

# Deploy Cisco Identity Services Engine Natively on Cloud Platforms

**First Published:** 2022-08-16

**Last Modified:** 2026-09-18

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2026 Cisco Systems, Inc. All rights reserved.



# CONTENTS


CHAPTER 1 **Cisco ISE on Cloud** 1

Cisco ISE on cloud 1

Cisco ISE licensing on cloud platforms 1

Upgrade Cisco ISE hybrid deployments 1

Upgrade hybrid deployments with PAN installed on premises 2

Upgrade hybrid deployments with PAN installed on cloud 2

Login credentials for Cisco ISE instances launched through cloud platforms 3

Usernames for Cisco ISE on cloud 3

Passwords for Cisco ISE on cloud 3

Additional information 3

CHAPTER 2 **Cisco ISE on Amazon Web Services** 5

Overview of Cisco ISE on Amazon Web Services 5

Methods to launch Cisco ISE on AWS 5

Overview of CFTs 5

Example of a deployment connected to AWS cloud 6

Cisco ISE instances and intended usage 6

Multi-node Cisco ISE deployments on AWS 8

Prerequisites to create a Cisco ISE AWS instance 8

Familiarity with AWS cloud concepts 8

Configuration prerequisites 8

IP address prerequisites 8

Known limitations of using Cisco ISE on AWS 9

Support limitations 9

Configuration limitations 9

CLI limitations 10

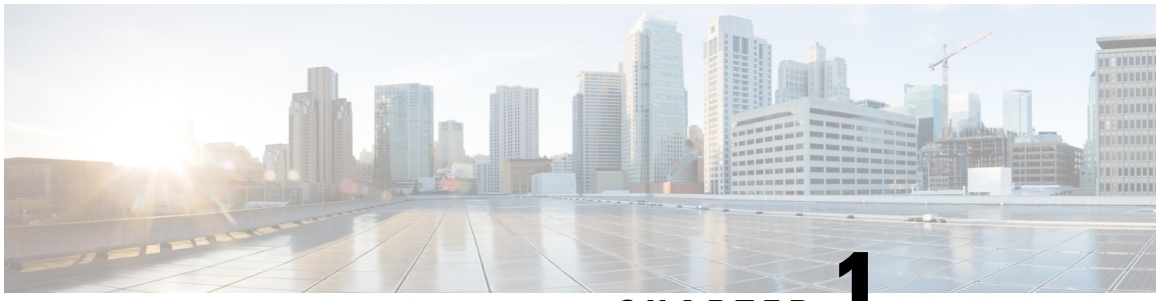
Memory, disk size, and volume limitations 10
Deployment limitations 10
Upgrade limitations 10
Latency limitation 11
User data backup and restore limitations 11
Launch a Cisco ISE CFT through AWS Marketplace 11
Configure a Cisco ISE instance 11
Automate the configuration of Cisco ISE instances 12
View CFT in AWS CloudFormation Designer 12
Launch CFT and specify the parameters 12
Configure the parameters for the Cisco ISE instance 13
Add multiple DNS or NTP servers 15
Launch Cisco ISE with CFT 15
Configure a Cisco ISE instance 16
Upload a CFT file and configure the parameters 16
Launch a Cisco ISE AMI 17
Navigate to the Cisco ISE option on the Amazon EC2 console 17
Configure instance details 18
Configure advanced details 19
User data parameters 20
Add storage 24
Add tags 25
Configure security group 25
Review and launch 25
Select an existing key pair or create a new key pair 26
Launch the Cisco ISE AMI instance 26
Postinstallation notes and tasks 27
Check the status of the instance launch 28
How and when to access the Cisco ISE GUI or CLI 28
Download the key pair 28
Check the status of the Cisco ISE processes 29
Compatibility information for Cisco ISE on AWS 29
Cisco Catalyst Center integration support 29
Load balancer integration support 29

NIC jumbo frame support 30
Password recovery and reset on AWS 30
Password reset on AWS 30
Change Cisco ISE password through AWS serial console 30
View configured password 31
Create a new public key pair 31
Password recovery on AWS 31

CHAPTER 3 **Cisco ISE on Azure Cloud Services 33**
Cisco ISE on Azure cloud 33
Azure deployment methods 33
Azure VM sizes supported by Cisco ISE 34
Known limitations of Cisco ISE in Microsoft Azure cloud services 36
Out-of-order fragmentation limitation for Cisco ISE deployments on Azure 37
Create a Cisco ISE instance using an Azure VM 38
Navigate to the Cisco ISE option on the Azure console 38
Configure instance details 38
Configure OS disk size 39
Configure network interface 39
Configure user details 39
Configure tags 42
Review and create 42
Edit disk size 42
Create a Cisco ISE instance using Azure application 43
Navigate to the Cisco ISE option on the Azure console 43
Add instance details 43
Configure network settings 43
Configure services 44
Add user details 44
User data parameters 45
Review and create 48
Postinstallation tasks 49
Compatibility information for Cisco ISE on Azure cloud 49
Load balancer integration support 49

Password recovery and reset on Azure cloud 49
Reset Cisco ISE GUI password through serial console 50
Create new public key pair for SSH access 50

CHAPTER 4 **Cisco ISE on Oracle Cloud Infrastructure 51**
Cisco ISE on Oracle Cloud Infrastructure 51
OCI instances supported by Cisco ISE 52
Known limitations of using Cisco ISE on OCI 52
Create a Cisco ISE instance in OCI 53
Navigate to the Cisco ISE option on the OCI console 54
Configure instance details 54
Configure advanced options for a Cisco ISE instance 55
User data parameters 57
Create a Cisco ISE instance in OCI using a Terraform Stack file 61
Create a Cisco ISE stack in OCI 61
Configure variables for Cisco ISE instance 62
Review configurations and create a Cisco ISE instance in OCI 62
Postinstallation tasks 62
Compatibility information for Cisco ISE on OCI 63
Load balancer integration support 63
NIC jumbo frame support 63
Password recovery and reset on OCI 63
Reset Cisco ISE GUI password through serial console 63
Create a new public key pair in OCI 64
Password recovery 64



CHAPTER 1

# Cisco ISE on Cloud


- Cisco ISE on cloud, on page 1
- Cisco ISE licensing on cloud platforms, on page 1
- Upgrade Cisco ISE hybrid deployments, on page 1
- Login credentials for Cisco ISE instances launched through cloud platforms, on page 3
- Additional information, on page 3


## Cisco ISE on cloud

Cisco Identity Services Engine (ISE) is now available natively from cloud service providers, enabling you to scale your Cisco ISE deployments quickly and easily to meet changing business needs. Cisco ISE is available as an Infrastructure as a Service solution, helping you to rapidly deploy network accesses and control services anywhere.

You can extend the Cisco ISE deployments in your on-premises network securely onto

- Amazon Web Services (AWS) from Cisco ISE release 3.1 and later releases
- Azure Cloud Services (Microsoft Azure) from Cisco ISE release 3.2 and later releases, and
- Oracle Cloud Infrastructure (OCI) from Cisco ISE release 3.2 and later releases.

## Cisco ISE licensing on cloud platforms

Cisco ISE leverages the Bring Your Own License (BYOL) solution that is available on cloud platforms. Use the Common VM License to enable Cisco ISE on cloud platforms, in addition to the other Cisco ISE licenses that you need for the Cisco ISE features you want to use. Refer to Cisco ISE Licensing Guide for information on Cisco ISE licenses.

## Upgrade Cisco ISE hybrid deployments

Cisco ISE upgrade workflow is not available in Cisco ISE on AWS, Microsoft Azure, or OCI. Only fresh installs of Cisco ISE are supported. However, you can carry out backup and restore of configuration data. You can upgrade Cisco ISE hybrid deployments where the Primary Administration Node (PAN) is installed either on cloud or on premises.

• Upgrade hybrid deployments with PAN installed on premises, on page 2.
• Upgrade hybrid deployments with PAN installed on cloud, on page 2.

# Upgrade hybrid deployments with PAN installed on premises

Follow these steps to upgrade a hybrid deployment in which the PAN is installed on premises, and any or some of the secondary nodes are installed on the cloud.

### Procedure

**Step 1** Deregister the secondary nodes that are installed on the cloud from the Cisco ISE deployment.

If all the secondary nodes are installed on the cloud, this could cause a downtime.

**Step 2** Upgrade the on-prem deployment to a higher release.

For more information on this, refer to the section "Perform the Upgrade" in the *Cisco Identity Services Engine Upgrade Journey* for your release.

**Step 3** Install the required number of standalone Cisco ISE nodes on the cloud with the higher release.

You must install and configure the nodes with the same IP addresses to avoid configuration changes on the NADs. For more information on the installation process, refer to the *Cisco Identity Services Engine Installation Guide* for your release.

**Step 4** Register these standalone nodes to the upgraded on premises deployment.

You need to import the system certificates to the newly deployed nodes in Cisco ISE. For more information about how to import system certificates to a Cisco ISE node, refer to the "Import a System Certificate" section in the "Basic Setup" chapter of the *Cisco Identity Services Engine Administrator Guide* for your release.

The upgrade of a hybrid Cisco ISE deployment in which the PAN is installed on premises is complete.

# Upgrade hybrid deployments with PAN installed on cloud

Follow these steps to upgrade a hybrid deployment in which the PAN is installed on cloud.

### Procedure

**Step 1** Backup Cisco ISE configuration settings and operational logs from the existing deployment.

**Step 2** Shut down all the nodes in the deployment.

**Step 3** Install the required number of standalone Cisco ISE nodes on cloud and on premises with the higher release.

You must install and configure the nodes with the same IP addresses to avoid configuration changes on the NADs. For more information on the installation process, refer to the *Cisco Identity Services Engine Installation Guide* for your release.

**Step 4** Restore Cisco ISE configuration from the backup data. For more information, refer to the "Backup and Restore Upgrade Process" section in the *Cisco Identity Services Engine Upgrade Journey* for your release.

**Step 5** Register all the nodes to the upgraded cloud deployment.

The upgrade of a hybrid Cisco ISE deployment in which the PAN is installed on cloud is complete.

# Login credentials for Cisco ISE instances launched through cloud platforms

The username and password for any Cisco ISE instance launched using cloud-native images or hosted on supported cloud platforms must be secure.

## Usernames for Cisco ISE on cloud

The default username for Cisco ISE instances that are launched through cloud platforms is iseadmin. Even if you enter a different username in the user data, the Cisco ISE instance is created with the username iseadmin.



**Remember** For Cisco ISE release 3.1 instances that are launched through AWS, the default username is admin.

## Passwords for Cisco ISE on cloud

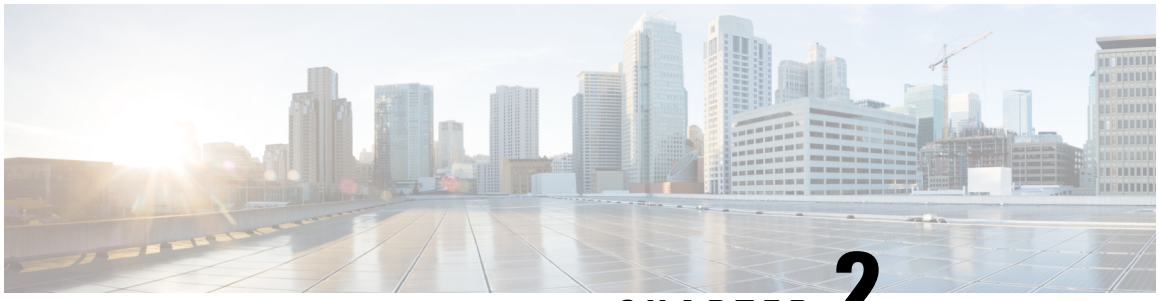
In all cloud platforms, the password that you configure when setting up an instance is stored as plaintext. However, a plaintext password can present a security risk. So, for any Cisco ISE instance launched from a cloud platform, you must reset the login password when you first access the Cisco ISE GUI. Then, you must also update your API-based automation scripts with the updated password to avoid any errors.

The username and password for any Cisco ISE instance launched using cloud-native images or hosted on supported cloud platforms must be secure.

# Additional information

Refer to

- Performance and Scalability Guide for Cisco Identity Services Engine for information on the performance and scalability of Cisco ISE deployments on cloud platforms.
- Cisco Identity Services Engine End-User Documentation for more information on Cisco ISE.



CHAPTER 2

# Cisco ISE on Amazon Web Services


- Overview of Cisco ISE on Amazon Web Services, on page 5
- Prerequisites to create a Cisco ISE AWS instance, on page 8
- Known limitations of using Cisco ISE on AWS, on page 9
- Launch a Cisco ISE CFT through AWS Marketplace, on page 11
- Launch Cisco ISE with CFT, on page 15
- Launch a Cisco ISE AMI, on page 17
- Postinstallation notes and tasks, on page 27
- Compatibility information for Cisco ISE on AWS, on page 29
- Password recovery and reset on AWS, on page 30


# Overview of Cisco ISE on Amazon Web Services

## Methods to launch Cisco ISE on AWS

You can configure and launch Cisco ISE in AWS through AWS CloudFormation Templates (CFTs) or Amazon Machine Images (AMIs). We recommend that you use CFTs through one of the ways in the following list. To launch Cisco ISE on AWS, perform one of the following procedures:

- Launch a Cisco ISE CloudFormation template through AWS Marketplace
- Launch Cisco ISE with CloudFormation template
- Launch a Cisco ISE AMI

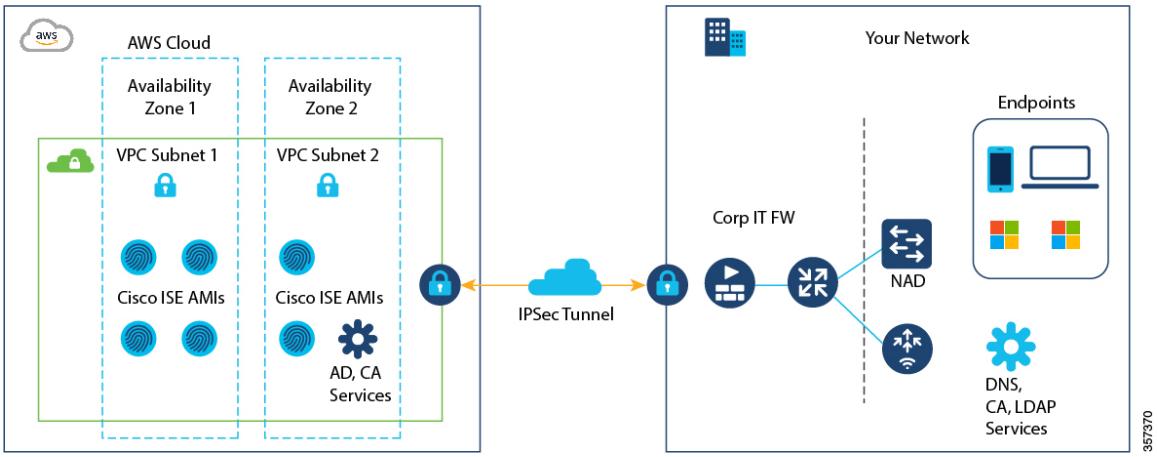
## Overview of CFTs

CFTs are AWS solutions that allow you to easily create and manage cloud deployments. Extend your network into the cloud by creating a virtual private cloud in AWS and configure a virtual private gateway to enable communication with your organization's network over an IPsec tunnel.

