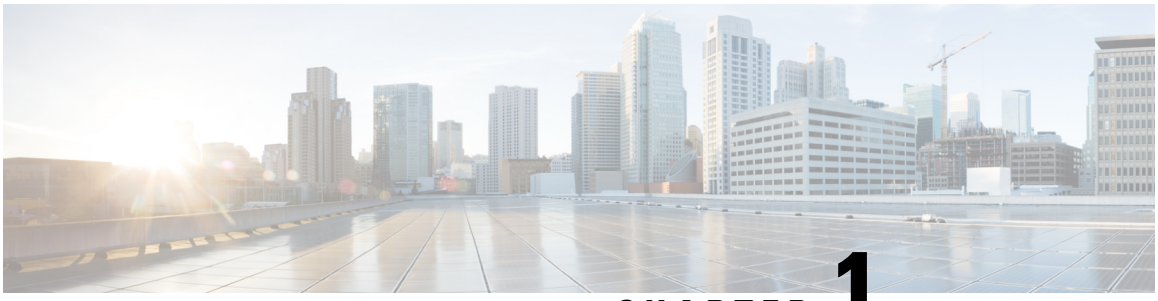
Deploy Cisco Identity Services Engine Natively on Cloud Platforms

First Published: 2022-08-16

Last Modified: 2024-09-17

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

CONTENTS



CHAPTER 1

Cisco ISE on Cloud

Overview of 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 policies in your home network to new remote deployments securely on the following cloud platforms:

- Amazon Web Services: Cisco ISE Release 3.1 and later
- Azure Cloud Services: Cisco ISE Release 3.2 and later
- Oracle Cloud Infrastructure: Cisco ISE Release 3.2 and later

For information on the performance and scalability of Cisco ISE deployments on cloud platforms, see the section "Cisco ISE on Cloud" in the *Performance and Scalability Guide for Cisco Identity Services Engine*.

For more information on Cisco ISE, see Cisco Identity Services Engine End-User Documentation.

For any Cisco ISE that is launched through cloud-native images or instances that are hosted by the supported cloud platforms:

- 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 that is 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 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**.

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

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. See the *Cisco ISE Ordering Guide* for information on Cisco ISE licenses.

Upgrade Guidelines for Hybrid Deployments

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

Upgrade Hybrid Deployments with PAN Installed On-Prem

To upgrade a hybrid deployment in which the Primary Administration Node (PAN) is installed on-prem, and any or some of the secondary nodes are installed on the cloud:

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, see the section "Perform the Upgrade" in the *Cisco Identity Services Engine Upgrade Journey* for your release.

Step 3 Install 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, see the *Cisco Identity Services Engine Installation Guide* for your release.

Step 4 Register these standalone nodes to the upgraded on-prem deployment.

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

Upgrade Hybrid Deployments with PAN Installed on the Cloud

To upgrade a hybrid deployment in which the PAN is installed on the cloud:

Step 1 Take a backup of Cisco ISE configuration settings and operational logs from the existing deployment.

Step 2 Shut down all the nodes in the deployment.

Step 3 Install required number of standalone Cisco ISE nodes on the cloud and on-prem 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, see the *Cisco Identity Services Engine Installation Guide* for your release.

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

Step 5 Join all nodes back into the deployment.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

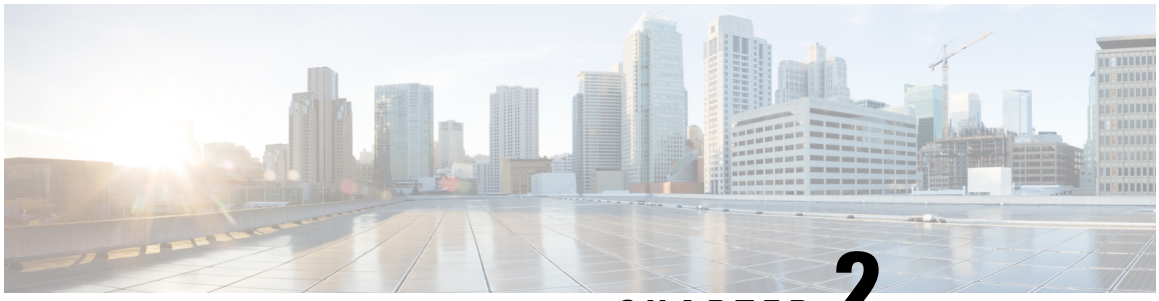
Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Additional References

See Cisco ISE End-User Resources for additional resources that you can use when working with Cisco ISE.



CHAPTER 2

Cisco ISE on Amazon Web Services

Cisco ISE on Amazon Web Services

Extend the Cisco ISE policies in your home network to new remote deployments securely through Amazon Web Services (AWS).

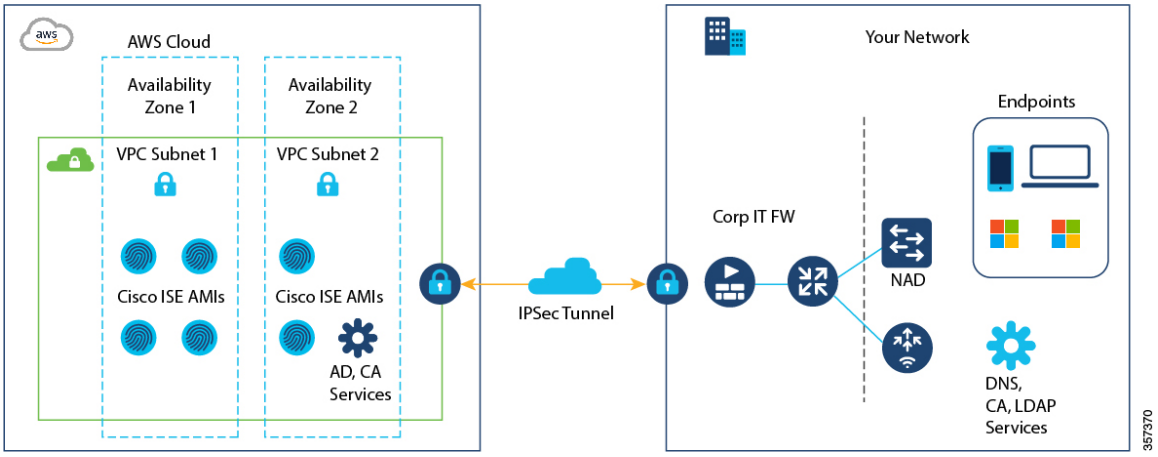
You can configure and launch Cisco ISE in AWS through AWS CloudFormation Templates (CFTs) or Amazon Machine Images (AMIs). We recommend that you use CFTs through one of the ways in the following list. To launch Cisco ISE on AWS, perform one of the following procedures:

- Launch a Cisco ISE CloudFormation Template Through AWS Marketplace, on page 9
- Launch Cisco ISE With CloudFormation Template , on page 12
- Launch a Cisco ISE AMI

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.

The following 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: An Example of a Deployment Connected to AWS Cloud



For information about using CFTs in AWS, see the AWS CloudFormation User Guide.

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

Table 1: Cisco ISE Instances

Cisco ISE Instance Type	CPU Cores	RAM (in GB)
t3.xlarge This instance supports the Cisco ISE evaluation use case and is supported in Cisco ISE Release 3.1 Patch 1 and later releases. 100 concurrent active endpoints are supported.	4	16
m5.2xlarge	8	32
c5.4xlarge	16	32
m5.4xlarge	16	64
c5.9xlarge	36	72
m5.8xlarge	32	128
m5.16xlarge	64	256

Compute-optimized instances such as c5.4xlarge and c5.9xlarge are intended for compute-intensive tasks or applications and are best suited for Policy Service Node (PSN) use.

General purpose instances such as m5.4xlarge, m5.8xlarge, and m5.16xlarge are intended for data processing tasks and database operations and are best suited for use as Policy Administration Node (PAN) or Monitoring and Troubleshooting (MnT) nodes, or both.

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 m5.2xlarge instance must be used as an extra small PSN only.

