Revised: June 29, 2026

Compatibility information for Cisco ISE instances on AWS

Compatibility information for Cisco ISE on AWS

This section provides compatibility information that is unique to Cisco ISE on AWS. For general compatibility details for Cisco ISE, refer to Cisco Identity Services Engine Network Component Compatibility.

Cisco Catalyst Center integration support

You can connect your Cisco ISE to Cisco Catalyst Center release 2.2.1 and later releases.

Load balancer integration support

You can integrate the AWS-native network load balancer with Cisco ISE for load balancing the RADIUS and TACACS traffic. However, these limitations are applicable:

- The Change of Authorization (CoA) feature is supported only when you enable client IP preservation in network load balancer.
- Unequal load balancing might occur because network load balancer only supports source IP affinity and not the calling station ID-based sticky sessions.
- Traffic can be sent to a Cisco ISE PSN even if the RADIUS service is not active on the node because network load balancer does not support RADIUS-based health checks.

You can integrate the AWS-native network load balancer with Cisco ISE for load balancing TACACS traffic. However, traffic might be sent to a Cisco ISE PSN even if the TACACS service is not active on the node because network load balancer does not support health checks based on TACACS+ services.

NIC jumbo frame support

Cisco ISE supports jumbo frames. The Maximum Transmission Unit (MTU) for Cisco ISE is 9,001 bytes, while the MTU of Network Access Devices is typically 1,500 bytes. Cisco ISE supports and receives both standard and jumbo frames without issue. You can reconfigure the Cisco ISE MTU as required, through the Cisco ISE CLI in configuration mode.

Prerequisites to create a Cisco ISE AWS instance

Before you deploy your Cisco ISE instance on Amazon Web Services, ensure that you have prepared your environment and confirmed your foundational knowledge. Reviewing these requirements ensures a smooth setup process and supports optimal performance for your deployment.

Configuration prerequisites

You must

- configure VPC in AWS
- create encrypted EBS volumes, and
- create security groups, subnets, and key pairs in AWS before you configure a Cisco ISE instance.

To successfully deploy Cisco ISE on AWS, your AWS Identity and Access Management (IAM) policy must allow access to Key Management Service (KMS) resources. When configuring a security group for Cisco ISE, you must create rules for all the ports and

protocols for the Cisco ISE services you want to use. From Cisco ISE release 3.5, to deploy Cisco ISE AWS instances on an IPv6 single-stack network, you must have a subnet configured for IPv6 within your AWS Virtual Private Cloud (VPC).

IP address prerequisites

These are the IP address prerequisites:

- To configure an IPv6 address for the network interface, the subnet must have an IPv6 Classless Inter-Domain Routing (CIDR) pool that is enabled in AWS.
- he IP address that you enter in the Management Network field in the Cisco ISE CloudFormation template must not be an IP address that exists as a network interface object in AWS.
- You can configure a static IP as a private IP in your deployment. However, the static IP must be configured with a DNS-resolvable hostname.

Familiarity with AWS cloud concepts

You must be familiar with

- managing AWS service quotas, and
- AWS solutions such as Amazon Elastic Compute Cloud (EC2) instances, Amazon Elastic Block Store (EBS) volumes, and concepts such as Regions, Availability Zones, Security Groups, Virtual Private Cloud (VPC), and so on.

References

Refer to AWS documentation for information on AWS solutions.