# Example of a deployment connected to AWS cloud

This illustration is only an example. You can place common services such as Certificate Authority (CA), Active Directory (AD), Domain Name System (DNS) servers, and Lightweight Directory Access Protocol (LDAP) on premises or in AWS, based on the requirements of your organization.

***Figure 1: Example of a deployment connected to AWS cloud***




**References**

For more information on using CFTs in AWS, refer to AWS CloudFormation User Guide.

# Cisco ISE instances and intended usage

This table contains details of the Cisco ISE instances that are currently available. You must purchase a Cisco ISE VM license to use any of these instances. For information on EC2 instance pricing for your specific requirements, refer to Amazon EC2 On-Demand Pricing.

***Table 1: Cisco ISE instances***

| Cisco ISE instance type | CPU cores | RAM (in GB) |
|---|---|---|
| t3.xlarge<br>This instance supports the Cisco ISE evaluation use case. 100 concurrent active endpoints are supported.<br>From Cisco ISE release 3.5, t3.xlarge instance type is not supported. | 4 | 16 |
| m5.2xlarge | 8 | 32 |
| c5.4xlarge | 16 | 32 |
| m5.4xlarge<br>From Cisco ISE release 3.3, m5.4xlarge instance type is not supported. | 16 | 64 |

| Cisco ISE instance type | CPU cores | RAM (in GB) |
|---|---|---|
| c5.9xlarge | 36 | 72 |
| m5.8xlarge | 32 | 128 |
| m5.16xlarge | 64 | 256 |
| c7i.4xlarge* | 16 | 32 |
| m7i.2xlarge* | 8 | 32 |
| m7i.8xlarge* | 32 | 128 |
| m7i.16xlarge* | 64 | 256 |

*Cisco ISE releases 3.4 patch 4, 3.5, and later support M7i and C7i instance types on AWS.

You can leverage the AWS S3 storage service to easily store backup and restore files, monitoring and troubleshooting reports, and more.



**Attention**

- If you use a general purpose instance as a PSN, the performance numbers are lower than the performance of a compute-optimized instance as a PSN.
- m5.2xlarge and m7i.2xlarge instances must be used as Extra Small PSN only.

### Intended use of specific instance types

This table categorizes some of the instance types and their intended usage.

***Table 2: Instance types and their intended usage***

| Instance category | Instance type example | Intended use |
|---|---|---|
| Compute-optimized instances | c5.4xlarge<br>c5.9xlarge<br>c7i.4xlarge | • Compute-intensive tasks or applications<br>• Policy Service Node (PSN) |
| General purpose instances | m5.4xlarge (This instance is available only in Cisco ISE release 3.2 and earlier releases.)<br>m5.8xlarge<br>m5.16xlarge<br>m7i.8xlarge<br>m7i.16xlarge | • Data processing tasks and database operations<br>• Policy Administration Node (PAN) or Monitoring and Troubleshooting (MnT) nodes, or both |

### References

For information on the scale and performance data for AWS instances, refer to Cisco ISE Performance and Scale guide.

## Multi-node Cisco ISE deployments on AWS

In addition to the procedures explained earlier, you can also use these Cisco-developed solutions to install and automatically create multi-node Cisco ISE deployments on AWS.

- Cisco ISE AWS Partner Solution for small deployments.
- Cisco Developed Terraform Script for deployments of any size.

# Prerequisites to create a Cisco ISE AWS instance

These are the prerequisites to create a Cisco ISE AWS instance.

## 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.

## 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.
- The 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.

# Known limitations of using Cisco ISE on AWS

These are the known limitations with using Cisco ISE in AWS.

## Support limitations

- The Amazon VPC supports only Layer 3 features. Cisco ISE nodes on AWS instances do not support Cisco ISE functions that depend on Layer 1 and Layer 2 capabilities. For example, working with DHCP SPAN profiler probes and CDP protocols that use the Cisco ISE CLI is currently not supported.

  The communication from on-prem devices to the VPC must be secure.
- NIC bonding is not supported.
- Dual NIC is supported with only two NICs—Gigabit Ethernet 0 and Gigabit Ethernet 1. To configure a secondary NIC in your Cisco ISE instance, you must
  1. Create a network interface object in AWS.
  2. Power off your Cisco ISE instance.
  3. Attach this network interface object to Cisco ISE.
  4. Install and launch Cisco ISE on AWS.
  5. Use the Cisco ISE CLI to manually configure the IP address of the network interface object as the secondary NIC.
- Amazon EC2 user data scripts are not supported.

## Configuration limitations

You cannot

- take an Amazon EBS snapshot of a Cisco ISE instance and then create another EBS volume with the snapshot
- configure an IPv6-based NTP server when launching Cisco ISE through AWS. From Cisco ISE release 3.5, IPv6-based NTP servers are supported for both dual-stack and pure IPv6 instances.
- change the IP address of an instance after it has been created successfully, and

- generate the initial administrator user account name. An initial administrator user account name, iseadmin, is generated by default. This user account name is used for both SSH and GUI access to Cisco ISE after the installation process is complete.

Cisco ISE sends traffic to AWS Cloud through IP address 169.254.169.254 to obtain the instance details. This is to check if it is a cloud instance and can be ignored in on-prem deployments.

# CLI limitations

These are the CLI limitations.

- SSH access to Cisco ISE CLI using password-based authentication is not supported in AWS. You can only access the Cisco ISE CLI through a secured key pair. If you use a private key (or PEM) file and you lose the file, you will not be able to access the Cisco ISE CLI. Any integration that uses a password-based authentication method to access Cisco ISE CLI is not supported, for example, Cisco Catalyst Center release 2.1.2 and earlier.
- In Cisco ISE release 3.1, when you run the show inventory command through a Cisco ISE instance that is launched through AWS, the output does not display the instance type of the Cisco ISE on AWS. This issue is resolved in Cisco ISE release 3.1 patch 1 and later releases.

# Memory, disk size, and volume limitations

These are the memory, disk size, and volume limitations:

- You cannot resize an EC2 instance.
- You cannot convert the Cisco ISE Disk EBS Volume as an AMI and then relaunch another EC2 instance with this AMI.
- In the Cisco ISE CFT that you configure, you define volume size in GB. However, AWS creates EBS storage volumes in Gibibyte (GiB). Therefore, when you enter 600 as the Volume Size in the Cisco ISE CFT, AWS creates 600 GiB (or 644.25 GB) of EBS volume.
- You might receive an Insufficient *Virtual Machine Resources* alarm when Cisco ISE is in idle state. You can ignore this alarm because the CPU frequency is maintained lower than the required baseline frequency (2 GHz) for effective power conservation.

# Deployment limitations

These are two deployment types supported, but you must ensure that internode latencies are less than 300 milliseconds.

- Hybrid deployments with some Cisco ISE nodes on premises and some nodes in AWS.
- Interregional deployments through VPC peering connections.

# Upgrade limitations

Cisco ISE upgrade workflow is not available in Cisco ISE on AWS. Only fresh installs are supported. However, you can carry out backup and restore of configuration data.

### References

Refer to *Upgrade Guidelines for Hybrid Deployments* for information on upgrading hybrid Cisco ISE deployments.

## Latency limitation

You can integrate the external identity sources that are located on the premises. However, because of latency, when on-premises identity sources are used, Cisco ISE's performance is not at par with Cisco ISE's performance when AWS-hosted identity sources or the Cisco ISE internal user database is used.

## User data backup and restore limitations

These are the user data backup and restore limitations.

- User data retrieval only works for Metadata V1 (IMDSv1); it does not work with V2.
- When restore operation is run during a configuration data backup through the Cisco ISE CLI or GUI, ADE-OS parameter should not be included.

# Launch a Cisco ISE CFT through AWS Marketplace

You can use this method to launch standalone Cisco ISE instances.

The Cisco ISE CFT creates an instance of the General Purpose SSD (gp2) volume type.

**Note** For PAN and MnT nodes, use the gp3 volume type to achieve improved I/O throughput. Configure the gp3 volume parameters by following the steps in the Launch a Cisco ISE AMI, on page 17 section.

To understand post-installation tasks and known limitations when working with Cisco ISE deployments on AWS, refer to Post-Installation Tasks and Known limitations.

Follow these steps to launch a Cisco ISE CFT through AWS marketplace.

### Procedure

**Step 1** Configure a Cisco ISE instance.

**Step 2** Launch CFT and specify the parameters.

## Configure a Cisco ISE instance

Follow these steps to configure a Cisco ISE instance.

**Procedure**

**Step 1** Log in to the Amazon Management Console at https://console.aws.amazon.com/.
**Step 2** Search for **AWS Marketplace Subscriptions**.
**Step 3** In the **Manage Subscriptions** screen, click **Discover Products**.
**Step 4** Click the product name.
**Step 5** Click **Continue to Configuration**.
**Step 6** In the **Configure this Software** area, click **Learn More**.
**Step 7** Click **Download CloudFormation Template** to download the Cisco ISE CFT to your local system.

You can use the downloaded CFT to automate the configuration of other Cisco ISE instances, as required.

You can click **View Template** in the **Learn More** dialog box to view the CFT in the AWS CloudFormation Designer.

**Step 8** Choose the required values from the **Software Version** and **AWS Region** drop-down lists.
**Step 9** Click **Continue to Launch**. For more information, refer to Launch CFT and specify the parameters, on page 12.

## Automate the configuration of Cisco ISE instances

You can use the downloaded CFT to automate the configuration of other Cisco ISE instances, as required.

## View CFT in AWS CloudFormation Designer

You can click **View Template** in the **Learn More** dialog box to view the CFT in the AWS CloudFormation Designer.

# Launch CFT and specify the parameters

Follow these steps to launch the CFT and configure the parameters.

**Procedure**

**Step 1** From the **Choose Action** drop-down list, choose **Launch CloudFormation**.
**Step 2** Click **Launch**.
**Step 3** In the **Create Stack** window, click the **Template Is Ready** and **Amazon S3 URL** radio buttons.
**Step 4** Click **Next**.
**Step 5** Enter a value in the **Stack Name** field.
**Step 6** Enter the required details in the **Parameters** area. For more information about the parameters, refer to Configure the parameters for the Cisco ISE instance, on page 13.
**Step 7** Click **Next** to initiate the instance-creation process.

**References**

Refer to Chapter "Deployment" in the *Cisco ISE Administrator Guide* for your release to create a Cisco ISE deployment.

