExpressRoute authorization	Yes
Authorization key	01234567-89ab-cdef-0123-456789abcdef
Peer circuit URI	/subscriptions/01234567-89ab-cdef-0123-45678...
Connection name	ER-VNet-Connection

OK

Clean up resources

1. You can delete a connection and unlink your VNet to an ExpressRoute circuit by selecting the **Delete** icon on the page for your connection.



Troubleshoot ExpressRoute connection issues

As an Azure network engineer supporting an ExpressRoute deployment, you will have to diagnose and resolve any ExpressRoute connection issues that arise.

ExpressRoute connectivity traditionally involves three distinct network zones, as follows:

- Customer Network
- Provider Network
- Microsoft Datacenter

Note

In the ExpressRoute direct connectivity model (offered at 10/100 Gbps bandwidth), customers can directly connect to Microsoft Enterprise Edge (MSEE) routers' port. Therefore, in the direct connectivity model, there are only customer and Microsoft network zones.

Verify circuit provisioning and state through the Azure portal

Provisioning an ExpressRoute circuit establishes a redundant Layer 2 connections between CEs/PE-MSEEs (2)/(4) and MSEEs (5).

Tip

A service key uniquely identifies an ExpressRoute circuit. Should you need assistance from Microsoft or from an ExpressRoute partner to troubleshoot an ExpressRoute issue, provide the service key to readily identify the circuit.

In the Azure portal, open the ExpressRoute circuit blade. In the section of the blade, the ExpressRoute essentials are listed as shown in the following screenshot:

ER-Demo-Ckt-SV
ExpressRoute circuit

Settings Delete

Essentials

Resource group	Provider
USWest-ER-Demo-RG	Equinix
Circuit status	Provider status
Enabled	Provisioned
Location	Peering location
West US	Silicon Valley
Subscription name	Bandwidth
ExpressRoute-Demo	200 Mbps
Subscription ID	Service key

[All settings](#)

Peerings

Add tiles

TYPE	STATUS	PRIMARY SUBNET	SECONDARY SUBNET	
Azure private	Disabled	-	-	...
Azure public	Disabled	-	-	...
Microsoft	Disabled	-	-	...

Add a section

In the ExpressRoute Essentials, Circuit status indicates the status of the circuit on the Microsoft side. Provider status indicates if the circuit has been Provisioned/Not provisioned on the service-provider side.

For an ExpressRoute circuit to be operational, the Circuit status must be Enabled, and the Provider status must be Provisioned.

Note

After configuring an ExpressRoute circuit, if the Circuit status is stuck in not enabled status, contact **Microsoft Support**. On the other hand, if the Provider status is stuck in not provisioned status, contact your service provider.

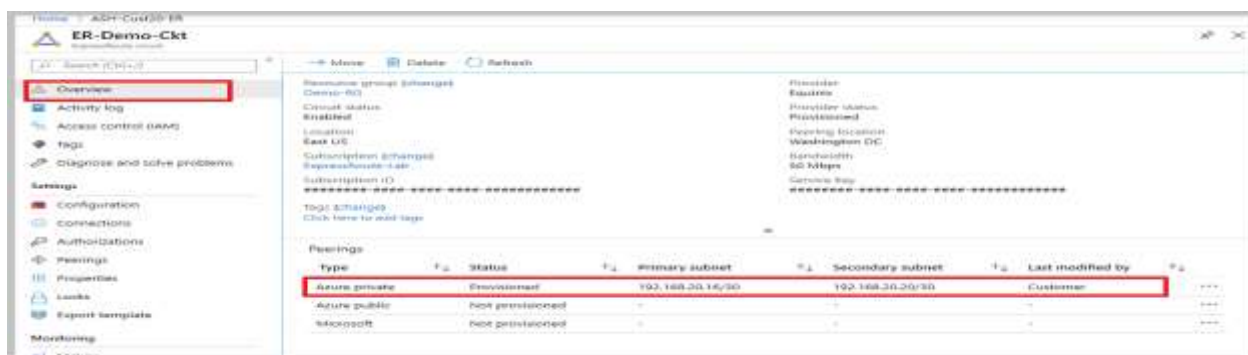
Validate peering configuration

After the service provider has completed the provisioning the ExpressRoute circuit, multiple eBGP based routing configurations can be created over the ExpressRoute circuit between CEs/MSEE-PEs (2)/ (4) and MSEEs (5). Each ExpressRoute circuit can have: Azure private peering (traffic to private virtual networks in Azure), and/or Microsoft peering (traffic to public endpoints of PaaS and SaaS).