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

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

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

In addition to the procedures explained above, you can also use the following 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

- You must be familiar with AWS solutions such as Amazon Elastic Compute Cloud (EC2) instances and Amazon Elastic Block Store (EBS) volumes, and concepts such as Regions, Availability Zones, Security Groups, Virtual Private Cloud (VPC), and so on. See the AWS documentation for information on these solutions.

  You must also be familiar with managing AWS service quotas.

- You must configure VPC in AWS.

  See VPC with public and private subnets and AWS Site-to-Site VPN access.

- To create encrypted EBS volumes, your AWS Identity and Access Management (IAM) policy must allow access to Key Management Service (KMS) resources. See Policies and permissions in IAM.

- Create security groups, subnets, and key pairs in AWS before you configure a Cisco ISE instance.

  When you create 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. See Chapter "Cisco ISE Ports Reference" in the *Cisco ISE Installation Guide* for your release.

- 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

The following are the known limitations with using Cisco ISE in AWS:

- You cannot take an Amazon EBS snapshot of a Cisco ISE instance and then create another EBS volume with the snapshot.
- 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.
- 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 first create a network interface object in AWS, power off your Cisco ISE instance, and then attach this network interface object to Cisco ISE. After you install and launch Cisco ISE on AWS, use the Cisco ISE CLI to manually configure the IP address of the network interface object as the secondary NIC.
- 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. For information on upgrading hybrid Cisco ISE deployments, see Upgrade Guidelines for Hybrid Deployments.
- 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 key pair, and this key pair must be stored securely.

  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 DNA Center Release 2.1.2 and earlier.
- 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.
- In the software version Cisco ISE 3.1, when you run the **show inventory** command through a Cisco ISE instance that is launched through AWS, the output for the command does not display the instance type of the Cisco ISE on AWS in the output. This issue does not occur with software versions Cisco ISE 3.1 Patch 1 and later releases.
- You cannot configure an IPv6 server as an NTP server when launching Cisco ISE through AWS.
- 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.
- 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.
- You cannot change the IP address or the default gateway of an instance after it has been created successfully.
- 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.
- The following deployment types are supported, but you must ensure that internode latencies are below 300 milliseconds:
  - Hybrid deployments with some Cisco ISE nodes on premises and some nodes in AWS.

- Interregion deployments through VPC peering connections.

- Amazon EC2 user data scripts are not supported.
- 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.
- When you run the restore operation during a configuration data backup through the Cisco ISE CLI or GUI, do not include the ADE-OS parameter.
- Userdata retrieval only works for Metadata V1 (IMDSv1); it does not work with V2.

Note

- The communication from on-prem devices to the VPC must be secure.
- In Cisco ISE Release 3.1 Patch 3, 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.

Launch a Cisco ISE CloudFormation Template Through AWS Marketplace

This method may launch standalone Cisco ISE instances only. To create a Cisco ISE deployment, see the Chapter "Deployment" in the *Cisco ISE Administrator Guide* for your release.

Note

- You cannot add multiple DNS or NTP servers through the CFT. After you create a Cisco ISE instance, you can add more DNS or NTP servers through the Cisco ISE CLI. However, from Cisco ISE Release 3.4, you can add secondary and tertiary DNS or NTP servers through the CFT.
- You cannot configure IPv6 DNS or NTP servers through the CFT. You can use the Cisco ISE CLI to configure IPv6 servers.

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

Note From Cisco ISE Release 3.4, OpenAPI services are enabled automatically, and hence, there's no need to send OpenAPI-related options while launching an instance.

Before you begin

In AWS, create the security groups and management networks that you want to include in your Cisco ISE CFT configuration.

Step 1 Log in to the Amazon Management Console at https://console.aws.amazon.com/, and search for **AWS Marketplace Subscriptions**.

Step 2 In the **Manage Subscriptions** window that is displayed, click **Discover Products** in the left pane.

Step 3 Enter **Cisco Identity Services Engine (ISE)** in the search bar.

Step 4 Click the product name.

Step 5 In the new window that is displayed, click **Continue to Subscribe**.

Step 6 Click **Continue to Configuration**.

Step 7 In the **Configure this software** area, click **Learn More** and then click **Download CloudFormation Template** to download the Cisco ISE CFT to your local system. You can use this template to automate the configuration of other Cisco ISE instances, as required.

You can also 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**.

Step 10 Choose **Launch CloudFormation** from the **Choose Action** drop-down list.

Step 11 Click **Launch**.

Step 12 In the **Create Stack** window, click the **Template Is Ready** and **Amazon S3 URL** radio buttons.

Step 13 Click **Next**.

Step 14 In the new window, enter a value in the **Stack Name** field.

Step 15 Enter the required details in the following fields in the **Parameters** area:

- **Hostname**: This field only supports alphanumeric characters and hyphen (-). 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 (username admin, for Cisco ISE Release 3.1). Create a PEM key pair in AWS now if you have not configured one already. An example of an SSH command in this scenario is **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.

  Note You can add only one security group in this step. You can add additional security groups in Cisco ISE after installation. The network traffic rules that you want to be available in Cisco ISE at launch must be configured in the security group that you add here.

- **Management Network**: Choose the subnet to be used for the Cisco ISE interface. To enable IPv6 addresses, you must associate an IPv6 CIDR block with your VPC and subnets. Create a subnet in AWS now if you have not configured one already.
- **Management Private IP**: Enter the IPv4 address from the subnet that you chose earlier. If this field is left blank, the AWS DHCP assigns an IP address.

  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.

- **Timezone**: Choose a system time zone from the drop-down list.

- **Instance Type**: Choose a Cisco ISE instance type from the drop-down list.
- **EBS Encryption**: Choose **True** from the drop-down list to enable encryption. The default value for this field is **False**. The default value for this field is **False**. In Cisco ISE Release 3.3 and later releases, the default value of the **EBS Encryption** field is **True**.
- (Optional) **KMS Key**: Enter the **KMS Key** or Amazon Resource Name or alias for data encryption.

  Note This is an optional field applicable for Cisco ISE Release 3.3 and later releases. If the **KMS Key** is provided, it will be used for data encryption. 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. We recommend 600 GB for production use. Configure a volume size lesser than 600 GB only for evaluation purposes. When you terminate the instance, the volume is also deleted.

  Note AWS creates EBS storage volumes in Gibibyte (GiB). 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 (.).
- **Name Server**: Enter the IP address of the name server in the correct syntax.

  Note You can add only one DNS server in this step. You can add additional DNS servers through the Cisco ISE CLI after installation. From Cisco ISE Release 3.4, you can add secondary and tertiary DNS servers as well in this step. If the **Secondary DNS Server** field is left blank, you cannot use the **Tertiary DNS Server** option.

- **NTP Server**: Enter the IP address or hostname of the NTP server in correct syntax, for example, **time.nist.gov**. Your entry is not verified on submission. If you use the wrong syntax, Cisco ISE services might not come up on launch.

  Note 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.

  You can add only one NTP server in this step. You can add additional NTP servers through the Cisco ISE CLI after installation. From Cisco ISE Release 3.4, you can also add secondary and tertiary NTP servers in this step. If the **Secondary NTP Server** field is left blank, you cannot use the **Tertiary NTP Server** option.

- **ERS**: To enable External RESTful Services (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**.
- **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**.
- **Enter Password**: Enter the administrative password that must be used for GUI. The password must be compliant with the Cisco ISE password policy. The password is displayed in plain text in the **User Data** area of the instance settings window in the AWS console. See the "User Password Policy" section in the Chapter "Basic Setup" of the *Cisco ISE Administrator Guide* for your release.
- **Confirm Password**: Re-enter the administrative password.

Step 16 Click **Next** to initiate the instance-creation process.

Launch Cisco ISE With CloudFormation Template

This method may launch standalone Cisco ISE instances only. To create a Cisco ISE deployment, see the Chapter "Deployment" in the *Cisco ISE Administrator Guide* for your release.

Note

- You cannot add multiple DNS or NTP servers through the CFT. After you create a Cisco ISE instance, you can add additional DNS or NTP servers through the Cisco ISE CLI. However, from Cisco ISE Release 3.4, you can add secondary and tertiary DNS or NTP servers through the CFT.
- You cannot configure IPv6 DNS or NTP servers through the CFT. You can only use the Cisco ISE CLI to configure IPv6 servers.