# Configure the parameters for the Cisco ISE instance

You can configure these parameters for the Cisco ISE instance:

| Field name | Field description |
|---|---|
| Hostname | This field only supports alphanumeric characters and hyphen (-).<br>The length of the hostname should not exceed 19 characters. |
| Instance Key Pair | To access the Cisco ISE instance through SSH, choose the PEM file that you created in AWS for the username iseadmin. For Cisco ISE release 3.1, the username is admin.<br>Create a PEM key pair in AWS now, if you have not configured one already.<br>Example:<br>`ssh -i mykeypair.pem iseadmin@myhostname.compute-1.amazonaws.com` |
| Management Security Group | Choose the security group from the drop-down list. You must create the security group in AWS before configuring this CFT.<br>You can add only one security group in this step. You can add additional security groups in Cisco ISE after installation. |
| Management Network | Choose the subnet to be used for the Cisco ISE interface.<br>To enable IPv6 addresses, you must associate an IPv6 CIDR block with your VPC and subnets.<br>Create a subnet in AWS now if you have not configured one already. |
| Management Private IP<br>(renamed as **Management Interface IPv4 Address** from Cisco ISE release 3.5) | Enter the IPv4 address from the subnet that you selected earlier. If this field is left blank, the AWS DHCP assigns an IP address.<br>After the Cisco ISE instance is created, copy the private IP address from the **Instance Summary** window. Then, map the IP and hostname in your DNS server before you create a Cisco ISE deployment. |
| Create IPv6-only Instance<br>(from Cisco ISE release 3.5) | Choose whether to create an IPv6-only instance. If yes, no IPv4 address will be assigned. |
| Management Private IPv6 Address<br>(from Cisco ISE release 3.5) | Enter the IPv6 address from the subnet that you chose earlier. If this field is left blank, the AWS DHCP assigns an IPv6 address. |
| Timezone | Choose a system time zone from the drop-down list. |
| Instance Type | Choose a Cisco ISE instance type from the drop-down list. |

| Field name | Field description |
|---|---|
| EBS Encryption | Choose **True** from the drop-down list to enable encryption.<br>In Cisco ISE release 3.3 and later releases, the default value for this field is **True**. |
| (Optional) KMS Key | Enter the KMS Key or Amazon Resource Name or alias for data encryption.<br>This is an optional field applicable for Cisco ISE release 3.3 and later releases.<br>• If the KMS Key is provided, it will be used for data encryption.<br>• If the KMS Key is not provided, the default key will be used for data encryption. |
| Volume Size | Specify the volume size, in GB. The accepted range is 300 GB to 2400 GB.<br>We recommend 600 GB for production use. Configure a volume size lesser than 600 GB only for evaluation purposes.<br>When you terminate the instance, the volume is also deleted.<br>AWS creates EBS storage volumes in Gibibyte (GiB). For example, when you enter 600 in the Volume Size field, AWS creates 600 GiB (or 644.25 GB) of EBS volume. |
| DNS Domain | Accepted values for this field are ASCII characters, numerals, hyphen (-), and period (.). |
| Primary Name Server<br>(**Name Server** before Cisco ISE release 3.4) | Enter the IP address of the name server. |
| (Optional) Secondary Name Server<br>(from Cisco ISE release 3.4) | Enter the IP address of the secondary name server to be configured for Cisco ISE. |
| (Optional) Tertiary Name Server<br>(from Cisco ISE release 3.4) | Enter the IP address of the tertiary name server to be configured for Cisoc ISE. |
| Primary NTP Server<br>(**NTP Server** before Cisco ISE release 3.4) | Enter the IP address or hostname of the Primary NTP server, for example, time.nist.gov. If you use the wrong syntax, Cisco ISE services might not come up on launch.<br>If the IP address or the hostname that you enter here is incorrect, Cisco ISE cannot synchronize with the NTP server. Use an SSH terminal to log in to Cisco ISE and then use the Cisco ISE CLI to configure the correct NTP server. |
| (Optional) Secondary NTP Server<br>(from Cisco ISE release 3.4) | Enter the IP address or hostname of the secondary NTP server, for example, time.nist.gov. If you use the wrong syntax, Cisco ISE services might not come up on launch. |

| Field name | Field description |
|---|---|
| (Optional) Tertiary NTP Server<br>(from Cisco ISE release 3.4) | Enter the IP address or hostname of the tertiary NTP server, for example, time.nist.gov. If you use the wrong syntax, Cisco ISE services might not come up on launch. |
| ERS | To enable ERS services at Cisco ISE launch, enter **yes**. The default value for this field is **no**. |
| OpenAPI | To enable OpenAPI services at Cisco ISE launch, enter **yes**. The default value for this field is **no**.<br>From Cisco ISE release 3.4, OpenAPI services are enabled by default. |
| pxGrid | To enable pxGrid services at Cisco ISE launch, enter **yes**. The default value for this field is **no**. |
| pxGrid Cloud | The default value for this field is **no**.<br>From Cisco ISE release 3.5, pxGrid Cloud can be enabled only from the Cisco ISE GUI. Therefore, this field is unavailable. |
| Password | Enter the administrative password that must be used for the Cisco ISE GUI. The password must be compliant with the Cisco ISE password policy.<br>The password is displayed in plain text in the **User Data** area of the instance settings window in the AWS console. |

#### References

Refer to the "User Password Policy" section in the chapter "Basic Setup" of the *Cisco ISE Administrator Guide* for your release.

## Add multiple DNS or NTP servers

From Cisco ISE release 3.4, you can configure up to three DNS or NTP servers through the CFT, but you can only add one server at a time. To add additional DNS or NTP servers after deploying a Cisco ISE instance, you must use the Cisco ISE CLI.

From Cisco ISE release 3.5, you can configure IPv6 DNS and NTP servers directly through the CFT. To configure IPv6 servers in earlier Cisco ISE releases, use the Cisco ISE CLI.

# Launch Cisco ISE with CFT

You can use this method to launch standalone Cisco ISE instances.

The Cisco ISE CFT creates an instance of the General Purpose SSD (gp2) volume type.

Follow these steps to launch Cisco ISE with CFT.

### Before you begin

### Procedure

**Step 1** Configure a Cisco ISE instance.
**Step 2** Upload a CFT file and configure the parameters.

# Configure a Cisco ISE instance

Follow these steps to configure a Cisco ISE instance.

### Procedure

**Step 1** Log in to the Amazon Management Console at https://console.aws.amazon.com/.
**Step 2** Search for **AWS Marketplace Subscriptions**.
**Step 3** In the **Manage Subscriptions** screen, click **Discover Products**.
**Step 4** Enter Cisco Identity Services Engine (ISE) in the search bar.
**Step 5** Click the product name.
**Step 6** In the new window that is displayed, click **Continue to Subscribe**.
**Step 7** Click **Continue to Configuration**.
**Step 8** In the **Configure this Software** area, click **Learn More**.

# Upload a CFT file and configure the parameters

Follow these steps to upload a CFT file and configure the parameters.

### Procedure

**Step 1** Click **Download CloudFormation Template** to download the Cisco ISE CFT to your local system.
**Step 2** Using the AWS search bar, search for **CloudFormation**.
**Step 3** From the **Create Stack** drop-down list, choose **With new resources (standard)**.
**Step 4** In the **Create Stack** window, choose **Template Is Ready** and **Upload a Template File**.
**Step 5** Click **Choose File** and upload the CFT file that you downloaded in Configure a Cisco ISE instance, on page 16.
**Step 6** Click **Next**.
**Step 7** Enter a value in the **Stack Name** field.

**Step 8** Enter the required details in the **Parameters** area. For more information about the parameters, refer to Configure the parameters for the Cisco ISE instance, on page 13.

# Launch a Cisco ISE AMI

Follow these steps to launch a Cisco ISE AMI:

1. Navigate to the Cisco ISE option on the Amazon EC2 console
2. Configure instance details
3. Configure advanced details
4. Add storage
5. Add tags
6. Configure security group
7. Review and launch
8. Select an existing key pair or create a new key pair
9. Launch instances



**Attention** Simplified Auto Recovery is an AWS feature that performs an automatic recovery of the underlying infrastructure when a system status check failure occurs. This process is managed by AWS and involves an automatic reboot of the instance to ensure service continuity.

During the automated reboot process, resource provisioning delays may occasionally prevent Cisco ISE from initializing correctly.

If this occurs, log in to the AWS Management Console, navigate to the EC2 Dashboard, select the relevant Cisco ISE instance, and perform a manual reboot to restore the service to a functional state. For further guidance on managing EC2 instances, refer to the official AWS documentation.

# Navigate to the Cisco ISE option on the Amazon EC2 console

Follow these steps to navigate to the **Cisco Identity Engine (ISE)** option on the AWS EC2 console:

**Procedure**

**Step 1** Log in to your Amazon EC2 console at https://console.aws.amazon.com/ec2/.

**Step 2** In the left pane, click **Instances**.

**Step 3** In the **Instances** window, click **Launch Instances**.

**Step 4** In the **Step 1: Choose AMI** window, in the left menu, click **AWS Marketplace**.

**Step 5** In the search field, enter **Cisco Identity Services Engine**.

**Step 6** In the **Cisco Identity Services Engine (ISE)** option, click **Select**.
A **Cisco Identity Services Engine (ISE)** dialog box is displayed with various details of the AMI.

**Step 7** Review the information and click **Continue** to proceed.

# Configure instance details

Follow these steps to add and configure Cisco ISE instance details on the AWS EC2 console:

### Procedure

**Step 1** In the **Step 2: Choose an Instance Type** window, click the radio button next to the instance type that you want to use.

**Step 2** Click **Next: Configure Instance Details**.

**Step 3** In the **Step 3: Configure Instance Details** window, enter the required information in each field as described in the guidelines:

*Table 3: Configuration guidelines for instance details*

| Field name | Field description |
|---|---|
| Number of Instances | Enter **1** in this field. |
| Network | Choose the VPC in which you want to launch the Cisco ISE instance. |
| Subnet | Choose the subnet in which you want to launch the Cisco ISE instance.<br>**Note**<br>From Cisco ISE release 3.5, you can launch a Cisco ISE AWS instance on an IPv6-only network using an IPv6-only AWS subnet. |
| Network Interfaces | The drop-down list displays **New Network Interface** by default, which means that an IP address is auto-assigned to Cisco ISE by the connected DHCP server. You can choose to enter an IP address in this field to assign a fixed IP address to Cisco ISE. You can also choose an existing network interface from the same subnet, from the **Network Interfaces** drop-down list. You can only configure one interface during the setup process. After Cisco ISE is installed, you can add more interfaces through Cisco ISE. |

### What to do next

Review the information and proceed to *Configure advanced details*.

# Configure advanced details

Follow these steps to add and configure advanced Cisco ISE instance details on the AWS EC2 console.

### Procedure

In the **Advanced Details** area, click the **As Text** radio button in the **User Data** section and enter the key-value pairs in the correct format. From Cisco ISE release 3.5, to launch a Cisco ISE AWS instance on an IPv6 single-stack network, you must enable the **Metadata IPv6 endpoint** option in **Advanced Details**.

You must use the correct syntax for each of the fields that you configure through the user data entry. The information you enter in the **User data** field is not validated when it is entered. Using incorrect syntax may cause Cisco ISE services to fail to start when launching the image. These are the guidelines for the configurations that you submit through the user data field:

***Table 4: Configuration guidelines for User Data field***

| Field Name | Field Description | Compliance and Behavior Changes |
|---|---|---|
| hostname | Enter a hostname that contains only alphanumeric characters and hyphen (-). The length of the hostname must be less than 19 characters and must not contain underscores (_). | Syntax must meet recommendations. |
| primarynameserver | Enter the IP address of the primary name server. Only IPv4 addresses are supported. | From Cisco ISE release 3.5, IPv6-based name servers are supported on AWS instances in IPv6 single-stack networks. |
| dnsdomain | Enter the FQDN of the DNS domain. The entry can contain ASCII characters, numerals, hyphens (-), and periods (.). | Syntax must meet recommendations. |
| ntpserver | Enter the IPv4 address or FQDN of the NTP server that must be used for synchronization, for example, time.nist.gov. | From Cisco ISE release 3.5, IPv6-based NTP servers are also supported in this field for dual-stack and IPv6 single-stack network-based AWS instances. |
| timezone | Enter a timezone, for example, Etc/UTC. We recommend that you set all the Cisco ISE nodes to the Coordinated Universal Time (UTC) timezone, especially if your Cisco ISE nodes are installed in a distributed deployment. This procedure ensures that the timestamps of the reports and logs from the various nodes in your deployment are always synchronized. | Syntax must meet recommendations. |

| Field Name | Field Description | Compliance and Behavior Changes |
|---|---|---|
| username | The default username that you configure must be **admin**. If you configure a username other than **admin**, you will not be able to access the Cisco ISE CLI when you launch the AMI. | From Cisco ISE release 3.2, the mandatory username is **iseadmin**; therefore, the tag username=<admin> is not supported. |
| password | Configure a password for GUI-based login to Cisco ISE. The password that you enter must comply with the Cisco ISE password policy. The password must contain 6 to 25 characters and include at least one numeral, one uppercase letter, and one lowercase letter. The password cannot contain or be the same as the username or its reverse (iseadmin or nimdaesi), cisco, or ocsic. The allowed special characters are @~*!,+=_-. . | Refer to "User Password Policy" section in the chapter "Basic Setup" of the Cisco ISE Administrator Guide for your release. |
| ersapi | Enter **yes** to enable ERS, or **no** to disallow ERS. | Syntax must meet recommendations. |
| openapi | Enter **yes** to enable OpenAPI, or **no** to disallow OpenAPI. | From Cisco ISE release 3.4, OpenAPI services are enabled by default. You don't have to specify OpenAPI-related options when launching an instance. |
| pxGrid | Enter **yes** to enable pxGrid, or **no** to disallow pxGrid. | Syntax must meet recommendations. |
| pxGrid_cloud | Enter **yes** to enable pxGrid Cloud or **no** to disallow pxGrid Cloud.<br>To enable pxGrid Cloud, you must enable pxGrid. If you disallow pxGrid, but enable pxGrid Cloud, pxGrid Cloud services are not enabled at launch. | From Cisco ISE release 3.5, pxGrid Cloud can be enabled only from Cisco ISE Cisco ISE GUI. Therefore, this field is not included in the user data. |

### What to do next

Review the information and proceed to *Add storage*.

