Advisory
Public

Customer Advisory: Cisco Catalyst SD-WAN and Microsoft Azure

April 23, 2026

Dear valued customer,

Cisco is committed to providing you with secure, reliable, and optimized connectivity solutions as part of our ongoing partnership with Microsoft Azure. Recent updates and ongoing considerations within Azure's infrastructure have impacted or may potentially affect customers, prompting us to issue this advisory notice.

Important considerations regarding the integration of Catalyst SD-WAN with Microsoft Azure networking are outlined below for your information. The solutions affected include Cisco Catalyst Cloud Onramp with Azure Virtual WAN, Cisco Catalyst Cloud OnRamp to Azure via Software Defined Cloud Interconnect (SDCI) and manual Catalyst 8000V deployments in Azure.

Impact on Catalyst 8000V performance due to Microsoft Azure Network Adapter (MANA) roll-out for older compute

Symptom

Cisco Catalyst SD-WAN customers using Catalyst 8000V VMs (including Azure Network Virtual Appliances - NVAs) in Azure can see a drop in throughput as Microsoft rolls out MANA support for existing VM SKUs. This can impact all VMs, those currently running and any new deployments.

Root Cause

Microsoft announced MANA (Microsoft Azure Network Adapter) support for Existing VM SKUs affecting v5 and older compute VM families. As of the publication of this notice, Catalyst 8000V VMs running in Azure do NOT support the required MANA NIC drivers for accelerated networking. Without the MANA driver Catalyst 8000V VMs continue to functionally work but at lower throughputs.

Mitigation

Refer to the Cisco document, Remediate: Advisory – Catalyst 8000V Running in Microsoft Azure on MANA Enabled Hosts, for further details on immediate mitigation and upgrade options.

Cisco has partnered with Microsoft and has already applied the temporary opt-out mechanism via tags for all managed NVA instances of Catalyst 8000V deployed in Azure Virtual WANs – those deployed using Cisco SD-WAN Manager Cloud OnRamp automation as well as those deployed manually.

Throughput limitations due to packet limits in Azure

Symptom

Branch traffic destined towards cloud gateways deployed in Azure over public IP addresses can face throughput limitations due to packet-per-second restrictions of Azure. (This limitation does not apply to traffic over private IP addresses.)

Root Cause

Within the public network, Microsoft has implemented DDoS prevention mechanisms to enforce rate limits on both inbound and outbound UDP traffic. The default limit for all customers is set at 200,000 packets per second (PPS) in each direction, per public destination IP address. Catalyst SD-WAN traffic to and from public IP addresses is subject to this PPS limitation, limiting throughput.

Mitigation

To increase throughput performance, do one of these:

- Follow the steps in this article: Improve Throughput on Catalyst 8000V in Azure
- Utilize Cloud OnRamp's integration with Software-Defined Cloud Interconnect (SDCI) providers to consolidate edge locations and establish private connectivity into Azure regions, supporting high-bandwidth traffic requirements.

SDCI connection deletion failure due to change in API payload of virtual network gateway

Symptom

When attempting to delete an SDCI (Software-Defined Cloud Interconnect) connection to Azure, configured using Cisco Catalyst Cloud OnRamp automation for Megaport or Equinix, the automation fails to delete the vNET-to-ExpressRoute gateway if the gateway does not have a public IP address assigned to it. This shows up as a failure in SD-WAN Manager task logs.

Root Cause

This issue is observed with newly created vNET-to-ExpressRoute gateways that do not have a public IP address, due to a recent change in Azure. When a connection is established from a branch to a vNET via ExpressRoute, using SD-WAN Manager Cloud OnRamp automation, subsequent deletion of this connection results in the entry being successfully removed from the SD-WAN Manager database. However, the vNET-to-ExpressRoute gateway on the Azure portal is not deleted.

Mitigation

Upgrade to Catalyst SD-WAN releases 20.12.6, 20.15.5, or 20.18.1. To resolve the issue without upgrading, after deleting the connection from SD-WAN Manager, directly delete the vNET-to-ExpressRoute gateway through the Azure portal.

Gateway creation failures for new Cloud OnRamp for Azure customers

Symptom

Customers deploying new Cloud OnRamp for Azure configurations — specifically those who have not yet created an Azure Cloud Gateway — may experience gateway creation failures after October 2026, described in this Azure update, if running Catalyst SD-WAN versions earlier than 20.15.5, or version 20.18.1. To ensure continued service availability, we recommend upgrading to a supported software version before this date. Customers with existing Azure Cloud Gateways are not affected by this issue and may continue to deploy gateways in new regions without interruption.

Root Cause

Microsoft Azure has announced the deprecation of General Purpose v1 (GPv1) and legacy blob storage accounts, which are an integral part of the Cloud OnRamp day-0 configuration process. In the absence of a blob storage account, the orchestration fails since it needs a blob storage account to store the configuration files. Cisco Catalyst SD-WAN release 20.15 removes the dependency on blob storage accounts

Mitigation

Upgrade to Catalyst SD-WAN releases 20.15.5 or 20.18.2, which remove the dependency on blob storage accounts.

Legal information