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 6
- Create a Cisco ISE Instance in OCI, on page 3

Table 1: 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.

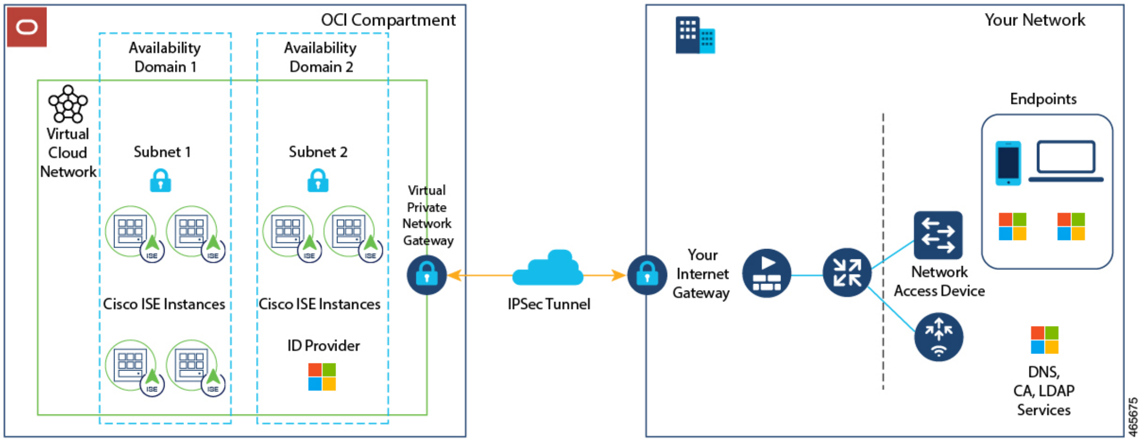
The Standard3.Flex shapes are general purpose shapes that are best suited for use as PAN or MnT nodes or both and are intended for data processing tasks and database operations.

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 1: 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.