# User data parameters

This table lists the supported user data parameters, their required formats, and their availability across Cisco ISE releases. Refer to it when entering user data in the **Advanced > User data** section during Azure VM deployment.

| Field | Format | Cisco ISE release 3.1 | Cisco ISE release 3.2 | Cisco ISE release 3.3 | Cisco ISE release 3.4 | Cisco ISE release 3.5 |
|---|---|---|---|---|---|---|
| hostname | hostname=<hostname of Cisco ISE> | Supported | Supported | Supported | Supported | Supported |
| primarynameserver | primarynameserver=<IPv4 address><br>(primarynameserver=<IPv6 address> supported for AWS from Cisco ISE release 3.5) | Supported | Supported | Supported | Supported | Supported<br>Cisco ISE release 3.5 and later support IPv6 addresses in AWS deployments. |
| secondarynameserver | secondarynameserver=<IPv4 address><br>(secondarynameserver=<IPv6 address> supported for AWS from Cisco ISE release 3.5) | Not supported | Not supported | Not supported | Supported.<br>You must enter a value in this field if you want to use the tertiarynameserver field. | Supported.<br>You must enter a value in this field if you want to use the tertiarynameserver field.<br>Cisco ISE release 3.5 and later support IPv6 addresses in AWS deployments. |
| tertiarynameserver | tertiarynameserver=<IPv4 address><br>(tertiarynameserver=<IPv6 address> supported for AWS from Cisco ISE release 3.5) | Not supported | Not supported | Not supported | Supported.<br>You must first enter a value in the secondarynameserver field if you want to use this field. | Supported.<br>You must first enter a value in the secondarynameserver field if you want to use this field.<br>Cisco ISE release 3.5 and later support IPv6 addresses in AWS deployments. |
| dnsdomain | dnsdomain=<example.com> | Supported | Supported | Supported | Supported | Supported |

| Field | Format | Cisco ISE release 3.1 | Cisco ISE release 3.2 | Cisco ISE release 3.3 | Cisco ISE release 3.4 | Cisco ISE release 3.5 |
|---|---|---|---|---|---|---|
| ntpserver | ntpserver=<IPv4 address or FQDN of the NTP server><br>(ntpserver=<IPv6 address or FQDN of the NTP server> supported for AWS from Cisco ISE release 3.5) | Supported | Supported | Supported | Not supported.<br>This field is replaced by primaryntpserver in Cisco ISE release 3.4 and later. Using ntpserver may prevent Cisco ISE services from starting. | Not supported. Use primaryntpserver instead. |
| primaryntpserver | primaryntpserver=<IPv4 address or FQDN><br>(primaryntpserver=<IPv6 address or FQDN of the NTP server> supported for AWS from Cisco ISE release 3.5) | Not supported | Not supported | Not supported | Supported.<br>This field replaces ntpserver in Cisco ISE release 3.4 and later. | Supported.<br>Cisco ISE release 3.5 and later support IPv6 addresses in AWS deployments. |
| secondaryntpserver | secondaryntpserver=<IPv4 address or FQDN><br>(secondaryntpserver=<IPv6 address or FQDN of the NTP server> supported for AWS from Cisco ISE release 3.5) | Not supported | Not supported | Not supported | Supported.<br>You must enter a value in this field if you want to use the tertiaryntpserver field. | Supported.<br>You must enter a value in this field if you want to use the tertiaryntpserver field.<br>Cisco ISE release 3.5 and later support IPv6 addresses in AWS deployments. |

| Field | Format | Cisco ISE release 3.1 | Cisco ISE release 3.2 | Cisco ISE release 3.3 | Cisco ISE release 3.4 | Cisco ISE release 3.5 |
|---|---|---|---|---|---|---|
| tertiaryntpserver | tertiaryntpserver=<IPv4 address or FQDN><br>(tertiaryntpserver=<IPv6 address or FQDN of the NTP server> supported for AWS from Cisco ISE release 3.5) | Not supported | Not supported | Not supported | Supported.<br>You must first enter a value in the secondaryntpserver field if you want to use this field. | Supported.<br>You must first enter a value in the secondaryntpserver field if you want to use this field.<br>Cisco ISE release 3.5 and later support IPv6 addresses in AWS deployments. |
| timezone | timezone=<timezone> | Supported | Supported | Supported | Supported | Supported |
| username | username=<admin> | Supported (example: <admin>)<br>Supported from Cisco ISE release 3.1 patch 1. | Not supported.<br>iseadmin is the default user. | Not supported.<br>iseadmin is the default user. | Not supported.<br>iseadmin is the default user. | Not supported.<br>iseadmin is the default user. |
| username | username=iseadmin | Not mandatory | Mandatory | Mandatory | Mandatory | Mandatory |
| password | password=<password> | Supported | Supported | Supported | Supported | Supported |
| ersapi | ersapi=<yes/no> | Supported | Supported | Supported | Supported | Supported |
| openapi | openapi=<yes/no> | Supported | Supported | Supported | OpenAPI is enabled by default. | OpenAPI is enabled by default. |
| pxGrid | pxGrid=<yes/no> | Supported | Supported | Supported | Supported | Supported |
| pxgrid_cloud | pxgrid_cloud=<yes/no> | Not supported | Not supported | Supported.<br>This is only supported for Cisco ISE releases 3.3 and 3.4. | Supported.<br>This is only supported for Cisco ISE releases 3.3 and 3.4. | Not supported.<br>From Cisco ISE release 3.5, pxGrid Cloud can be enabled only from the Cisco ISE GUI. |

### Parameter syntax requirements

When specifying user data parameters for Cisco ISE on Cloud, do not enclose any attribute or value in single or double quotes. You must enter all values in plain text, without quotes.

| Invalid entry | Valid entry |
|---|---|
| hostname="i34a" | hostname=i34a |
| primarynameserver="9.9.9.9" | primarynameserver=9.9.9.9 |
| dnsdomain="example.com" | dnsdomain=example.com |
| primaryntpserver="north-america.pool.ntp.org" | primaryntpserver=north-america.pool.ntp.org |

From Cisco ISE release 3.3, validation output messages are displayed in the serial console. These messages are visible only if the serial console is open at the time the output is generated.

# Add storage

Follow these steps to add storage to the Cisco ISE instance:

### Procedure

**Step 1** Click **Next: Add Storage**.

**Step 2** In the **Step 4: Add Storage** window:

a) Enter a value in the **Size (GiB)** column.

The valid range for this field is 279.4 to 2235.2 GiB. In a production environment, you must configure storage equal to or greater than 558.8 GiB. Storage lesser than 558.8 GiB only supports an evaluation environment. Note that Cisco ISE is created with storage defined in GB. The GiB value that you enter here is automatically converted into GB values during the Cisco ISE image-creation process. In GB, the valid storage range is 300 to 2400 GB, with 600 GB as the minimum value for a Cisco ISE in a production environment.

b) From the **Volume Type** drop-down list, select **General Purpose SSO (gp2 or gp3)**.

For gp3 volumes, use the recommended minimum configuration:

- IOPS: 3,000
- Throughput: 400 MiB/s

c) To enable EBS encryption, from the **Encryption** drop-down list, select an encryption key.

**Warning**
Do not click the **Add New Volume** button that is displayed on this window.

### What to do next

Review the information and proceed to *Add tags*.

# Add tags

### Procedure

**Step 1** Click **Next: Add Tags**.

**Step 2** (Optional) In the **Step 5: Add Tags** window, click **Add Tag** and enter the required information in the **Key** and **Value** fields. The check boxes in the **Instances**, **Volumes**, and **Network Interfaces** columns are checked by default. If you have chosen a specific network interface in the **Step 3: Configure Instance Details** window, you must uncheck the **Network Interfaces** check box for each tag that you add in this window.

### What to do next

Review the information and proceed to *Configure security group*.

# Configure security group

Follow these steps to create a new security group or add an existing security group:

### Procedure

**Step 1** Click **Next: Configure Security Group**.

**Step 2** In the **Step 6: Configure Security Group** window, in the **Assign a security group area** area, you can choose to create a new security group or choose an existing security group by clicking the corresponding radio button.

a) If you choose **Create a new security group**, enter the required details in the **Type**, **Protocol**, **Port Range**, **Source**, and **Description** fields.

b) If you choose **Select an existing security group**, check the check boxes next to the security groups you want to add.

### What to do next

Review the information and proceed to *Review and launch*.

# Review and launch

Follow these steps to review the configurations you have created so far and to launch a Cisco ISE AMI:

### Procedure

**Step 1** Click **Review and Launch**.

**Step 2** In the **Step 7: Review Instance Launch** window, review all the configurations that you have created in this workflow. You can edit the values of these sections by clicking the corresponding **Edit** link.

**Step 3** Click **Launch**.

### What to do next

Proceed to *Select an existing key pair or create a new key pair*.

# Select an existing key pair or create a new key pair

Follow this step to select an existing key pair or create a new key pair:

### Procedure

In the **Select an existing key pair or create a new key pair** dialog box, select one of these options from the drop-down list:

- **Choose an existing key pair**
- **Create a new key pair**

**Note**
To use SSH to log in to Cisco ISE, use a key pair where the username is **iseadmin**. The key pair must be kept intact. If the key pair is lost or corrupted, you cannot recover your Cisco ISE because you cannot map a new key pair to the existing instance.

### What to do next

Review the information and proceed to *Launch instances*.

# Launch the Cisco ISE AMI instance

Launch the Cisco ISE AMI instance:

### Procedure

Check the check box for the acknowledgment statement and click **Launch Instances**.

The **Launch Status** window displays the progress of the instance creation.

### What to do next

You can create more Cisco ISE AMI instances using the same procedure.

# Postinstallation notes and tasks

To check the status of the instance launch, in the left pane of the AWS console, click **Instances**. The **Status Check** column for the instance displays **Initializing** while the instance is being configured. When the instance is ready and available, the column displays **x checks done**.

You can access the Cisco ISE GUI or CLI about 30 minutes after the Cisco ISE EC2 instance is built. You can access the CLI and GUI of Cisco ISE with the IP address that AWS provides for your instance and log in to the Cisco ISE administration portal or console.

When the Cisco ISE instance is ready and available for use, carry out these steps:

1. When you create a key pair in AWS, you are prompted to download the key pair into your local system. Download the key pair because it contains specific permissions that you must update to successfully log in to your Cisco ISE instance from an SSH terminal.

   Do one of these based on the operating system that you use:

***Table 5: Actions based on OS***

| If you are using... | Then... |
|---|---|
| Linux or macOS | Run this command from your CLI.<br>`sudo chmod 0400 mykeypair.pem` |
| Windows | **a.** Right-click the key file in your local system.<br>**b.** Choose **Properties > Security > Advanced**.<br>**c.** In the **Permissions** tab, assign full control to the appropriate user by clicking the corresponding option, and click **Disable Inheritance**.<br>**d.** In the **Block Inheritance** dialog box, click **Convert inherited permissions into explicit permissions on this object**.<br>**e.** In the **Permissions** tab, in the **Permissions entries** area, choose system and administrator users by clicking the corresponding entries, and then click **Remove**.<br>**f.** Click **Apply**, and then click **OK**. |

2. Access the Cisco ISE CLI by running these command in your CLI application:

   **ssh -i mykeypair.pem iseadmin@**<*Cisco ISE Private IP Address*>

3. At the login prompt, enter **iseadmin** as the username.
4. At the system prompt, enter **show application version ise** and press **Enter**.
5. To check the status of the Cisco ISE processes, enter **show application status ise** and press **Enter**.

   If the output displays that an application server is in Running state, Cisco ISE is ready for use.

6. You can then log in to the Cisco ISE GUI.

7. Carry out the postinstallation tasks listed in the topic "List of Postinstallation Tasks" in the Chapter "Installation Verification and Postinstallation Tasks" in the *Cisco ISE Installation Guide* for your release.

# Check the status of the instance launch

To check the status of the instance launch, in the left pane of the AWS console, click **Instances**. The **Status Check** column for the instance displays **Initializing** while the instance is being configured. When the instance is ready and available, the column displays **x checks done**.

# How and when to access the Cisco ISE GUI or CLI

You can access the Cisco ISE GUI or CLI about 30 minutes after the Cisco ISE EC2 instance is built. You can access the CLI and GUI of Cisco ISE with the IP address that AWS provides for your instance and log in to the Cisco ISE administration portal or console.

# Download the key pair

When the Cisco ISE instance is ready and available for use, carry out the following steps to download the key pair:

1. When you create a key pair in AWS, you are prompted to download the key pair into your local system.

   Download the key pair because it contains specific permissions that you must update to successfully log in to your Cisco ISE instance from an SSH terminal.

2. Do one of the following based on the operating system that you use:

***Table 6: Actions to take based on your OS***

| If you are using... | Then... |
|---|---|
| Linux or macOS | Run the following command from your CLI:<br>`sudo chmod 0400 mykeypair.pem` |
| Windows | **a.** Right-click the key file in your local system.<br>**b.** Choose **Properties** > **Security** > **Advanced**.<br>**c.** In the **Permissions** tab, assign full control to the appropriate user by clicking the corresponding option, and click **Disable Inheritance**.<br>**d.** In the **Block Inheritance** dialog box, click **Convert inherited permissions into explicit permissions on this object**.<br>**e.** In the **Permissions** tab, in the **Permissions entries** area, choose system and administrator users by clicking the corresponding entries, and then click **Remove**.<br>**f.** Click **Apply**, and then click **OK**. |

# Check the status of the Cisco ISE processes

Follow these steps to check the status of the Cisco ISE processes.

### Procedure

**Step 1** Access the Cisco ISE CLI by running the following command in your CLI application:

**ssh -i mykeypair.pem iseadmin@**<*Cisco ISE Private IP Address*>

**Step 2** At the login prompt, enter **iseadmin** as the username.

**Step 3** At the system prompt, enter **show application version ise** and press **Enter**.

**Step 4** To check the status of the Cisco ISE processes, enter **show application status ise** and press **Enter**.

If the output displays that an application server is in Running state, Cisco ISE is ready for use.

### What to do next

Log in to the Cisco ISE GUI and carry out the post-installation tasks listed in the topic "List of Post-Installation Tasks" in the Chapter "Installation Verification and Post-Installation Tasks" in the *Cisco ISE Installation Guide*.

# 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.

# Password recovery and reset on AWS

## Password reset on AWS

These tasks guide you through resetting your Cisco ISE virtual machine password.

- Change Cisco ISE password through AWS serial console , on page 30.
- View configured password, on page 31.
- Create a new public key pair, on page 31.

### Change Cisco ISE password through AWS serial console

Follow these steps to change Cisco ISE GUI password through serial console on AWS:

**Procedure**

**Step 1** Log in to your AWS account and go to the EC2 dashboard.

**Step 2** Click **Instances** from the left-side menu.

**Step 3** Click the Cisco ISE instance ID for which you need to change the password. If you know the password, skip to Step 5 of this task.

**Step 4** To log in to the serial console, you must use the original password that was set at the installation of the Cisco ISE instance. To view the password, refer to View the configured password.

**Step 5** Click **Connect**.

The EC2 serial console tab is displayed.

**Step 6** Click **Connect**.

**Step 7** A new browser tab is displayed. If the screen is black, press **Enter** to view the login prompt.

**Step 8** Log in to the serial console. If the password that was displayed in Step 4 does not work, refer to the Password Recovery section.

**Step 9** Use the application **reset-passwd ise iseadmin** command to set a new web UI password for the iseadmin account. The iseadmin account's web UI password is reset.