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

Note From Cisco ISE Release 3.4, OpenAPI services are enabled automatically, and hence, there's no need to send OpenAPI-related options while launching an instance.

Before you begin

In AWS, create the security groups and management networks that you want to include in your Cisco ISE CFT configuration.

Step 1 Log in to the Amazon Management Console at https://console.aws.amazon.com/, and search for **AWS Marketplace Subscriptions**.

Step 2 In the **Manage Subscriptions** window that is displayed, click **Discover Products** in the left pane.

Step 3 Enter **Cisco Identity Services Engine (ISE)** in the search bar.

Step 4 Click the product name.

Step 5 In the new window that is displayed, click **Continue to Subscribe**.

Step 6 Click **Continue to Configuration**.

Step 7 In the **Configure this software** area, click **Learn More** and then click **Download CloudFormation Template** to download the Cisco ISE CFT to your local system. You can use this template to automate the configuration of other Cisco ISE instances, as required.

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

Step 8 Using the AWS search bar, search for **CloudFormation**.

Step 9 From the **Create Stack** drop-down list, choose **With new resources (standard)**.

Step 10 In the **Create Stack** window, choose **Template Is Ready** and **Upload a Template File**.

Step 11 Click **Choose File** and upload the CFT file that you downloaded in Step 7.

Step 12 Click **Next**.

Step 13 In the new window, enter a value in the **Stack Name** field.

Step 14 Enter the required details in the following fields in the **Parameters** area:

- **Hostname**: This field only supports alphanumeric characters and hyphen (-). 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 admin. Create a PEM key pair in AWS now if you have not configured one already. An example of an SSH command in this scenario is **ssh -i mykeypair.pem admin@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.

  Note You can add only one security group in this step. You can add additional security groups in Cisco ISE after installation. The network traffic rules that you want available in Cisco ISE at instance launch must be configured in the security group that you add here.

- **Management Network**: Choose the subnet to be used for the Cisco ISE interface. To enable IPv6 addresses, you must associate an IPv6 CIDR block with your VPC and subnets. Create a subnet in AWS now if you have not configured one already.
- **Management Private IP**: Enter the IPv4 address from the subnet that you chose earlier. If this field is left blank, the AWS DHCP assigns an IP address.

  After the Cisco ISE instance is created, copy the private IP address from the **Instance Summary** window. Then, map the IP address and hostname in your DNS server before you create a Cisco ISE deployment.
- **Timezone**: Choose a system time zone from the drop-down list.
- **Instance Type**: Choose a Cisco ISE instance type from the drop-down list.
- **EBS Encryption**: Choose **True** from the drop-down list to enable encryption. The default value for this field is **False**. In Cisco ISE Release 3.3 and later releases, the default value of the **EBS Encryption** field is **True**.
- (Optional) **KMS Key**: Enter the **KMS Key** or Amazon Resource Name or alias for data encryption.

  Note This is an optional field applicable for Cisco ISE Release 3.3 and later releases. If the **KMS Key** is provided, it will be used for data encryption. 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. We recommend 600 GB for production use. Configure a volume size lesser than 600 GB only for evaluation purposes. When you terminate the instance, the volume is also deleted.

  Note AWS creates EBS storage volumes in Gibibyte (GiB). 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 (.).
- **Name Server**: Enter the IP address of the name server in correct syntax.

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

  From Cisco ISE Release 3.4, you can also add secondary and tertiary NTP servers in this step. If the **Secondary DNS Server** field is left blank, you cannot use the **Tertiary DNS Server** option.

- **NTP Server**: Enter the IP address or hostname of the NTP server in correct syntax, for example, **time.nist.gov**. Your entry is not verified on submission. If you use the wrong syntax, Cisco ISE services might not come up on launch.

  Note 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 use the Cisco ISE CLI to configure the correct NTP server.

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

  From Cisco ISE Release 3.4, you can also add secondary and tertiary NTP servers in this step. If the **Secondary NTP Server** field is left blank, you cannot use the **Tertiary NTP Server** option.

- **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**.
- **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**.

  Note The pxGrid Cloud feature is currently not available because there are dependencies on complementary product releases. Do not enable pxGrid Cloud services.

- **Enter Password**: Enter the administrative password that must be used for GUI. The password must be compliant with the Cisco ISE password policy. The password is displayed in plaintext in the **User Data** area of the instance settings window in the AWS console. See the "User Password Policy" section in the Chapter "Basic Setup" of the *Cisco ISE Administrator Guide* for your release.
- **Confirm Password**: Re-enter the administrative password.

Step 15 Click **Next** to initiate the instance-creation process.

Launch a Cisco ISE AMI

Note From Cisco ISE Release 3.4, OpenAPI services are enabled automatically, and hence, there's no need to send OpenAPI-related options while launching an instance.

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.

Step 8 In the **Step 2: Choose an Instance Type** window, click the radio button next to the instance type that you want to use.

Step 9 Click **Next: Configure Instance Details**.

Step 10 In the **Step 3: Configure Instance Details** window, enter the required details in the following fields:

- **Number of Instances**: Enter **1** in this field.
- **Network**: From the drop-down list, choose the VPC in which you want to launch the Cisco ISE instance.
- **Subnet**: From the drop-down list, choose the subnet in which you want to launch the Cisco ISE instance.
- **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.

Step 11 In the **Advanced Details** area, in the **User Data** area, click the **As Text** radio button and enter the key-value pairs in the following format:

hostname=<*hostname of Cisco ISE*>

primarynameserver=<*IPv4 address*>

secondarynameserver=<*IPv4 address of secondary nameserver*> (Applicable to Cisco ISE 3.4 and later releases)

tertiarynameserver=<*IPv4 address of tertiary nameserver*> (Applicable to Cisco ISE 3.4 and later releases)

dnsdomain=<*example.com*>

ntpserver=<*IPv4 address or FQDN of the NTP server*>

secondaryntpserver=<*IPv4 address or FQDN of the secondary NTP server*> (Applicable to Cisco ISE 3.4 and later releases)

tertiaryntpserver=<*IPv4 address or FQDN of the tertiary NTP server*> (Applicable to Cisco ISE 3.4 and later releases)

timezone=<*timezone*>

password=<*password*>

ersapi=<*yes/no*>

openapi=<*yes/no*>

pxGrid=<*yes/no*>

pxgrid_cloud=<*yes/no*>

Important From Cisco ISE Release 3.4,

a. The **ntpserver** field name is changed to **primaryntpserver**. If you use **ntpserver**, Cisco ISE services will not start.

b. OpenAPI is enabled by default. Hence, the **openapi=<yes/no>** field is not required.

c. If you leave the **secondarynameserver** field blank and use only the **tertiarynameserver** field, the Cisco ISE services will not start.

d. If you leave the **secondaryntpserver** field blank and use only the **tertiaryntpserver** field, the Cisco ISE services will not start.

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. If you use the wrong syntax, Cisco ISE services might not come up when you launch the AMI. The following are the guidelines for the configurations that you submit through the **User Data** field:

- hostname: Enter a hostname that contains only alphanumeric characters and hyphen (-). The length of the hostname must not exceed 19 characters and cannot contain underscores (_).
- primarynameserver: Enter the IP address of the primary name server. Only IPv4 addresses are supported. From Cisco ISE Release 3.4, you can configure secondarynameserver and tertiarynameserver during installation by using the **secondarynameserver** and **tertiarynameserver** fields.
- dnsdomain: Enter the FQDN of the DNS domain. The entry can contain ASCII characters, numerals, hyphens (-), and periods (.).
- 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 3.4, you can configure secondary and tertiary NTP servers during installation by using the **secondaryntpserver** and **tertiaryntpserver** fields.
- 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.
- 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 @~*!,+=_-. See the "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.
- openapi: Enter **yes** to enable OpenAPI, or **no** to disallow OpenAPI.
- pxGrid: Enter **yes** to enable pxGrid, or **no** to disallow pxGrid.
- 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.

Step 12 Click **Next: Add Storage**.

Step 13 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, choose **General Purpose SSO (gp2)**.