Note

In IPVPN connectivity model, service providers handle the responsibility of configuring the peering (layer 3 services). In such a model, after the service provider has configured a peering and if the peering is blank in the portal, try refreshing the circuit configuration using the refresh button on the portal. This operation will pull the current routing configuration from your circuit.

In the Azure portal, status of an ExpressRoute circuit peering can be checked under the ExpressRoute circuit blade. In the overview section of the blade, the ExpressRoute peering would be listed as shown in the following screenshot:



In the preceding example, as noted Azure private peering is provisioned, whereas Azure public and Microsoft peering are not provisioned. A successfully provisioned peering context would also have the primary and secondary point-to-point subnets listed. The /30 subnets are used for the interface IP address of the MSEEs and CEs/PE-MSEEs. For the peering that are provisioned, the listing also indicates who last modified the configuration.

Note

If enabling a peering fails, check if the primary and secondary subnets assigned match the configuration on the linked CE/PE-MSEE. Also check if the correct VlanId, AzureASN, and PeerASN are used on MSEEs and if these values map to the ones used on the linked CE/PE-MSEE. If MD5 hashing is chosen, the shared key should be same on MSEE and PE-MSEE/CE pair. Previously configured shared key would not be displayed for security reasons. Should you need to change any of these configuration on an MSEE router, refer to **Create and modify routing for an ExpressRoute circuit**.

Note

On a /30 subnet assigned for interface, Microsoft will pick the second usable IP address of the subnet for the MSEE interface. Therefore, ensure that the first usable IP address of the subnet has been assigned on the peered CE/PE-MSEE.

Validate Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) is a layer 2 protocol defined in RFC 826. ARP is used to map the Ethernet address (MAC address) with an ip address. ARP tables can help validate layer 2 configuration and troubleshooting basic layer 2 connectivity issues.

The ARP table provides a mapping of the IP address and MAC address for a particular peering. The ARP table for an ExpressRoute circuit peering provides the following information for each interface (primary and secondary):

- Mapping of on-premises router interface ip address to the MAC address
- Mapping of ExpressRoute router interface ip address to the MAC address
- Age of the mapping ARP tables can help validate layer 2 configuration and troubleshooting basic layer 2 connectivity issues.

ARP table when Microsoft side has problems

- You won't see an ARP table shown for a peering if there are issues on the Microsoft side.
- Open a support ticket with Microsoft support. Specify that you have an issue with layer 2 connectivity.

Next Steps

- Validate Layer 3 configurations for your ExpressRoute circuit.
 - Get route summary to determine the state of BGP sessions.
 - Get route table to determine which prefixes are advertised across ExpressRoute.
- Validate data transfer by reviewing bytes in / out.
- Open a support ticket with Microsoft support if you're still experiencing issues.

ExpressRoute monitoring tools

ExpressRoute uses Network insights to provide a detailed topology mapping of all ExpressRoute components (peerings, connections, gateways) in relation with one another. Network insights for ExpressRoute also have preloaded metrics dashboard for availability, throughput, packet drops, and gateway metrics.

You can analyze metrics for Azure ExpressRoute with metrics from other Azure services using metrics explorer by opening Metrics from the Azure Monitor menu.

- To view ExpressRoute metrics, filter by Resource Type ExpressRoute circuits.
- To view Global Reach metrics, filter by Resource Type ExpressRoute circuits and select an ExpressRoute circuit resource that has Global Reach enabled.
- To view ExpressRoute Direct metrics, filter Resource Type by ExpressRoute Ports.