## View configured password

Follow these steps to view the configured password.

### Procedure

**Step 1** Click **Actions** in EC2 dashboard.

**Step 2** Go to **Instance Settings**.

**Step 3** Choose **Edit user data** to view the current password.

## Create a new public key pair

The existing key pair that was created at the time of Cisco ISE instance configuration is not replaced by the new public key that you create.

Follow these steps to create a new public key pair:

### Procedure

**Step 1** Create a new public key in AWS. For information on how to create public key pairs, refer to Create key pairs.

**Step 2** Log in to the AWS serial console as detailed in the preceding task.

**Step 3** To create a new repository to save the public key, refer to Creating a private repository.

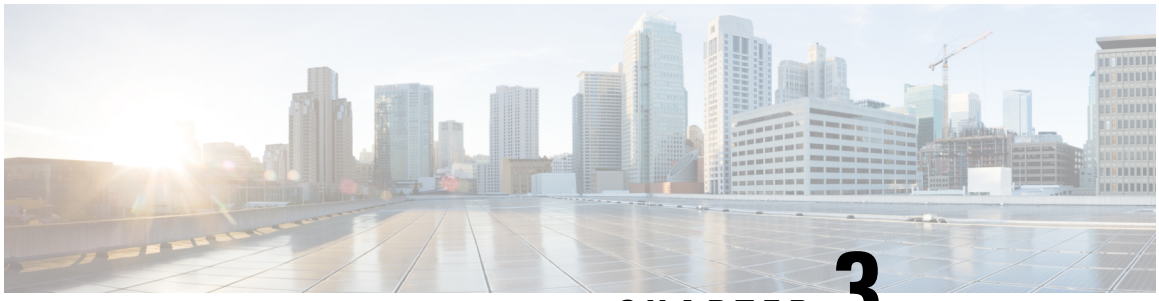
If you already have a repository that is accessible through the CLI, skip to the next step.

**Step 4** To import the new public key, use the command **crypto key import <public key filename> repository <repository name>**.

When the import is complete, you can log in to Cisco ISE through SSH using the new public key.

# Password recovery on AWS

There is no mechanism for password recovery for Cisco ISE on AWS. You may need to create new Cisco ISE instances and perform backup and restore of configuration data. Editing the user data for an EC2 instance in AWS does not change the CLI password that is used to log in to the serial console, as the setup script is not run. The Cisco ISE virtual instance is not affected.



CHAPTER 3

# Cisco ISE on Azure Cloud Services


- Cisco ISE on Azure cloud, on page 33
- Azure deployment methods, on page 33
- Azure VM sizes supported by Cisco ISE, on page 34
- Known limitations of Cisco ISE in Microsoft Azure cloud services, on page 36
- Out-of-order fragmentation limitation for Cisco ISE deployments on Azure, on page 37
- Create a Cisco ISE instance using an Azure VM, on page 38
- Edit disk size, on page 42
- Create a Cisco ISE instance using Azure application, on page 43
- Postinstallation tasks, on page 49
- Compatibility information for Cisco ISE on Azure cloud, on page 49
- Password recovery and reset on Azure cloud, on page 49


## Cisco ISE on Azure cloud

Cisco ISE is available on Azure cloud services. To configure and install Cisco ISE on Azure cloud, you must be familiar with Azure cloud features and solutions. Familiarize yourself with these Azure cloud concepts before starting:

- Subscriptions and resource groups
- Azure Virtual Machines. Refer to Instances, Images, SSH Keys, Tags, and VM Resizing.

## Azure deployment methods

You can deploy Cisco ISE on Microsoft Azure using an Azure application or an Azure VM.

There are no differences in cost or Cisco ISE features when you deploy Cisco ISE using an Azure application or an Azure VM.

We recommend using the Azure application for these advantages it offers in comparison to the Azure VM:

- Azure application allows you to easily configure Cisco ISE-specific choices directly through its UI instead of a user-data field as in the case of Azure VM configuration.

- At the initial configuration of an Azure application, you can choose an OS disk volume ranging between 300 and 2400 GB. However, during the initial configuration of an Azure VM, you can change the OS disk volume to a fixed set of values provided in the Azure portal.

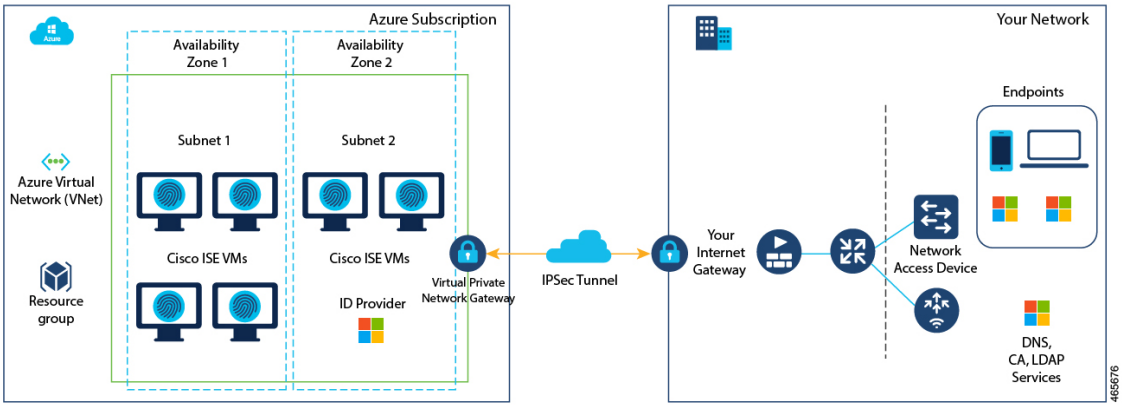
  You must carry out more steps after Cisco ISE installation and launch to reconfigure the virtual machine.
- You can directly choose from the specific Azure VM sizes that Cisco ISE supports.
- You can configure a static private IP address at the initial configuration.

You can use the Azure VM if:

- you do not use the Azure portal UI to deploy Cisco ISE.
- you need to use one of the additional settings that are available in the Azure VM configuration workflow.

This is an example of a deployment connected to the Azure cloud.

***Figure 2: Example of a deployment connected to Azure cloud***




In addition to these deployment methods, you can also use Cisco Developed Terraform Script to install and automatically create multi-node Cisco ISE deployments on Azure.

**Note** Do not clone an existing Azure cloud image to create a Cisco ISE instance.

# Azure VM sizes supported by Cisco ISE

Cisco ISE can be installed by using one of these Azure VM sizes.

*Table 7: Azure VM sizes that are supported by Cisco ISE*

| Azure VM sizes | vCPU | RAM (in GB) |
|---|---|---|
| Standard_D4s_v4<br>This instance supports the Cisco ISE evaluation use case. 100 concurrent active endpoints are supported. | 4 | 16 |
| Standard_D8s_v4 | 8 | 32 |
| Standard_F16s_v2 | 16 | 32 |
| Standard_F32s_v2 | 32 | 64 |
| Standard_D16s_v4 | 16 | 64 |
| Standard_D32s_v4 | 32 | 128 |
| Standard_D64s_v4 | 64 | 256 |

From Cisco ISE release 3.5, Standard_D4s_v4 and Standard_D16s_v4 VMs are not supported.

The Fsv2-series Azure VM sizes are compute-optimized and are best suited for use as PSNs for compute-intensive tasks and applications.

The Dsv4-series are general purpose Azure VM sizes that are best suited for use as PAN or MnT nodes or both and are intended for data processing tasks and database operations.

If you use a general purpose instance as a PSN, the performance numbers are lower than the performance of a compute-optimized instance as a PSN.

The Standard_D8s_v4 VM size must be used as an extra small PSN only.

For information on the scale and performance data for Azure VM sizes, refer to the *Performance and Scalability Guide for Cisco Identity Services Engine*.



**Note** Microsoft may retire, restrict, or change the availability, reservation purchase, or reservation renewal support for Azure VM sizes over time. Cisco periodically updates the list of Azure VM sizes supported for Cisco ISE as Azure platform support and Cisco ISE cloud integration evolve.

Review the latest Microsoft Azure VM lifecycle and reservation guidance before deploying, resizing, or purchasing reservations for Cisco ISE on Azure.

The most recent Microsoft guidance indicates changes beginning July 1, 2026, affecting Reserved VM Instance purchases and renewals for certain VM series, including the Fsv2 series. This list includes Cisco ISE-supported VM sizes such as Standard_F16s_v2 and Standard_F32s_v2.

If you are replacing Standard_F16s_v2 or Standard_F32s_v2, which are no longer available for reserved instance renewals, Cisco strongly recommends using Standard_D32s_v4 as the alternative Cisco ISE-supported VM size. These instances remain available on a Pay-As-You-Go basis until Microsoft discontinues support.

# 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.

# Create a Cisco ISE instance using an Azure VM

Cisco ISE can be deployed as a virtual machine in Microsoft Azure. Before creating an instance, prepare the required SSH key pair, virtual network gateways, subnets, security groups, and internet connectivity. For more information, refer to Overview of Cisco ISE instances on Azure.

Complete these prerequisites before you create the Cisco ISE instance:

- Create an SSH key pair.
- Create the virtual network gateways, required subnets, and security groups.
- Ensure that the subnet that you want to use with Cisco ISE can reach the internet. In Microsoft Azure, in the Public Route Table window, configure the next hop of the subnet as the internet.

To understand compatibility information and known limitations when working with Cisco ISE deployments on Azure, refer to Compatibility information and Known Limitations.

## Navigate to the Cisco ISE option on the Azure console

Follow these steps to navigate to the Cisco ISE option on the Azure console.

**Procedure**

**Step 1** Go to https://portal.azure.com and log in to your Microsoft Azure account.

**Step 2** Use the search field at the top of the window to search for **Marketplace**.

**Step 3** Use the **Search the Marketplace** search field to search for **Cisco Identity Services Engine (ISE)**.

## Configure instance details

Follow these steps to configure the instance details on the Azure console.

**Procedure**

**Step 1** Click **Virtual Machine**.

**Step 2** In the new window that is displayed, click **Create**.

**Step 3** In the **Basics** tab, perform these actions:

# Configure OS disk size

Follow these steps to configure OS disk size.

### Procedure

**Step 1** Click **Next: Disks**.

**Step 2** In the **Disks** tab, select a disk size from the **OS Disk Size** drop-down list or retain the default value.

**Note**
We recommend that you use a customer-managed key for disk encryption in the **Key Management** field. A platform-managed key is used by default. For more information on key creation, refer to About encryption key management.

For the rest of the mandatory fields, you can retain the default values.

# Configure network interface

Follow these steps to configure a network interface.

### Procedure

**Step 1** Click **Next: Networking**.

**Step 2** In the **Network Interface** area, from the **Virtual network** and **Subnet** drop-down lists, select the virtual network and subnet that you have created.

Note that a subnet with a public IP address receives online and offline posture feed updates, while a subnet with a private IP address receives only offline posture feed updates.

# Configure user details

Follow these steps to configure the user details.

### Procedure

**Step 1** Click **Next: Management**.

**Step 2** In the **Management** tab, retain the default values for the mandatory fields and click **Next: Advanced**.

**Step 3** In the **User data** field, enter the parameters in the correct format.

You must use the correct syntax for each of the fields that you configure through the user data entry. The information you enter in the **User data** field is not validated. If you use incorrect syntax, Cisco ISE services might not start when you launch the image.

Follow these guidelines for the configurations that you submit through the **User data** field:

***Table 8: Configuration guidelines for User Data field***

| Field Name | Field Description | Compliance and Behavior Changes |
|---|---|---|
| hostname | Enter a hostname that contains only alphanumeric characters and hyphen (-). The length of the hostname must be less than 19 characters and must not contain underscores (_). | Syntax must meet recommendations. |
| primarynameserver | Enter the IP address of the primary name server. Only IPv4 addresses are supported. | From Cisco ISE release 3.4:<br>• You can configure secondary and tertiary name servers during installation by using the **secondarynameserver** and **tertiarynameserver** fields. |
| secondarynameserver<br>(From Cisco ISE release 3.4) | Enter the IP address of the secondary name server. Only IPv4 addresses are supported. | • If you leave the **secondarynameserver** field blank and use only the **tertiarynameserver** field, the Cisco ISE services will not start. |
| tertiarynameserver<br>(From Cisco ISE release 3.4) | Enter the IP address of the tertiary name server. Only IPv4 addresses are supported. | Use only after secondarynameserver value is set. |
| dnsdomain | Enter the FQDN of the DNS domain. The entry can contain ASCII characters, numerals, hyphens (-), and periods (.). | Syntax must meet recommendations. |
| ntpserver<br>(renamed as **primaryntpserver** from Cisco ISE release 3.4) | Enter the IPv4 address or FQDN of the NTP server that must be used for synchronization, for example, time.nist.gov. | From Cisco ISE release 3.4:<br>• The **ntpserver** field name is changed to **primaryntpserver**. If you use **ntpserver**, Cisco ISE services will not start. |
| secondaryntpserver<br>(From Cisco ISE release 3.4) | Enter the IPv4 address or FQDN of the secondary NTP server. | • If you leave the **secondaryntpserver** field blank and use only the **tertiaryntpserver** field, the Cisco ISE services will not start. |

| Field Name | Field Description | Compliance and Behavior Changes |
|---|---|---|
| tertiaryntpserver<br>(From Cisco ISE release 3.4) | Enter the IPv4 address or FQDN of the tertiary NTP server. | Use only after secondaryntpserver value is set. |
| timezone | Enter a timezone, for example, Etc/UTC. We recommend that you set all the Cisco ISE nodes to the Coordinated Universal Time (UTC) timezone, especially if your Cisco ISE nodes are installed in a distributed deployment. This procedure ensures that the timestamps of the reports and logs from the various nodes in your deployment are always synchronized. | Syntax must meet recommendations. |
| password | Configure a password for GUI-based login to Cisco ISE. The password that you enter must comply with the Cisco ISE password policy. The password must contain 6 to 25 characters and include at least one numeral, one uppercase letter, and one lowercase letter. The password cannot contain or be the same as the username or its reverse (iseadmin or nimdaesi), cisco, or ocsic. The allowed special characters are @~*!,+=_-. . | Refer to "User Password Policy" section in the chapter "Basic Setup" of the Cisco ISE Administrator Guide for your release. |
| ersapi | Enter **yes** to enable ERS, or **no** to disallow ERS. | Syntax must meet recommendations. |
| openapi | Enter **yes** to enable OpenAPI, or **no** to disallow OpenAPI. | From Cisco ISE release 3.4, OpenAPI services are enabled by default. You don't have to specify OpenAPI-related options when launching an instance. |
| pxGrid | Enter **yes** to enable pxGrid, or **no** to disallow pxGrid. | Syntax must meet recommendations. |
| pxgrid_cloud | Enter **yes** to enable pxGrid Cloud, or **no** to disallow pxGrid Cloud. | To enable pxGrid Cloud, you must enable pxGrid. If you disallow pxGrid, but enable pxGrid Cloud, pxGrid Cloud services are not enabled at launch.<br>From Cisco ISE release 3.5, pxGrid Cloud can be enabled only from Cisco ISE Cisco ISE GUI. Therefore, this field is not included in the user data. |

# Configure tags

Follow these steps to configure your tags:

**Procedure**

**Step 1** Click **Next: Tags**.

**Step 2** To create name-value pairs that allow you to categorize and consolidate multiple resources and resource groups, enter values in the **Name** and **Value** fields.