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

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

Step 14 Click **Next: Add Tags**.

Step 15 (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.

Step 16 Click **Next: Configure Security Group**.

Step 17 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.

Step 18 Click **Review and Launch**.

Step 19 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 20 Click **Launch**.

Step 21 In the **Select an existing key pair or create a new key pair** dialog box choose one of the following 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.

Step 22 Check the check box for the acknowledgment statement and click **Launch Instances**.

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

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 the following 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.

   If you use Linux or MacOS, run the following command from your CLI:

sudo chmod 0400 mykeypair.pem

If you use Windows:

a. Right-click the key file in your local system.

b. Choose **Properties** > **Security** > **Advanced**.

c. In the **Permissions** tab, assign full control to the appropriate user by clicking the corresponding option, and click **Disable Inheritance**.

d. In the **Block Inheritance** dialog box, click **Convert inherited permissions into explicit permissions on this object**.

e. In the **Permissions** tab, in the **Permissions entries** area, choose system and administrator users by clicking the corresponding entries, and then click **Remove.**

f. Click **Apply**, and then click **OK**.

2. Access the Cisco ISE CLI by running the following 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 Post-Installation Tasks" in the Chapter "Installation Verification and Post-Installation Tasks" in the *Cisco ISE Installation Guide* for your release.

Compatibility Information for Cisco ISE on AWS

This section details compatibility information that is unique to Cisco ISE on AWS. For general compatibility details for Cisco ISE, see Cisco Identity Services Engine Network Component Compatibility, Release 3.1.

Cisco DNA Center Integration Support

You can connect your Cisco ISE to Cisco DNA Center Release 2.2.1 and later releases.

Load Balancer Integration Support

You can integrate the AWS-native Network Load Balancer (NLB) with Cisco ISE for load balancing the RADIUS traffic. However, the following caveats are applicable:

- The Change of Authorization (CoA) feature is supported only when you enable client IP preservation in NLB.
- Unequal load balancing might occur because NLB 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 NLB does not support RADIUS-based health checks.

You can integrate the AWS-native Network Load Balancer (NLB) 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 NLB 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.

Retrieve deprecated Amazon Machine Images in AWS

Amazon Machine Images (AMIs) are given an automatic two-year deprecation date from the day they are published in AWS. AWS hides all AMI IDs after their deprecation date, meaning that images cannot be found in the AMI Catalog or EC2 Console but are still available when referenced explicitly by their AMI ID. You can retrieve deprecated AMIs from AWS marketplace or by using the AWS CLI.

For information on how to fetch deprecated AMIs using the AWS CLI, see Describe deprecated AMIs.

Follow these steps to retrieve deprecated AMIs from AWS marketplace.

Step 1 Login to AWS marketplace.

Step 2 Search for **ISE** using the search bar.

Step 3 Select **Cisco Identity Services Engine (ISE)** from the search results.

Step 4 Click **Continue to Subscribe**.

Step 5 Click **Continue to Configuration**.

Step 6 From the **Fulfillment option** drop-down list, select **Amazon Machine Image**.

Step 7 From the **Software version** drop-down list, select the required software version.

Step 8 From the **Region** drop-down list, select the required region.

Step 9 Click **Continue to Launch**.

Step 10 From the **Choose Action** drop-down list, select **Launch through EC2**.

Step 11 Click **Launch**.

A new tab opens showing the required region and the EC2 console which can be used to launch the instance.

Step 12 From the **AMI from catalog** tab in the **Application and OS Images (Amazon Machine Image)** section, copy the deprecated AMI IDs for the chosen region.

Password Recovery and Reset on AWS

The following tasks guide you through the tasks that help your reset your Cisco ISE virtual machine password. Choose the tasks that you need and carry out the steps detailed.

Change Cisco ISE GUI Password via Serial Console

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 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 instance. To view the configured password, carry out the following steps:

a) Click **Actions**.

b) Choose **Instance Settings**.

c) Click **Edit user data**.

The current user data is displayed, including the 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, see 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.

Create New Public Key Pair

Through this task, you 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.

Step 1 Create a new public key in AWS. For instructions on how to create public key pairs, see 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 to, see Creating a private repository.

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

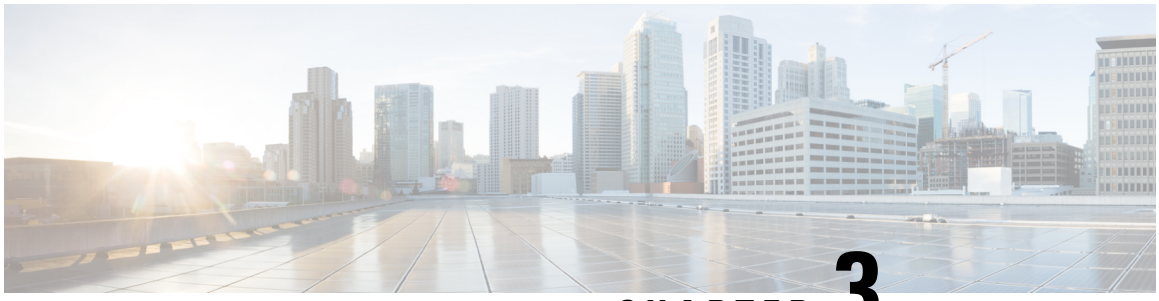
Step 4 To import the new public key, use the command **crypto key import <public key filename> repository <repository name>**

Step 5 When the import is complete, you can log in to Cisco ISE via SSH using the new public key.

Password Recovery

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

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. Some Azure Cloud concepts that you should be familiar with before you begin are:

- Subscriptions and Resource Groups
- Azure Virtual Machines: See Instances, Images, SSH Keys, Tags, VM Resizing.

You can deploy Cisco ISE on Microsoft Azure using an Azure Application or an Azure Virtual Machine. There are no differences in cost or Cisco ISE features when you deploy Cisco ISE using an Azure Application or an Azure Virtual Machine. We recommend using the Azure Application for the following advantages it offers in comparison to the Azure Virtual Machine:

- 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 Virtual Machine 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 Virtual Machine, you can change the OS disk volume to a fixed set of values provided by Azure portal in their drop-down menu. 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 Virtual Machine when:

- You do not use the Azure portal UI to deploy Cisco ISE.

- If you need to use one of the additional settings that are available in the Azure Virtual Machine configuration workflow.

The following task flows guide you through deploying Cisco ISE on Microsoft Azure using an Azure Application or an Azure Virtual Machine.

- Create A Cisco ISE Instance Using Azure Application, on page 28
- Create A Cisco ISE Instance Using Azure Virtual Machine, on page 25

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

Table 2: Azure VM Sizes that are Supported by Cisco ISE

Azure VM Sizes	vCPU	RAM (in GB)
Standard_D4s_v4 (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

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

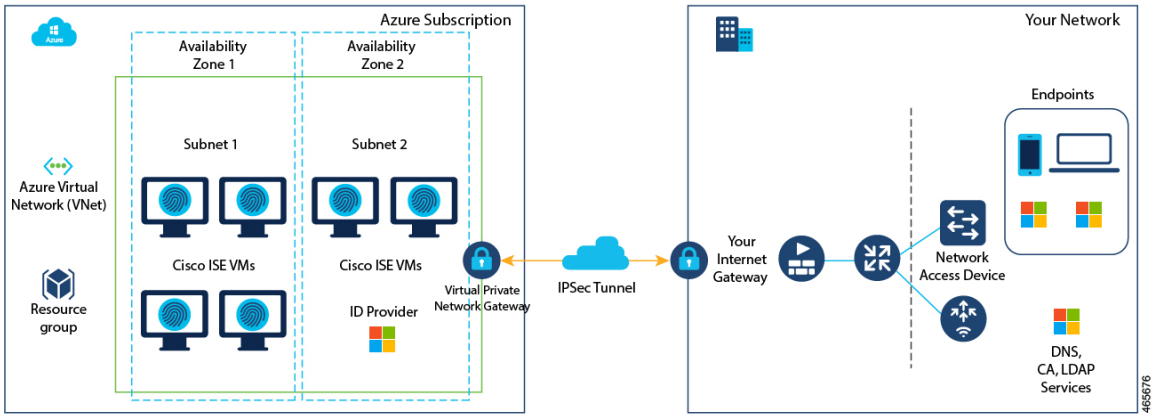
The Dsv4-series are general purpose Azure VM sizes that are best suited for use as PAN or MnT nodes or both and are intended for data processing tasks and database operations.

