Revised: May 13, 2026

Known limitations of using Cisco ISE on Azure

Known limitations of Cisco ISE in Microsoft Azure cloud services

These are the known limitations with using Cisco ISE with Microsoft Azure cloud services:

- If you create Cisco ISE using the Azure Virtual Machine, Microsoft Azure assigns private IP addresses to VMs through DHCP servers by default. Before creating a Cisco ISE deployment on Microsoft Azure, update the forward and reverse DNS entries with the IP addresses assigned by Microsoft Azure.

  After installing Cisco ISE, you can assign a static IP address to your VM by updating the Network Interface object in Microsoft Azure. To do this:

  1. Stop the VM.
  2. Choose **Private IP address settings > Assignment > Static**.
  3. Restart the VM.
  4. In the Cisco ISE serial console, assign the IP address to the Gi0 interface.
  5. Restart the Cisco ISE application server.

- Dual NIC supports only two NICs: Gigabit Ethernet 0 and Gigabit Ethernet 1. To configure a secondary NIC, first create a network interface object in Azure, power off your Cisco ISE instance, and then attach the network interface object to your Cisco ISE.

  After you install and launch Cisco ISE on Azure, use the Cisco ISE CLI to manually configure the IP address of the network interface object as the secondary NIC.

- You cannot upgrade Cisco ISE in a Microsoft Azure environment. You can only perform fresh installations. However, you can carry out backup and restore of configuration data. For information on upgrading hybrid Cisco ISE deployments, refer to Upgrade Guidelines for Hybrid Deployments.

- The public cloud supports only Layer 3 features. Cisco ISE nodes on Microsoft Azure do not support Layer 2 features. For example, DHCP SPAN profiler probes and CDP protocol functions accessed through the Cisco ISE CLI are not supported.

- To restore and back up configuration data, first complete the backup operation. Then, restart Cisco ISE through the CLI and initiate the restore operation from the Cisco ISE GUI. For more information, refer to the Chapter "Maintain and Monitor" in the *Cisco ISE Administrator Guide* for your release.

- SSH access to the Cisco ISE CLI with password-based authentication is not supported in Azure. You can access the Cisco ISE CLI only through a key pair, which must be stored securely.

  If you use a private key (or PEM) file and lose the file, you cannot access the Cisco ISE CLI.

  Integrations that use password-based authentication to access the Cisco ISE CLI are not supported.

- Cisco ISE deployments on Azure Cloud do not support Accelerated Networking. Enabling this feature may cause operations such as node registration and deregistration to fail.

Out-of-order fragmentation limitation for Cisco ISE deployments on Azure

Microsoft Azure's default virtual network stack drops out-of-order IP fragments for security reasons (specifically to address the FragmentSmack vulnerability), which prevents these fragments from reaching the destination virtual machine. This behavior can affect Cisco ISE deployments. As a result, Cisco ISE and network devices may not receive complete RADIUS packets, leading to authentication, authorization, and Dynamic Access Control List (DACL) push failures.

You may encounter this issue on all Cisco ISE versions when using the Azure default VPN Gateway, Azure ExpressRoute, or Azure Virtual WAN. This issue is especially common with large RADIUS packets, such as EAP-TLS packets with large certificates, DACL pushes, or RADIUS authentication and accounting requests with multiple attributes.

To mitigate this issue, deploy a third-party VPN gateway (such as Cisco Catalyst 8000V or Cisco ASAv) as an Azure virtual machine. This gateway terminates VPN tunnels from on-premises environments and supports fragmentation reassembly. The Azure default VPN Gateway does not support fragmentation reassembly.

After deploying third-party VPN gateways in Azure to establish site-to-site VPN connectivity with on-premises, perform these steps to ensure reliable handling of large RADIUS packets and to mitigate authentication failures due to fragmentation issues in Azure environments:

1. On the third-party VPN gateway, enable ip virtual-reassembly to correctly reassemble fragmented packets, even if they are received out of order.

   For Catalyst 8000V, use this command:

   ```
   ip virtual-reassembly-out
   ```

   For Cisco ASAv, use this command:

   ```
   fragment reassembly full outside
   ```

2. Enable fragmentation before encryption on the third-party VPN gateway, because NAT traversal for site-to-site VPNs may fragment large IPsec packets converted to UDP 4500.

   For Cisco ASAv, use this command:

   ```
   crypto ipsec fragmentation before-encryption
   ```

3. In the Azure portal, enable IP forwarding on both the inside and outside interfaces of the VPN gateway VM.

4. Update Azure routing tables to allow virtual network connectivity through the third-party VPN gateway. This allows access to on-premises resources.

If you continue to experience intermittent authentication failures after configuring these settings, open a Microsoft support ticket to enable the **allow out-of-order fragments** option for Azure VPN networking components in your subscription.

Note

To reduce packet fragmentation at both the network device (such as WLC or switch) and Cisco ISE egress, consider lowering the MTU on the network device's RADIUS source interface and Cisco ISE's RADIUS interface. While a general MTU value of 1400 bytes works well in most environments, optimal performance can be achieved by using Path MTU Discovery (PMTUD) tools to determine the best MTU between the subnets.