# Review and create

Follow these steps to review the configurations you have created so far and to create a Cisco ISE instance.

**Procedure**

**Step 1** Click **Next: Review + Create**.

**Step 2** Review the information that you have provided so far and click **Create**.

The **Deployment is in progress** window is displayed. It takes about 30 minutes for the Cisco ISE instance to be created and available for use. The Cisco ISE VM instance is displayed in the **Virtual Machines** window (use the main search field to find the window).

# Edit disk size

This section is applicable only if the disk size of your Cisco ISE VM is 300 GB. If you have chosen any other disk size, then these steps are not applicable.

Due to Microsoft Azure default settings, the Cisco ISE VM is configured with only 300 GB disk size. Cisco ISE nodes typically require more than 300 GB disk size. You might see the **Insufficient Virtual Memory** alarm when you first launch Cisco ISE from Microsoft Azure.

After you create the Cisco ISE VM, log in to the Cisco ISE administration portal to verify that Cisco ISE is set up correctly. Then, in the Microsoft Azure portal, carry out these steps in the **Virtual Machines** page to edit the disk size:

**Procedure**

**Step 1** Stop the Cisco ISE instance.

**Step 2** Click **Disk** in the left pane, and click the disk that you are using with Cisco ISE.

**Step 3** Click **Size + performance** in the left pane.

**Step 4** In the **Custom disk size** field, enter the disk size you want in GiB.

# Create a Cisco ISE instance using Azure application

Before creating a Cisco ISE instance, create the Azure resources that you need, such as Resource Groups, Virtual Networks, Subnets, SSH keys, and so on.

## Navigate to the Cisco ISE option on the Azure console

Follow these steps to navigate to the Cisco ISE option on the Azure console.

### Procedure

**Step 1** Go to https://portal.azure.com and log in to your Microsoft Azure account.

**Step 2** Use the search field at the top of the window to search for **Marketplace**.

**Step 3** Use the **Search the Marketplace** search field to search for **Cisco Identity Services Engine (ISE)**.

## Add instance details

Follow these steps to add the basic configuration details for the Cisco ISE instance.

### Procedure

**Step 1** Click **Azure Application**.

**Step 2** In the new window that is displayed, click **Create**.
A five-step workflow is displayed.

**Step 3** From the **Basics** tab, perform these actions.

## Configure network settings

Follow these steps to configure the network settings.

### Procedure

**Step 1** Click **Next**.

**Step 2** In the **Network Settings** tab, enter these details:

From Cisco ISE release 3.4,

- the **NTP Server** field name is changed to **Primary NTP Server**.
- the IP address or hostname of the secondary NTP server can be entered in the **Secondary NTP Server** field. Your entry is not validated upon input.
- the IP address or hostname of the tertiary NTP server can be entered in the **Tertiary NTP Server** field. Your entry is not validated upon input. To use this field and to launch the application successfully, you must not leave the **Secondary NTP Server** field blank.

You can add only one NTP server in this step. You can add additional NTP servers through the Cisco ISE CLI after installation.

**Note**
If the entered IP address is incorrect or not reachable, Cisco ISE services may not be launched.

# Configure services

Follow these steps to configure the services.

**Procedure**

In the **Services** tab:

a) From the **ERS** drop-down list, choose **Yes** or **No**.
b) From the **Open API** drop-down list, choose **Yes** or **No**. From Cisco ISE release 3.4, OpenAPIs are enabled by default. Therefore, this field is unavailable.
c) From the **pxGrid** drop-down list, choose **Yes** or **No**.
d) From the **pxGrid Cloud** drop-down list, choose **Yes** or **No**. From Cisco ISE release 3.5, pxGrid Cloud can be enabled only from the Cisco ISE GUI. Therefore, this field is unavailable.

# Add user details

Follow these steps to add the user details.

**Procedure**

**Step 1** Click **Next** to go to the **User Details** tab.
**Step 2** In the **User Details** tab, enter the password in the **Enter Password for iseadmin** and **Confirm Password** fields.

The password must comply with the Cisco ISE password policy and contain a maximum of 25 characters.

# User data parameters

This table lists the supported user data parameters, their required formats, and their availability across Cisco ISE releases. Refer to it when entering user data in the **Advanced > User data** section during Azure VM deployment.

| Field | Format | Cisco ISE release 3.1 | Cisco ISE release 3.2 | Cisco ISE release 3.3 | Cisco ISE release 3.4 | Cisco ISE release 3.5 |
|---|---|---|---|---|---|---|
| hostname | hostname=<hostname of Cisco ISE> | Supported | Supported | Supported | Supported | Supported |
| primarynameserver | primarynameserver=<IPv4 address><br>(primarynameserver=<IPv6 address> supported for AWS from Cisco ISE release 3.5) | Supported | Supported | Supported | Supported | Supported<br>Cisco ISE release 3.5 and later support IPv6 addresses in AWS deployments. |
| secondarynameserver | secondarynameserver=<IPv4 address><br>(secondarynameserver=<IPv6 address> supported for AWS from Cisco ISE release 3.5) | Not supported | Not supported | Not supported | Supported.<br>You must enter a value in this field if you want to use the tertiarynameserver field. | Supported.<br>You must enter a value in this field if you want to use the tertiarynameserver field.<br>Cisco ISE release 3.5 and later support IPv6 addresses in AWS deployments. |

| Field | Format | Cisco ISE release 3.1 | Cisco ISE release 3.2 | Cisco ISE release 3.3 | Cisco ISE release 3.4 | Cisco ISE release 3.5 |
|---|---|---|---|---|---|---|
| tertiarynameserver | tertiarynameserver=<IPv4 address><br>(tertiarynameserver=<IPv6 address> supported for AWS from Cisco ISE release 3.5) | Not supported | Not supported | Not supported | Supported.<br>You must first enter a value in the secondarynameserver field if you want to use this field. | Supported.<br>You must first enter a value in the secondarynameserver field if you want to use this field.<br>Cisco ISE release 3.5 and later support IPv6 addresses in AWS deployments. |
| dnsdomain | dnsdomain=<example.com> | Supported | Supported | Supported | Supported | Supported |
| ntpserver | ntpserver=<IPv4 address or FQDN of the NTP server><br>(ntpserver=<IPv6 address or FQDN of the NTP server> supported for AWS from Cisco ISE release 3.5) | Supported | Supported | Supported | Not supported.<br>This field is replaced by primaryntpserver in Cisco ISE release 3.4 and later. Using ntpserver may prevent Cisco ISE services from starting. | Not supported. Use primaryntpserver instead. |
| primaryntpserver | primaryntpserver=<IPv4 address or FQDN><br>(primaryntpserver=<IPv6 address or FQDN of the NTP server> supported for AWS from Cisco ISE release 3.5) | Not supported | Not supported | Not supported | Supported.<br>This field replaces ntpserver in Cisco ISE release 3.4 and later. | Supported.<br>Cisco ISE release 3.5 and later support IPv6 addresses in AWS deployments. |

| Field | Format | Cisco ISE release 3.1 | Cisco ISE release 3.2 | Cisco ISE release 3.3 | Cisco ISE release 3.4 | Cisco ISE release 3.5 |
|---|---|---|---|---|---|---|
| secondaryntpserver | secondaryntpserver=<IPv4 address or FQDN><br>(secondaryntpserver=<IPv6 address or FQDN of the NTP server> supported for AWS from Cisco ISE release 3.5) | Not supported | Not supported | Not supported | Supported.<br>You must enter a value in this field if you want to use the tertiaryntpserver field. | Supported.<br>You must enter a value in this field if you want to use the tertiaryntpserver field.<br>Cisco ISE release 3.5 and later support IPv6 addresses in AWS deployments. |
| tertiaryntpserver | tertiaryntpserver=<IPv4 address or FQDN><br>(tertiaryntpserver=<IPv6 address or FQDN of the NTP server> supported for AWS from Cisco ISE release 3.5) | Not supported | Not supported | Not supported | Supported.<br>You must first enter a value in the secondaryntpserver field if you want to use this field. | Supported.<br>You must first enter a value in the secondaryntpserver field if you want to use this field.<br>Cisco ISE release 3.5 and later support IPv6 addresses in AWS deployments. |
| timezone | timezone=<timezone> | Supported | Supported | Supported | Supported | Supported |
| username | username=<admin> | Supported (example: <admin>)<br>Supported from Cisco ISE release 3.1 patch 1. | Not supported.<br>iseadmin is the default user. | Not supported.<br>iseadmin is the default user. | Not supported.<br>iseadmin is the default user. | Not supported.<br>iseadmin is the default user. |
| username | username=iseadmin | Not mandatory | Mandatory | Mandatory | Mandatory | Mandatory |
| password | password=<password> | Supported | Supported | Supported | Supported | Supported |
| ersapi | ersapi=<yes/no> | Supported | Supported | Supported | Supported | Supported |
| openapi | openapi=<yes/no> | Supported | Supported | Supported | OpenAPI is enabled by default. | OpenAPI is enabled by default. |
| pxGrid | pxGrid=<yes/no> | Supported | Supported | Supported | Supported | Supported |

| Field | Format | Cisco ISE release 3.1 | Cisco ISE release 3.2 | Cisco ISE release 3.3 | Cisco ISE release 3.4 | Cisco ISE release 3.5 |
|---|---|---|---|---|---|---|
| pxgrid_cloud | pxgrid_cloud=<yes/no> | Not supported | Not supported | Supported.<br>This is only supported for Cisco ISE releases 3.3 and 3.4. | Supported.<br>This is only supported for Cisco ISE releases 3.3 and 3.4. | Not supported.<br>From Cisco ISE release 3.5, pxGrid Cloud can be enabled only from the Cisco ISE GUI. |

#### Parameter syntax requirements

When specifying user data parameters for Cisco ISE on Cloud, do not enclose any attribute or value in single or double quotes. You must enter all values in plain text, without quotes.

| Invalid entry | Valid entry |
|---|---|
| hostname="i34a" | hostname=i34a |
| primarynameserver="9.9.9.9" | primarynameserver=9.9.9.9 |
| dnsdomain="example.com" | dnsdomain=example.com |
| primaryntpserver="north-america.pool.ntp.org" | primaryntpserver=north-america.pool.ntp.org |

From Cisco ISE release 3.3, validation output messages are displayed in the serial console. These messages are visible only if the serial console is open at the time the output is generated.

# Review and create

Follow these steps to review your configurations and create a Cisco ISE instance.

#### Procedure

**Step 1** In the **Review + create** tab, review the details of the instance.

**Step 2** Click **Create**.

The **Overview** window displays the progress of the instance creation.

**Step 3** Use the search bar and navigate to the **Virtual Machines** window.

Your Cisco ISE instance is listed in the **Virtual Machines** window. It takes about 30 minutes to create a Cisco ISE instance.

### What to do next

To verify the instances and learn about the tasks to perform after deployment, refer to Installation Verification and Post-Installation Tasks.

# Postinstallation tasks

For information about the postinstallation tasks that you must carry out after creating a Cisco ISE instance, refer to the chapter "Installation Verification and Postinstallation Tasks" in the *Cisco ISE Installation Guide* for your release.

# Compatibility information for Cisco ISE on Azure cloud

This section provides compatibility information that is unique to Cisco ISE on Azure cloud. For general compatibility details for Cisco ISE, refer to the Cisco Identity Services Engine Network Component Compatibility guide for your release.

## Load balancer integration support

You can integrate the Azure Load Balancer with Cisco ISE for load balancing RADIUS traffic. However, these caveats are applicable:

- The Change of Authorization (CoA) feature is supported only if client IP preservation is enabled when you configure Session Persistence property in the load balancing rule in the Azure portal.
- Unequal load balancing might occur as the Azure Load Balancer supports only source IP affinity and does not support calling station ID-based sticky sessions.
- Traffic can be sent to a PSN even if the RADIUS service is not active on the node, because the Azure Load Balancer does not support RADIUS-based health checks.

For more information on the Azure Load Balancer, refer to What is Azure Load Balancer?.

You can integrate the Azure 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 the Azure Load Balancer does not support health checks based on TACACS+ services.

# Password recovery and reset on Azure cloud

You can reset or recover your Cisco ISE VM password using these tasks. Select the necessary tasks and follow the detailed steps.

The **Help** > **Reset Password** option in the Azure portal is not supported for Cisco ISE Azure VM.