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, see the *Performance and Scalability Guide for Cisco Identity Services Engine*.

Figure 2: Example of a Deployment Connected to Azure Cloud



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

In addition to the procedures explained above, you can also use the following Cisco developed solution to install and automatically create multi-node Cisco ISE deployments on Azure:

- Cisco Developed Terraform Script

Known Limitations of Cisco ISE in Microsoft Azure Cloud Services

- If you create Create A Cisco ISE Instance Using Azure Application, by default, Microsoft Azure assigns private IP addresses to VMs through DHCP servers. Before you create a Cisco ISE deployment on Microsoft Azure, you must update the forward and reverse DNS entries with the IP addresses assigned by Microsoft Azure.

  Alternatively, after you install Cisco ISE, assign a static IP address to your VM by updating the Network Interface object in Microsoft Azure:

  1. Stop the VM.
  2. In the **Private IP address settings** area of the VM, in the **Assignment** area, click **Static**.
  3. Restart the VM.
  4. In the Cisco ISE serial console, assign the IP address as Gi0.
  5. Restart the Cisco ISE application server.

- 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 first create a network interface object in Azure, power off your Cisco ISE instance, and then attach this network interface object to 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.

- The Cisco ISE upgrade workflow is not available in Cisco ISE on Microsoft Azure. Only fresh installs are supported. However, you can carry out backup and restore of configuration data. For information on upgrading hybrid Cisco ISE deployments, see Upgrade Guidelines for Hybrid Deployments.
- The public cloud supports Layer 3 features only. Cisco ISE nodes on Microsoft Azure do not support Cisco ISE functions that depend on Layer 2 capabilities. For example, working with DHCP SPAN profiler probes and CDP protocol functions through the Cisco ISE CLI are functions that are currently not supported.
- 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 about the Cisco ISE backup and restore processes, see 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 Azure. You can only access the Cisco ISE CLI through a key pair, and this key pair must be stored securely.

  If you are using 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 DNA Center Release 2.1.2 and earlier.
- Azure's VPN gateway in Gen 8 cannot be used as a result of fragmentation. This is an Azure's first party gateway limitation.
- In Azure, a networking virtual network stack drops out-of-order fragments without forwarding them to the end virtual machine host. This design aims to address the network security vulnerability FragmentSmack, as documented in Azure and fragmentation.

  Cisco ISE deployments on Azure typically leverage VPN solutions like Dynamic Multipoint Virtual Private Networks (DMVPN) and Software-Defined Wide Area Networks (SD-WAN), where the IPsec tunnel overheads can cause MTU and fragmentation issues. In such scenarios, Cisco ISE may not receive complete RADIUS packets and an authentication failure occurs without triggering a failure error log.

  Due to this known issue, do one of the following:

  1. Select regions where Azure Cloud has already implemented the fixes: East Asia (eastasia) and West Central US (westcentralus).
  2. Cisco ISE customers should raise an Azure support ticket. Microsoft has agreed to take the following actions:
     a. Pin the subscription to ensure all instances within that subscription are deployed on hardware generation 7.
     b. Enable the "allow out-of-order fragments" option, which allows fragments to pass through to the destination instead of being dropped.

- Cisco ISE deployments on Azure Cloud do not support the Accelerated Networking feature. If you enable this feature at any stage in a Cisco ISE deployment, it might cause operations such as node registration and deregistration to fail.

Create A Cisco ISE Instance Using Azure Virtual Machine

Before you begin

- Create an SSH key pair.
- Create the VN gateways, subnets, and security groups that you require.
- The subnet that you want to use with Cisco ISE must be able to reach the internet. In Microsoft Azure, in the Public Route Table window, configure the next hop of the subnet as the internet.

Note From Cisco ISE Release 3.4, OpenAPI services are enabled automatically, and hence, there's no need to send OpenAPI-related options while launching an instance.

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)**.

Step 4 Click **Virtual Machine**.

Step 5 In the new window that is displayed, click **Create**.

Step 6 In the **Basics** tab:

a) In the **Project details** area, choose the required values from the **Subscription** and **Resource group** drop-down lists.

b) In the **Instance details** area, enter a value in the **Virtual Machine name** field.

c) From the **Image** drop-down list, choose the Cisco ISE image.

d) From the **Size** drop-down list, choose the instance size that you want to install Cisco ISE with. Choose an instance that is supported by Cisco ISE, as listed in the table titled **Azure Cloud instances that are supported by Cisco ISE**, in the section Cisco ISE on Azure Cloud, on page 21.

e) In the **Administrator account** > **Authentication type** area, click the **SSH Public Key** radio button.

f) In the **Username** field, enter **iseadmin**.

Note The only permitted username is **iseadmin**. Use of any other username is not supported.

g) From the **SSH public key source** drop-down list, choose **Use existing key stored in Azure**.

h) From the **Stored keys** drop-down list, choose the key pair that you created as a prerequisite for this task.

i) In the **Inbound port rules** area, click the **Allow selected ports** radio button.

j) From the **Select inbound ports** drop-down list, choose all the protocol ports that you want to allow accessibility to.

k) In the **Licensing** area, from the **Licensing type** drop-down list, choose **Other**.

Step 7 Click **Next: Disks**.

Step 8 In the **Disks** tab, choose 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. By default, a platform-managed key is used. For more information on key creation, see About encryption key management.

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

Step 9 Click **Next: Networking**.

Step 10 In the **Network Interface** area, from the **Virtual network**, **Subnet** and **Configure network security group** drop-down lists, choose 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 only receives offline posture feed updates.

Step 11 Click **Next: Management**.

Step 12 In the **Management** tab, retain the default values for the mandatory fields and click **Next: Advanced**.

Step 13 In the **User data** area, check the **Enable user data** check box.

In the **User data** field, enter the following information:

hostname=<*hostname of Cisco ISE*>

primarynameserver=<*IPv4 address*>

secondarynameserver=<*IPv4 address of secondary nameserver*> (Applicable to Cisco ISE 3.4 and later releases)

tertiarynameserver=<*IPv4 address of tertiary nameserver*> (Applicable to Cisco ISE 3.4 and later releases)

dnsdomain=<*example.com*>

ntpserver=<*IPv4 address or FQDN of the NTP server*>

secondaryntpserver=<*IPv4 address or FQDN of the secondary NTP server*> (Applicable to Cisco ISE 3.4 and later releases)

tertiaryntpserver=<*IPv4 address or FQDN of the tertiary NTP server*> (Applicable to Cisco ISE 3.4 and later releases)

timezone=<*timezone*>

password=<*password*>

ersapi=<*yes/no*>

openapi=<*yes/no*>

pxGrid=<*yes/no*>

pxgrid_cloud=<*yes/no*>

Important From Cisco ISE Release 3.4,

a. The **ntpserver** field name is changed to **primaryntpserver**. If you use **ntpserver**, Cisco ISE services will not start.

b. OpenAPI is enabled by default. Hence, the **openapi=<yes/no>** field is not required.

c. If you leave the **secondarynameserver** field blank and use only the **tertiarynameserver** field, the Cisco ISE services will not start.

d. If you leave the **secondaryntpserver** field blank and use only the **tertiaryntpserver** field, the Cisco ISE services will not start.

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. If you use the wrong syntax, Cisco ISE services might not come up when you launch the image. The following are the guidelines for the configurations that you submit through the user data field:

- hostname: Enter a hostname that contains only alphanumeric characters and hyphens (-). The length of the hostname must not exceed 19 characters and cannot contain underscores (_).
- primarynameserver: Enter the IP address of the primary name server. Only IPv4 addresses are supported.