# Reset Cisco ISE GUI password through serial console

### Procedure

**Step 1** Log in to Azure Cloud and choose the resource group that contains your Cisco ISE virtual machine.

**Step 2** From the list of resources, click the Cisco ISE instance for which you want to reset the password.

**Step 3** From the left-side menu, in the **Help** section, click **Serial console**.

The Azure Cloud Shell is displayed in a new window.

If the screen is black, press **Enter** to view the login prompt.

If you view an error message here, you may have to enable boot diagnostics by carrying out these steps:

**a.** From the left-side menu, click **Boot diagnostics**.

**b.** Click **Enable with custom storage account**.

**c.** Choose the storage account and click **Save**.

**Step 4** Log in to the serial console.

To log in to the serial console, you must use the original password that was configured at the installation of the instance.

Use the **application reset-passwd ise iseadmin** command to configure a new GUI password for the iseadmin account.

# Create new public key pair for SSH access

Follow these steps to add additional key pairs to a repository.

The existing key pair that was created at the time of Cisco ISE instance configuration is not replaced by the new public key that you create.

### Procedure

**Step 1** Create a new public key in Azure Cloud. Refer to Generate and store SSH keys in the Azure portal.

**Step 2** Log in to the Azure Cloud serial console.

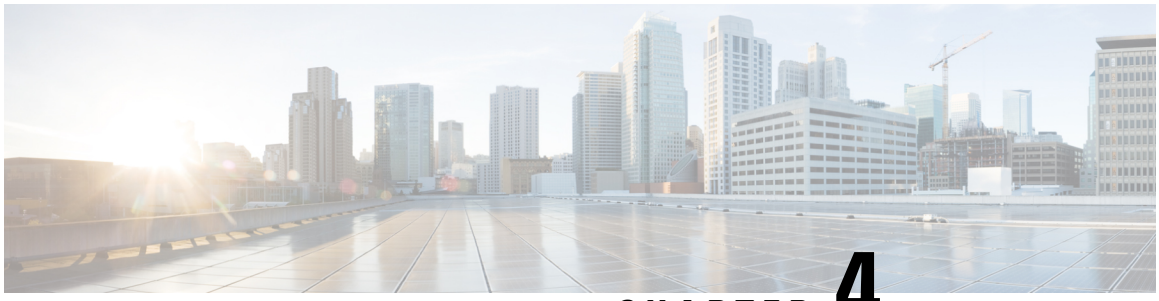
**Step 3** To create a new repository to save the public key, refer to Azure Repos documentation.

If you already have a repository that is accessible through the CLI, skip to step 4.

**Step 4** To import the new public key, use this command:

**crypto key import <public key filename> repository <repository name>**

When the import is complete, you can log in to Cisco ISE via SSH using the new public key.



CHAPTER 4

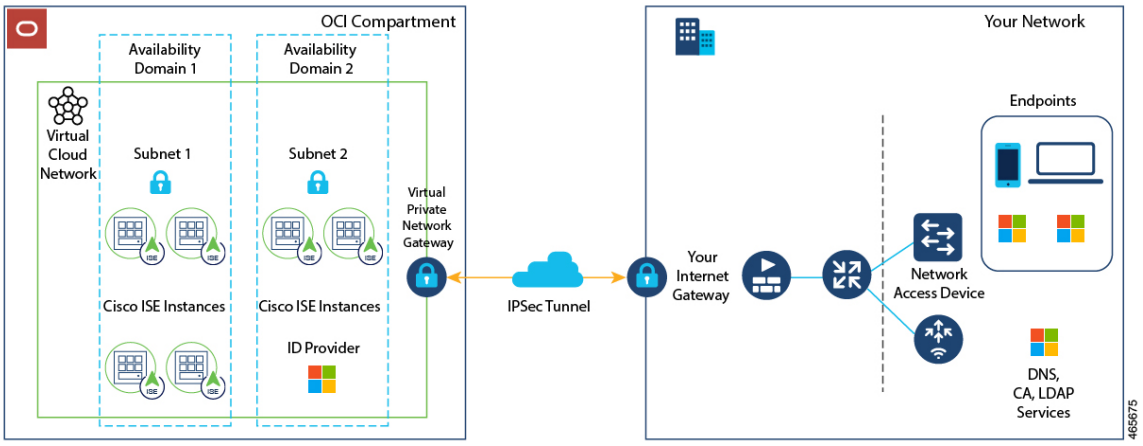
# Cisco ISE on Oracle Cloud Infrastructure


- Cisco ISE on Oracle Cloud Infrastructure, on page 51
- OCI instances supported by Cisco ISE, on page 52
- Known limitations of using Cisco ISE on OCI, on page 52
- Create a Cisco ISE instance in OCI, on page 53
- Create a Cisco ISE instance in OCI using a Terraform Stack file, on page 61
- Postinstallation tasks, on page 62
- Compatibility information for Cisco ISE on OCI, on page 63
- Password recovery and reset on OCI, on page 63


## Cisco ISE on Oracle Cloud Infrastructure

Cisco ISE is available on Oracle Cloud Infrastructure (OCI) in two forms: Image and Stack. We recommend that you use the stack type to install Cisco ISE because this resource type is customized for ease of use for Cisco ISE users.

This figure shows an example of a deployment connected to Oracle Cloud.




To configure and install Cisco ISE on OCI, you must be familiar with certain OCI features and solutions. Before you begin, understand compartments, availability domains, images, shapes, and boot volumes.

OCI uses Oracle CPUs (OCPUs) as its compute resource unit. One OCPU equals two vCPUs. For more information, refer to Oracle Cloud Infrastructure Documentation.

**Important** Do not clone an existing OCI image to create a Cisco ISE instance.

# OCI instances supported by Cisco ISE

You can use these OCI instances with Cisco ISE.

| OCI instance type | OCPU | OCI instance memory (in GB) |
|---|---|---|
| Standard3.Flex<br>This instance supports the Cisco ISE evaluation use case. 100 concurrent active endpoints are supported. | 2 | 16 |
| Optimized3.Flex | 8 | 32 |
| | 16 | 64 |
| Standard3.Flex | 4 | 32 |
| | 8 | 64 |
| | 16 | 128 |
| | 32 | 256 |

The Optimized3.Flex shapes are compute-optimized instances. They are best suited for use as PSNs for compute-intensive tasks and applications.

The Standard3.Flex shapes are general purpose shapes that are best suited for use as PAN or MnT nodes or both. These shapes are intended for data processing tasks and database operations.

If you use a general purpose instance as a PSN, the performance numbers are lower than that of a compute-optimized instance as a PSN.

The Standard3.Flex (4 OCPU, 32 GB) shape must be used as an extra-small PSN only.

From Cisco ISE release 3.5, Standard3.Flex instances with these configurations are not supported:

- 2 OCPUs and 16 GB memory
- 8 OCPUs and 64 GB memory

For information on the scale and performance data for OCI instance types, refer to the *Performance and Scalability Guide for Cisco Identity Services Engine*.

# Known limitations of using Cisco ISE on OCI

- The Cisco ISE upgrade workflow is not supported for OCI. Only fresh installs are supported. However, you can back up and restore 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 OCI do not support functions that depend on Layer 2 capabilities. For example, DHCP SPAN profiler probes and CDP protocol functions that are accessed through the Cisco ISE CLI are not supported.
- To enable IPv6 addresses in Cisco ISE, configure an IPv6 address in the OCI portal for Cisco ISE and restart interface Gigabit Ethernet 0. Log in as an administrator in the Cisco ISE Serial Console and run these commands:

```
#configure terminal
Entering configuration mode terminal
(config)#interface GigabitEthernet 0
(config-GigabitEthernet-0)#shutdown
(config-GigabitEthernet-0)#no shutdown
(config-GigabitEthernet-0)#exit
(config)#exit
```

- When you carry out the restore and backup function of configuration data, after the backup operation is complete, first restart Cisco ISE through the CLI. Then, initiate the restore operation from the Cisco ISE GUI. For more information on the Cisco ISE backup and restore processes, refer to the chapter "Maintain and Monitor" in the *Cisco ISE Administrator Guide* for your release.
- SSH access to Cisco ISE CLI using password-based authentication is not supported in OCI. You can only access the Cisco ISE CLI through a key pair. Store this key pair securely.

  If you lose your Private Key (or PEM) file, you cannot access the Cisco ISE CLI.

  Any integration that uses a password-based authentication method to access Cisco ISE CLI is not supported, for example, Cisco Catalyst Center 2.1.2 and earlier releases.

# Create a Cisco ISE instance in OCI

Follow these steps to create a Cisco ISE instance in OCI.

### Before you begin

- Create compartments, custom images, shapes, virtual cloud networks, subnets, and site-to-site VPNs before starting this task.

  Create the virtual cloud networks and subnets in the same compartment as your Cisco ISE instance.
- When you create a virtual cloud network for Cisco ISE, we recommend that you choose the **Create VCN with Internet Connectivity** VCN type.
- To understand post-installation tasks and known limitations when working with Cisco ISE deployments on OCI, refer to Installation Verification and Post-Installation Tasks and Known limitations.

### Procedure

**Step 1** Navigate to the Cisco ISE option on the OCI console, on page 54.

**Step 2** Configure instance details, on page 54.

**Step 3** Configure advanced options for a Cisco ISE instance, on page 55.

# Navigate to the Cisco ISE option on the OCI console

Follow these steps to navigate to the Cisco Identity Services Engine (ISE) option on the OCI console.

### Procedure

**Step 1** Log in to your OCI account.

**Step 2** In the search field, enter **Marketplace**.

**Step 3** In the **Search for listings** search field, enter **Cisco Identity Services Engine (ISE)**.

# Configure instance details

Follow these steps to add and configure Cisco ISE instance details on the OCI console.

### Procedure

**Step 1** Click the Cisco ISE option that is of **Image** type and click **Launch Instance**.

**Step 2** In the **List Scope** area, from the **Compartment** drop-down list, choose a compartment.

a) Click **Create Instance**.

**Step 3** In the **Create Compute Instance** window, enter a name for your Cisco ISE instance.

a) From the **Create in compartment** drop-down list, choose the compartment for the Cisco ISE instance.

Choose the compartment where you created other resources, such as virtual cloud networks and subnets for Cisco ISE.

**Step 4** In the **Placement** area, click an availability domain.

The domain determines the compute shapes that are available to you.

**Step 5** In the **Image and Shape** area:

a) From the **Image and Shape** area, click **Change Shape**.

b) From the **Shape Series** area, click **Intel**.

A list of available shapes is displayed.

c) Check the check box next to the required shape name and click **Select Shape**.

**Step 6** In the **Networking** area:

a) In the **Primary Network** area, click the **Select existing virtual cloud network** radio button.

b) Choose a virtual cloud network from the drop-down list.

c) In the **Subnet** area, click **Select existing subnet**.

d) Choose a subnet from the drop-down list.

The system displays the subnets that are created in the same compartment.

**Step 7** In the **Add SSH Keys** area, you can either generate a key pair or use an existing public key by clicking the corresponding radio button.

**Step 8** In the **Boot Volume** area, check the **Specify a custom boot volume size** check box and enter the required boot volume in GB.

The minimum volume required for a Cisco ISE production environment is 600 GB. The default volume assigned to an instance is 250 GB if a boot volume is not specified in this step.

**Note**
Use a customer-managed key for encryption in the **Encrypt this volume with a key that you manage** field. By default, Oracle-managed key is used. For more information on key creation, refer to Key Management.

# Configure advanced options for a Cisco ISE instance

To configure the advanced options, follow these steps.

**Procedure**

**Step 1** Click **Show advanced options**.

**Step 2** In the **Management** tab, under the **Instance metadata service** section, disable the **Require an authorization header** toggle.

**Note**
Cisco ISE on OCI does not support IMDSv2.

**Step 3** In the **Initialization script** tab, choose the **Paste cloud-init script** option.

**Step 4** In the **Cloud-init script** text box, enter the required user data.

**Step 5** In the **User data** field, enter the parameters in the correct format.

You must use the correct syntax for each of the fields that you configure through the user data entry. The information you enter in the **User data** field is not validated. If you use incorrect syntax, Cisco ISE services might not start when you launch the image.

Follow these guidelines for the configurations that you submit through the **User data** field:

***Table 9: Configuration guidelines for User Data field***

| Field Name | Field Description | Compliance and Behavior Changes |
|---|---|---|
| hostname | Enter a hostname that contains only alphanumeric characters and hyphen (-). The length of the hostname must be less than 19 characters and must not contain underscores (_). | Syntax must meet recommendations. |

| Field Name | Field Description | Compliance and Behavior Changes |
|---|---|---|
| primarynameserver | Enter the IP address of the primary name server. Only IPv4 addresses are supported. | From Cisco ISE release 3.4:<br>• You can configure secondary and tertiary name servers during installation by using the **secondarynameserver** and **tertiarynameserver** fields. |
| secondarynameserver<br>(From Cisco ISE release 3.4) | Enter the IP address of the secondary name server. Only IPv4 addresses are supported. | • If you leave the **secondarynameserver** field blank and use only the **tertiarynameserver** field, the Cisco ISE services will not start. |
| tertiarynameserver<br>(From Cisco ISE release 3.4) | Enter the IP address of the tertiary name server. Only IPv4 addresses are supported. | Use only after secondarynameserver value is set. |
| dnsdomain | Enter the FQDN of the DNS domain. The entry can contain ASCII characters, numerals, hyphens (-), and periods (.). | Syntax must meet recommendations. |
| ntpserver<br>(renamed as **primaryntpserver** from Cisco ISE release 3.4) | Enter the IPv4 address or FQDN of the NTP server that must be used for synchronization, for example, time.nist.gov. | From Cisco ISE release 3.4:<br>• The **ntpserver** field name is changed to **primaryntpserver**. If you use **ntpserver**, Cisco ISE services will not start. |
| secondaryntpserver<br>(From Cisco ISE release 3.4) | Enter the IPv4 address or FQDN of the secondary NTP server. | • If you leave the **secondaryntpserver** field blank and use only the **tertiaryntpserver** field, the Cisco ISE services will not start. |
| tertiaryntpserver<br>(From Cisco ISE release 3.4) | Enter the IPv4 address or FQDN of the tertiary NTP server. | Use only after secondaryntpserver value is set. |
| timezone | Enter a timezone, for example, Etc/UTC. We recommend that you set all the Cisco ISE nodes to the Coordinated Universal Time (UTC) timezone, especially if your Cisco ISE nodes are installed in a distributed deployment. This procedure ensures that the timestamps of the reports and logs from the various nodes in your deployment are always synchronized. | Syntax must meet recommendations. |

| Field Name | Field Description | Compliance and Behavior Changes |
|---|---|---|
| password | Configure a password for GUI-based login to Cisco ISE. The password that you enter must comply with the Cisco ISE password policy. The password must contain 6 to 25 characters and include at least one numeral, one uppercase letter, and one lowercase letter. The password cannot contain or be the same as the username or its reverse (iseadmin or nimdaesi), cisco, or ocsic. The allowed special characters are @~*!,+=_-. . | Refer to "User Password Policy" section in the chapter "Basic Setup" of the Cisco ISE Administrator Guide for your release. |
| ersapi | Enter **yes** to enable ERS, or **no** to disallow ERS. | Syntax must meet recommendations. |
| openapi | Enter **yes** to enable OpenAPI, or **no** to disallow OpenAPI. | From Cisco ISE release 3.4, OpenAPI services are enabled by default. You don't have to specify OpenAPI-related options when launching an instance. |
| pxGrid | Enter **yes** to enable pxGrid, or **no** to disallow pxGrid. | Syntax must meet recommendations. |
| pxgrid_cloud | Enter **yes** to enable pxGrid Cloud, or **no** to disallow pxGrid Cloud. | To enable pxGrid Cloud, you must enable pxGrid. If you disallow pxGrid, but enable pxGrid Cloud, pxGrid Cloud services are not enabled at launch.<br>From Cisco ISE release 3.5, pxGrid Cloud can be enabled only from Cisco ISE Cisco ISE GUI. Therefore, this field is not included in the user data. |

**Step 6** Click **Create**.

It takes about 30 minutes for the instance to be created and available for use. The Cisco ISE instance is listed in the **Instances** page.

# User data parameters

This table lists the supported user data parameters, their required formats, and their availability across Cisco ISE releases. Refer to it when entering user data in the **Advanced > User data** section during Azure VM deployment.

| Field | Format | Cisco ISE release 3.1 | Cisco ISE release 3.2 | Cisco ISE release 3.3 | Cisco ISE release 3.4 | Cisco ISE release 3.5 |
|---|---|---|---|---|---|---|
| hostname | hostname=<hostname of Cisco ISE> | Supported | Supported | Supported | Supported | Supported |

| Field | Format | Cisco ISE release 3.1 | Cisco ISE release 3.2 | Cisco ISE release 3.3 | Cisco ISE release 3.4 | Cisco ISE release 3.5 |
|---|---|---|---|---|---|---|
| primarynameserver | primarynameserver=<IPv4 address><br>(primarynameserver=<IPv6 address> supported for AWS from Cisco ISE release 3.5) | Supported | Supported | Supported | Supported | Supported<br>Cisco ISE release 3.5 and later support IPv6 addresses in AWS deployments. |
| secondarynameserver | secondarynameserver=<IPv4 address><br>(secondarynameserver=<IPv6 address> supported for AWS from Cisco ISE release 3.5) | Not supported | Not supported | Not supported | Supported.<br>You must enter a value in this field if you want to use the tertiarynameserver field. | Supported.<br>You must enter a value in this field if you want to use the tertiarynameserver field.<br>Cisco ISE release 3.5 and later support IPv6 addresses in AWS deployments. |
| tertiarynameserver | tertiarynameserver=<IPv4 address><br>(tertiarynameserver=<IPv6 address> supported for AWS from Cisco ISE release 3.5) | Not supported | Not supported | Not supported | Supported.<br>You must first enter a value in the secondarynameserver field if you want to use this field. | Supported.<br>You must first enter a value in the secondarynameserver field if you want to use this field.<br>Cisco ISE release 3.5 and later support IPv6 addresses in AWS deployments. |
| dnsdomain | dnsdomain=<example.com> | Supported | Supported | Supported | Supported | Supported |

| Field | Format | Cisco ISE release 3.1 | Cisco ISE release 3.2 | Cisco ISE release 3.3 | Cisco ISE release 3.4 | Cisco ISE release 3.5 |
|---|---|---|---|---|---|---|
| ntpserver | ntpserver=<IPv4 address or FQDN of the NTP server><br>(ntpserver=<IPv6 address or FQDN of the NTP server> supported for AWS from Cisco ISE release 3.5) | Supported | Supported | Supported | Not supported.<br>This field is replaced by primaryntpserver in Cisco ISE release 3.4 and later. Using ntpserver may prevent Cisco ISE services from starting. | Not supported. Use primaryntpserver instead. |
| primaryntpserver | primaryntpserver=<IPv4 address or FQDN><br>(primaryntpserver=<IPv6 address or FQDN of the NTP server> supported for AWS from Cisco ISE release 3.5) | Not supported | Not supported | Not supported | Supported.<br>This field replaces ntpserver in Cisco ISE release 3.4 and later. | Supported.<br>Cisco ISE release 3.5 and later support IPv6 addresses in AWS deployments. |
| secondaryntpserver | secondaryntpserver=<IPv4 address or FQDN><br>(secondaryntpserver=<IPv6 address or FQDN of the NTP server> supported for AWS from Cisco ISE release 3.5) | Not supported | Not supported | Not supported | Supported.<br>You must enter a value in this field if you want to use the tertiaryntpserver field. | Supported.<br>You must enter a value in this field if you want to use the tertiaryntpserver field.<br>Cisco ISE release 3.5 and later support IPv6 addresses in AWS deployments. |

| Field | Format | Cisco ISE release 3.1 | Cisco ISE release 3.2 | Cisco ISE release 3.3 | Cisco ISE release 3.4 | Cisco ISE release 3.5 |
|---|---|---|---|---|---|---|
| tertiaryntpserver | tertiaryntpserver=<IPv4 address or FQDN><br>(tertiaryntpserver=<IPv6 address or FQDN of the NTP server> supported for AWS from Cisco ISE release 3.5) | Not supported | Not supported | Not supported | Supported.<br>You must first enter a value in the secondaryntpserver field if you want to use this field. | Supported.<br>You must first enter a value in the secondaryntpserver field if you want to use this field.<br>Cisco ISE release 3.5 and later support IPv6 addresses in AWS deployments. |
| timezone | timezone=<timezone> | Supported | Supported | Supported | Supported | Supported |
| username | username=<admin> | Supported (example: <admin>)<br>Supported from Cisco ISE release 3.1 patch 1. | Not supported.<br>iseadmin is the default user. | Not supported.<br>iseadmin is the default user. | Not supported.<br>iseadmin is the default user. | Not supported.<br>iseadmin is the default user. |
| username | username=iseadmin | Not mandatory | Mandatory | Mandatory | Mandatory | Mandatory |
| password | password=<password> | Supported | Supported | Supported | Supported | Supported |
| ersapi | ersapi=<yes/no> | Supported | Supported | Supported | Supported | Supported |
| openapi | openapi=<yes/no> | Supported | Supported | Supported | OpenAPI is enabled by default. | OpenAPI is enabled by default. |
| pxGrid | pxGrid=<yes/no> | Supported | Supported | Supported | Supported | Supported |
| pxgrid_cloud | pxgrid_cloud=<yes/no> | Not supported | Not supported | Supported.<br>This is only supported for Cisco ISE releases 3.3 and 3.4. | Supported.<br>This is only supported for Cisco ISE releases 3.3 and 3.4. | Not supported.<br>From Cisco ISE release 3.5, pxGrid Cloud can be enabled only from the Cisco ISE GUI. |

### Parameter syntax requirements

When specifying user data parameters for Cisco ISE on Cloud, do not enclose any attribute or value in single or double quotes. You must enter all values in plain text, without quotes.

| Invalid entry | Valid entry |
|---|---|
| hostname="i34a" | hostname=i34a |
| primarynameserver="9.9.9.9" | primarynameserver=9.9.9.9 |
| dnsdomain="example.com" | dnsdomain=example.com |
| primaryntpserver="north-america.pool.ntp.org" | primaryntpserver=north-america.pool.ntp.org |

From Cisco ISE release 3.3, validation output messages are displayed in the serial console. These messages are visible only if the serial console is open at the time the output is generated.

# Create a Cisco ISE instance in OCI using a Terraform Stack file

Follow these steps to create a Cisco ISE instance in OCI using a Terraform Stack file.

### Before you begin

Create the resources needed for your Cisco ISE instance, such as SSH keys, Virtual Cloud Network (VCN), subnets, network security groups, and other required components in OCI. For information about using Terraform in OCI, refer to the Oracle documentation.

### Procedure

**Step 1** Create a Cisco ISE stack in OCI, on page 61.
**Step 2** Configure variables for Cisco ISE instance, on page 62.
**Step 3** Review configurations and create a Cisco ISE instance in OCI, on page 62.

# Create a Cisco ISE stack in OCI

Follow these steps to create a Cisco ISE stack in OCI.

### Procedure

**Step 1** Log in to your OCI account.
**Step 2** Use the search field to search for **Marketplace**.
**Step 3** In the **Search for listings** field, enter **Cisco Identity Services Engine (ISE)**.
**Step 4** Click **Cisco Identity Services Engine (ISE) Stack**.
**Step 5** In the new window that is displayed, click **Create Stack**.
**Step 6** In the **Stack Information** window:
a) Click **My Configuration**.

b) From the **Create in Compartment** drop-down list, select the compartment in which you want to create the Cisco ISE instance.

# Configure variables for Cisco ISE instance

Follow these steps to configure the variables for your Cisco ISE instance.

### Procedure

**Step 1** In the **Configure Variables** page:

**Step 2** Click **Next**.

In the **Review** window, a summary of all the configurations defined in the stack is displayed.

# Review configurations and create a Cisco ISE instance in OCI

Follow these steps to review the configurations you have created so far and to create the Cisco ISE instance.

### Procedure

**Step 1** Review the information and click **Previous** to make changes, if any.

**Step 2** In the **Run Apply on the created stack?** area, check the **Run Apply** check box to build the stack when you click **Create**.

If you do not select **Run Apply**, the stack information is saved when you click **Create**. You can choose the stack from the **Stacks** window later and click **Apply** to execute the build.

**Step 3** Click **Create**.

**Step 4** Navigate to the **Instances** window in OCI.

The instance is listed with the hostname that you provided in the stack form. Click the hostname to view the configuration details.

The Cisco ISE instance will be ready for launch in OCI in about 30 minutes.

# Postinstallation tasks

For information about the postinstallation tasks that you must carry out after creating a Cisco ISE instance, refer to the chapter "Installation Verification and Postinstallation Tasks" in the *Cisco ISE Installation Guide* for your release.

# Compatibility information for Cisco ISE on OCI

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

## Load balancer integration support

You can integrate OCI-native network load balancer with Cisco ISE for load balancing RADIUS traffic. However, these caveats are applicable:

- The Change of Authorization (CoA) feature is supported only when you enable client IP preservation in the Source or Destination Header (IP,Port) Preservation section when you create the network load balancer.
- Unequal load balancing might occur because the network load balancer supports only source IP affinity and does not support calling station ID-based sticky sessions.
- The network load balancer might send traffic to a PSN even if the RADIUS service is not active on the node, because it does not support RADIUS-based health checks.

For more information on the OCI-native network load balancer, refer to Introduction to Network Load Balancer.

You can integrate the OCI-native network load balancer with Cisco ISE for load balancing TACACS+ traffic. However, the network load balancer might send traffic to a PSN even if the TACACS+ service is not active on the node, because it 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 both standard and jumbo frames. You can reconfigure the MTU for Cisco ISE as required through the CLI in configuration mode.

# Password recovery and reset on OCI

Use these tasks to reset your Cisco ISE virtual machine password. Select the tasks you need and follow the steps.

## Reset Cisco ISE GUI password through serial console

Follow these steps to reset the Cisco ISE GUI password through the OCI serial console.

**Procedure**

**Step 1** Log in to OCI and choose **Compute** > **Instances**.

**Step 2** From the instance list, select the instance for which you need to change the password.

**Step 3** Choose **Resources** > **Console connection**.

**Step 4** Click **Launch Cloud Shell connection**.

A new screen displays the Oracle Cloud Shell. If the screen is black, press **Enter** to view the login prompt.

**Step 5** Log in to the serial console.

To log in to the serial console, you must use the original password that was set at the installation of the instance. OCI masks this password value. If you do not remember this password, refer to the Password Recovery section.

**Step 6** Use the **application reset-passwd ise iseadmin** command to configure a new Cisco ISE GUI password for the iseadmin account.

# Create a new public key pair in OCI

This task helps you add additional key pairs to a repository. The new public key does not replace the key pair you created during Cisco ISE instance configuration.

### Procedure

**Step 1** Create a new public key in OCI. Refer to Creating a Key Pair.

**Step 2** Log in to the OCI serial console.

**Step 3** Create a new repository to save the public key. Refer to Creating a Repository.

If you already have a repository accessible through the CLI, skip this step.

**Step 4** Import the new public key using this command:

**crypto key import <public key filename> repository <repository name>**

When the import is complete, you can log in to Cisco ISE by using SSH and the new public key.

# Password recovery

There is no mechanism for password recovery for Cisco ISE on OCI. You may need to create new Cisco ISE instances and perform backup and restore of configuration data.

If you edit the OCI stack variables, the Cisco ISE instance is removed and a new instance is created. The system does not retain any settings or configurations.