  You can add only one DNS server in this step. You can add additional DNS servers through the Cisco ISE CLI after installation. However, from Cisco ISE Release 3.4, you can configure secondary and tertiary name servers during installation by using the **secondarynameserver** and **tertiarynameserver** fields.
- dnsdomain: Enter the FQDN of the DNS domain. The entry can contain ASCII characters, numerals, hyphens (-), and periods (.).
- ntpserver: Enter the IPv4 address or FQDN of the NTP server that must be used for synchronization, for example, time.nist.gov.

  You can add only one NTP server in this step. You can add additional NTP servers through the Cisco ISE CLI after installation. However, from Cisco ISE Release 3.4, you can configure secondary and tertiary NTP servers during installation by using the **secondaryntpserver** and **tertiaryntpserver** fields.
- 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.
- 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 be the same as the username or its reverse (iseadmin or nimdaesi), cisco, or ocsic. The allowed special characters are @~*!,+=_-. See the "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.
- openapi: Enter **yes** to enable OpenAPI, or **no** to disallow OpenAPI.
- pxGrid: Enter **yes** to enable pxGrid, or **no** to disallow pxGrid.
- 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 on launch.

Step 14 Click **Next: Tags**.

Step 15 To create name-value pairs that allow you to categorize resources, and consolidate multiple resources and resource groups, enter values in the **Name** and **Value** fields.

Step 16 Click **Next: Review + Create**.

Step 17 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).

What to do next

Note 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.

Because of a Microsoft Azure default setting, the Cisco ISE VM you have created 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 the Cisco ISE VM creation is complete, log in to the Cisco ISE administration portal to verify that Cisco ISE is set up. Then, in the Microsoft Azure portal, carry out the following steps in the **Virtual Machines** window to edit the disk size:

1. Stop the Cisco ISE instance.
2. Click **Disk** in the left pane, and click the disk that you are using with Cisco ISE.
3. Click **Size + performance** in the left pane.
4. In the **Custom disk size** field, enter the disk size you want, in GiB.

Create A Cisco ISE Instance Using Azure Application

Before you begin

Create the Azure resources that you need, such as Resource Groups, Virtual Networks, Subnets, SSH keys, and so on.

Note From Cisco ISE Release 3.4, OpenAPI services are enabled automatically. Therefore, there's no need to send OpenAPI-related options while launching an instance.

Step 1 Go to https://portal.azure.com and log in to the Azure portal.

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)**.

Step 4 Click **Azure Application**.

Step 5 In the new window that is displayed, click **Create**.
A five-step workflow is displayed.

Step 6 In the **Basics** tab:

a) From the **Resource Group** drop-down list, choose the option that you want to associate with Cisco ISE.
b) From the **Region** drop-down list, choose the region in which the Resource Group is placed.
c) In the **Hostname** field, enter the hostname.
d) From the **Time zone** drop-down list, choose the time zone.
e) From the **VM Size** drop-down list, choose the Azure VM size that you want to use for Cisco ISE.
f) From the **Disk Encryption Key** drop-down list, choose your key for disk encryption.

Note We recommend that you use a customer-managed key for disk encryption in the **Disk Encryption Key** field. By default, a platform-management key is used. This field is available from Cisco ISE Release 3.3. For more information, see About encryption key management.

g) From the **Disk Storage Type** drop-down list, choose an option.
h) In the **Volume Size** field, enter, in GB, the volume that you want to assign to the Cisco ISE instance. 600 GB is the default value.

Step 7 Click **Next**.

Step 8 In the **Network Settings** tab:

a) From the **Virtual Network** drop-down list, choose an option from the list of virtual networks available in the selected resource group.
b) From the **Subnet** drop-down list, choose an option from the list of subnets associated with the selected virtual group.
c) (Optional) From the **Network Security Group** drop-down list, choose an option from the list of security groups in the selected Resource Group.
d) From the **SSH public key source** drop-down list, choose whether you want to create a new key pair or use an existing key pair by clicking the corresponding option.
e) If you chose **the Use existing key stored in Azure** option in the previous step, from the **Stored Keys** drop-down list, choose the key you want to use.
f) To assign a static IP address to Cisco ISE, enter an IP address in the **Private IP address** field. Ensure that this IP address is not being used by any other resource in the selected subnet.
g) In the **Public IP Address** drop-down list, choose the address that you want to use with Cisco ISE. If this field is left blank, a public IP address is assigned to the instance by the Azure DHCP server.
h) In the **DNS Name** field, enter the DNS domain name.

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

i) In the **Name Server** field, enter the IP address of the name server.

   Note From Cisco ISE Release 3.4, the **Name Server** field name is changed to **Primary Name Server**.

   In the **Secondary Name Server** field, enter the IP address of the secondary name server. This field is available from Cisco ISE Release 3.4.

   In the **Tertiary Name Server** field, enter the IP address of the tertiary name server. This field is available from Cisco ISE Release 3.4. To use this field and to launch the application successfully, you must not leave the **Secondary Name Server** field blank.

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

j) In the **NTP Server** field, enter the IP address or hostname of the NTP server. Your entry is not validated upon input.

Note From Cisco ISE Release 3.4, the **NTP Server** field name is changed to **Primary NTP Server**.

In the **Secondary NTP Server** field, enter the IP address or hostname of the secondary NTP server. Your entry is not validated upon input. This field is available from Cisco ISE Release 3.4.

In the **Tertiary NTP Server** field, enter the IP address or hostname of the tertiary NTP server. Your entry is not validated upon input. This field is available from Cisco ISE Release 3.4. To use this field and to launch the application successfully, you must not leave the **Secondary NTP Server** field blank.

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

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

Step 9 Click **Next**.

Step 10 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**.

Note From Cisco ISE Release 3.4, OpenAPIs are enabled by default. Hence, this field is not available.

c) From the **pxGrid** drop-down list, choose **Yes** or **No**.

d) From the **pxGrid Cloud** drop-down list, choose **Yes** or **No**.

Step 11 Click **Next**.

Step 12 In the **User Details** tab:

a) In the **Enter Password for iseadmin** and **Confirm Password** fields, enter a password for Cisco ISE. The password must comply with the Cisco ISE password policy and contain a maximum of 25 characters.

Step 13 Click **Next**.

Step 14 In the **Review + create** tab, review the details of the instance.

Step 15 Click **Create**.

The **Overview** window displays the progress in the instance creation process.

Step 16 Use the search bar and navigate to the **Virtual Machines** window. The Cisco ISE instance that you created is listed in the window, with the **Status** as **Creating**. It takes about 30 minutes to create a Cisco ISE instance.

Postinstallation Tasks

For information about the postinstallation tasks that you must carry out after successfully creating a Cisco ISE instance, see the Chapter "Installation Verification and Post-Installation Tasks" in the *Cisco ISE Installation Guide* for your Cisco ISE release.

Compatibility Information for Cisco ISE on Azure Cloud

This section details compatibility information that is unique to Cisco ISE on Azure Cloud. For general compatibility details for Cisco ISE, see 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, the following caveats are applicable:

- The Change of Authorization (CoA) feature is supported only when you enable client IP preservation when you configure Session Persistence property in the load balancing rule in the Azure portal.

- Unequal load balancing might occur because the Azure Load Balancer only supports source IP affinity and does not support 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 as the Azure Load Balancer does not support RADIUS-based health checks.

For more information on the Azure Load Balancer, see 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

The following tasks guide you through the tasks that help your reset or recover your Cisco ISE virtual machine password. Choose the tasks that you need and carry out the steps detailed.

Note 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

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, from the **Help** section, click **Serial console**.

Step 4 If you view an error message here, you may have to enable boot diagnostics by carrying out the following 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 5 From the left-side menu, from the **Help** section, click **Serial console**.

Step 6 The Azure Cloud Shell is displayed in a new window.

Step 7 If the screen is black, press Enter to view the login prompt.

Step 8 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. If you do not remember this password, see the Password Recovery section.

Step 9 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

Through this task, you 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.

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

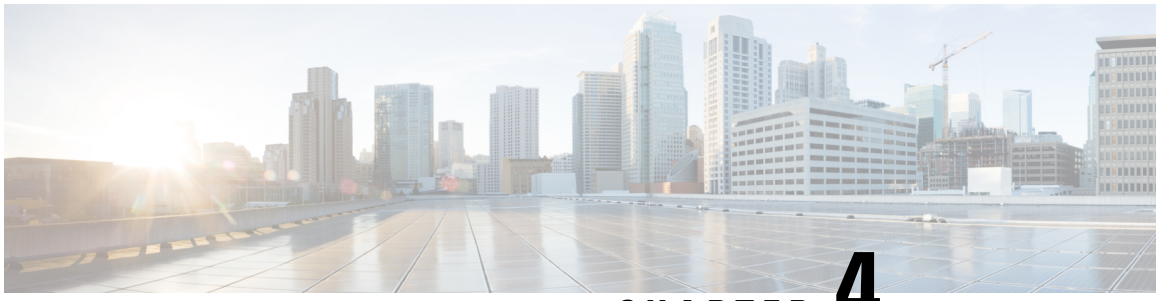
Step 2 Log in to the Azure Cloud serial console as detailed in the preceding task.

Step 3 To create a new repository to save the public key to, see 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 the command **crypto key import <public key filename> repository <repository name>**

Step 5 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 (OCI)

Cisco ISE on Oracle Cloud Infrastructure (OCI)

Cisco ISE is available on Oracle Cloud Infrastructure (OCI). To configure and install Cisco ISE on OCI, you must be familiar with some OCI features and solutions. Some concepts that you must be familiar with before you begin include compartments, availability domains, images and shapes, and boot volumes. The unit of OCI's compute resources is Oracle CPUs (OCPUs). One OCPU is equal to two vCPUs.

See Oracle Cloud Infrastructure Documentation.

Cisco ISE is available on 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.

- Create a Cisco ISE Instance in OCI Using a Terraform Stack File, on page 38
- Create a Cisco ISE Instance in OCI, on page 35

Table 3: OCI Instances that are Supported by Cisco ISE

OCI Instance	OCPU	OCI Instance Memory (in GB)
Standard3.Flex (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 and are best suited for use as PSNs for compute-intensive tasks and applications.

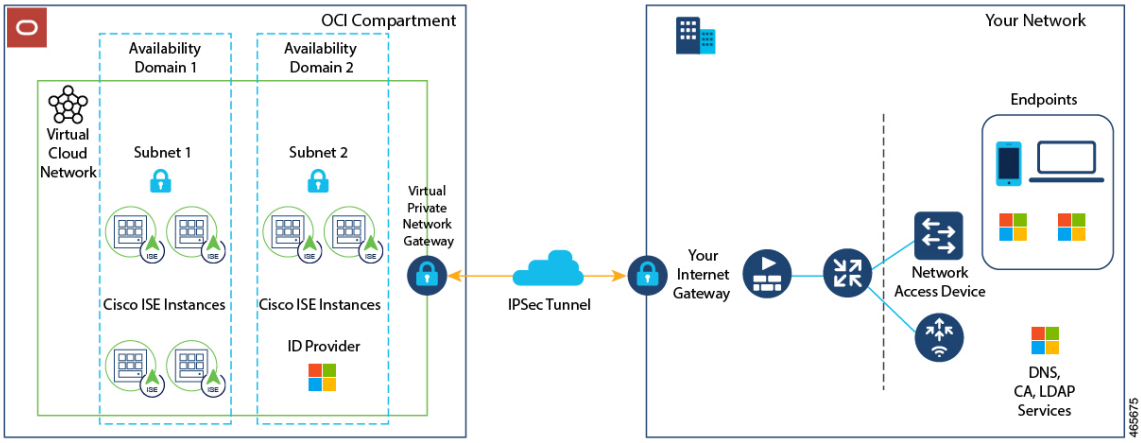
The Standard3.Flex shapes are general purpose shapes that are best suited for use as PAN or MnT nodes or both and are intended for data processing tasks and database operations.

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

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

Figure 3: Example of a Deployment Connected to Oracle Cloud



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

Known Limitations of Using Cisco ISE on OCI

- The Cisco ISE upgrade workflow is not available in Cisco ISE on OCI. Only fresh installs are supported. However, you can carry out backup and restoration of configuration data. For information on upgrading hybrid Cisco ISE deployments, see Upgrade Guidelines for Hybrid Deployments.
- The public cloud supports Layer 3 features only. Cisco ISE nodes on OCI do not support Cisco ISE functions that depend on Layer 2 capabilities. For example, working with DHCP SPAN profiler probes and CDP protocol functions through the Cisco ISE CLI are functions that are currently 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 the following 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, see 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 are using a Private Key (or PEM) file and you lose the 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 DNA Center Release 2.1.2 and earlier.

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 you start with Step 3 of the following task.

  Create the virtual cloud networks and subnets in the same compartment in which you will create your Cisco ISE instance.
- When you create a virtual cloud network for use with Cisco ISE, we recommend that you choose the **Create VCN with Internet Connectivity** VCN type.

Note From Cisco ISE Release 3.4, OpenAPI services are enabled automatically, and hence, there's no need to send OpenAPI-related options while launching an instance.

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...** search field, enter **Cisco Identity Services Engine (ISE)**.

Step 4 Click the Cisco ISE option that is of **Image** type.

Step 5 In the new window that is displayed, click **Launch Instance**.

Step 6 In the **List Scope** area of the left pane, from the **Compartment** drop-down list, choose a compartment.

Step 7 Click **Create Instance** in the right pane.

Step 8 In the **Create Compute Instance** window, in the **Name** field, enter a name for your Cisco ISE instance.

Step 9 From the **Create in compartment** drop-down list, choose the compartment in which the Cisco ISE instance must be created. You must choose the compartment in which you have created other resources such as virtual cloud networks and subnets for Cisco ISE use.

Step 10 In the **Placement** area, click an availability domain. The domain determines the compute shapes that are available to you.

Step 11 In the **Image and Shape** area:

a) Click **Change Image**.
b) From the **Image Source** drop-down list, choose **Custom Image**.
c) Check the check box next to the required custom image name.
d) Click **Select Image**.
e) From the **Image and Shape** area, click **Change Shape**.
f) From the **Shape Series** area, click **Intel**. A list of available shapes is displayed.
g) Check the check box next to the required shape name. Click **Select Shape**.

Step 12 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 the **Select existing subnet** radio button.
d) Choose a subnet from the drop-down list. The subnets displayed are those that have been created in the same compartment.

Step 13 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 14 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 We recommend that you 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, see Key Management.

Step 15 Click **Show advanced options**.

Step 16 In the **Management** tab, click the **Paste cloud-init script** radio button.

Step 17 In the **Cloud-init script** text box, enter the required user data:

In the **User data** field, enter the following information:

hostname=<*hostname of Cisco ISE*>

primarynameserver=<*IPv4 address*>

secondarynameserver=<*IPv4 address of secondary nameserver*> (Applicable for Cisco ISE 3.4 and later releases)

tertiarynameserver=<*IPv4 address of tertiary nameserver*> (Applicable for Cisco ISE 3.4 and later releases)

dnsdomain=<*example.com*>

ntpserver=<*IPv4 address or FQDN of the NTP server*>

secondaryntpserver=<*IPv4 address or FQDN of the secondary NTP server*> (Applicable for Cisco ISE 3.4 and later releases)

tertiaryntpserver=<*IPv4 address or FQDN of the tertiary NTP server*> (Applicable for Cisco ISE 3.4 and later releases)

timezone=<*timezone*>

password=<*password*>

ersapi=<*yes/no*>

openapi=<*yes/no*>

pxGrid=<*yes/no*>

pxgrid_cloud=<*yes/no*>

Important From Cisco ISE Release 3.4,

a. The **ntpserver** field name is changed to **primaryntpserver**. If you use **ntpserver**, Cisco ISE services will not start.

b. OpenAPI is enabled by default. Hence, the **openapi=<yes/no>** field is not required.

c. If you leave the **secondarynameserver** field blank and use only the **tertiarynameserver** field, the Cisco ISE services will not start.

d. If you leave the **secondaryntpserver** field blank and use only the **tertiaryntpserver** field, the Cisco ISE services will not start.

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. If you use the wrong syntax, Cisco ISE services might not come up when you launch the image. The following are the guidelines for the configurations that you submit through the **User data** field:

- hostname: Enter a hostname that contains only alphanumeric characters and hyphens (-). The length of the hostname must not exceed 19 characters and cannot contain underscores (_).
- primarynameserver: Enter the IP address of the primary name server. Only IPv4 addresses are supported. From Cisco ISE Release 3.4, you can configure secondary and tertiary name servers during installation by using the **secondarynameserver** and **tertiarynameserver** fields.
- dnsdomain: Enter the FQDN of the DNS domain. The entry can contain ASCII characters, numerals, hyphens (-), and periods (.).
- 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 3.4, you can configure secondary and tertiary NTP servers during installation by using **secondaryntpserver** and **tertiaryntpserver** fields.
- timezone: Enter a timezone, for example, Etc/UTC. We recommend that you set all Cisco ISE nodes to the Coordinated Universal Time (UTC) timezone, especially if your Cisco ISE nodes are installed in a distributed deployment. This ensures that the timestamps of the reports and logs from the various nodes in your deployment are always synchronized.
- 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 @~*!,+=_-. If you use special characters in the password, they must be escaped by a backslash (\). See the "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.
- openapi: Enter **yes** to enable OpenAPI, or **no** to disallow OpenAPI.

- pxGrid: Enter **yes** to enable pxGrid, or **no** to disallow pxGrid.
- 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 on launch.

Step 18 Click **Create**. It takes about 30 minutes for the instance to be created and available for use.

To view the Cisco ISE instance, go to the **Instances** window (you can use the search field to find the window). The Cisco ISE instance is listed in this window.

Create a Cisco ISE Instance in OCI Using a Terraform Stack File

Before you begin

OCI Terraform is leveraged to create Cisco ISE instances. For information about Terraform in OCI, see https://docs.oracle.com/en-us/iaas/Content/API/SDKDocs/terraform.htm

In OCI, create the resources that you need to create a Cisco ISE instance, such as like SSH keys, Virtual Cloud Network (VCN), subnets, network security groups, and so on.

Note From Cisco ISE Release 3.4, OpenAPI services are enabled automatically, and hence, there's no need to send OpenAPI-related options while launching an instance.

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...** search 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 the **My Configuration** radio button.

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

Step 7 Click **Next**.

Step 8 In the **Configure Variables** window:

a) In the **Hostname** field, enter the hostname.

b) From the **Shape** drop-down list, choose the OCI shape you want to use. If you choose **VM.Optimized3.Flex**, from the **Flex OCPUs** drop-down list, choose the required value. The **Flex Memory in GB** field automatically displays the corresponding value. For the other shapes, the values are preconfigured and these fields are not displayed in the stack form.

c) The **Boot Volume Size** field automatically displays the required value based on the shape chosen in the previous step.

1. In the **Vault** field, choose the vault for boot volume encryption keys.
2. In the **Volume Encryption Key** field, choose the key to encrypt the boot volume.

Note We recommend you to use Customer Managed Key for encryption under **Volume Encryption Key** and **Vault** fields. By default, **Oracle Managed Key** is used. These fields are available from Cisco ISE Release 3.3. For more information on key creation, see to Key Management.

d) In the **SSH Key** area, you can either upload an SSH key file or paste an SSH key code by clicking the corresponding radio button.
e) From the **Time zone** drop-down list, choose the time zone.
f) From the **Availability Domain** drop-down list, choose an option from the list of domains in your region.
g) From the **Virtual Cloud Network** drop-down list, choose an option from the list of VCNs in the compartment that you chose in Step 6b.
h) From the **Subnet** drop-down list, choose an option from the list of subnets associated with the VCN you chose in step 8g.
i) (Optional) From the **Network Security Group** drop-down list, choose an option from the list of security groups associated with the component you chose earlier.
j) The **Assign Public IP Address** check box is checked by default. You can uncheck the check box if you want to assign only private IP addresses to your Cisco ISE instance.
k) In the **Private IP Address** field, enter an IP address that complies with the IP address range defined in the selected subnet. If this field is left blank, the OCI DHCP server assigns an IP address to Cisco ISE.
l) In the **DNS Name** field, enter the domain name.
m) In the **Name Server** field, enter the IP address of the name server.

Note From Cisco ISE Release 3.4, the **Name Server** field name is changed to **Primary Name Server**.

In the **Secondary Name Server** field, enter the IP address of the secondary name server. This field is available from Cisco ISE Release 3.4.

In the **Tertiary Name Server** field, enter the IP address of the tertiary name server. This field is available from Cisco ISE Release 3.4. If the **Secondary Name Server** field is left blank, you cannot use the **Tertiary Name Server** option.

Note In the event that any of the entered IP addresses are unavailable or not reachable, the Cisco ISE services might not be launched.

n) In the **NTP Server** field, enter the IP address or hostname of the NTP server. Your entry is not validated on input. From Cisco ISE Release 3.4, this field name is changed to **Primary NTP Server**.

In the **Secondary NTP Server** field, enter the IP address or hostname of the secondary NTP server. Your entry is not validated on input. This field is available from Cisco ISE Release 3.4.

In the **Tertiary NTP Server** field, enter the IP address or hostname of the tertiary NTP server. Your entry is not validated on input. This field is available from Cisco ISE Release 3.4. If the **Secondary NTP Server** field is left blank, you cannot use the **Tertiary NTP Server** option.

Note If the entered IP addresses are unavailable or not reachable, the Cisco ISE services might not be launched.

o) From the **ERS** drop-down list, choose **Yes** or **No**.
p) From the **Open API** drop-down list, choose **Yes** or **No**.
q) From the **pxGrid** drop-down list, choose **Yes** or **No**.
r) From the **pxGrid Cloud** drop-down list, choose **Yes** or **No**.

s) In the **Password** and **Re-enter the Password** fields, enter a password for Cisco ISE. The password must comply with the Cisco ISE password policy and contain a maximum of 25 characters.

Step 9 Click **Next**.

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

Step 10 Review the information and click **Previous** to make changes, if any.

Step 11 In the **Run Apply on the created stack?** area, check the **Run Apply** check box to execute stack building 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 12 Click **Create**.

Step 13 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.

Step 14 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 successfully creating a Cisco ISE instance, see the Chapter "Installation Verification and Post-Installation Tasks" in the *Cisco ISE Installation Guide* for your Cisco ISE release.

Compatibility Information for Cisco ISE on OCI

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

Load Balancer Integration Support

You can integrate OCI-native Network Load Balancer (NLB) with Cisco ISE for load balancing RADIUS traffic. However, the following caveats are applicable:

- The Change of Authorization (CoA) feature is supported only when you enable client IP preservation in the Source/Destination Header (IP,Port) Preservation section when you create the network load balancer.
- Unequal load balancing might occur because NLB only supports source IP affinity and does not support 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 as NLB does not support RADIUS-based health checks.

For more information on the OCI-native Network Load Balancer, see Introduction to Network Load Balancer.

You can integrate OCI-native Network Load Balancer (NLB) 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 NLB 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 OCI

The following tasks guide you through the tasks that help your reset your Cisco ISE virtual machine password. Choose the tasks that you need and carry out the steps detailed.

Reset Cisco ISE GUI Password Through Serial Console

Step 1 Log in to OCI and go to the **Compute** > **Instances** window.

Step 2 From the list of instances, click the instance for which you need to change the password.

Step 3 From the **Resources** menu on the left pane, click **Console connection**.

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

Step 5 A new screen displays the Oracle Cloud Shell.

Step 6 If the screen is black, press Enter to view the login prompt.

Step 7 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 stores this value as a masked password. If you do not remember this password, see the Password Recovery section.

Step 8 Use the **application reset-passwd ise iseadmin** command to configure a new Cisco ISE GUI password for the iseadmin account.

Create New Public Key Pair

Through this task, you 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.

Step 1 Create a new public key in OCI. See Creating a Key Pair.

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

Step 3 To create a new repository to save the public key to, see Creating a Repository.

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

Step 5 When the import is complete, you can log in to Cisco ISE via SSH using 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.

Editing the variables for an OCI stack results in the Cisco ISE instance being destroyed and recreated as a new Cisco ISE instance, without saving any settings or configurations.