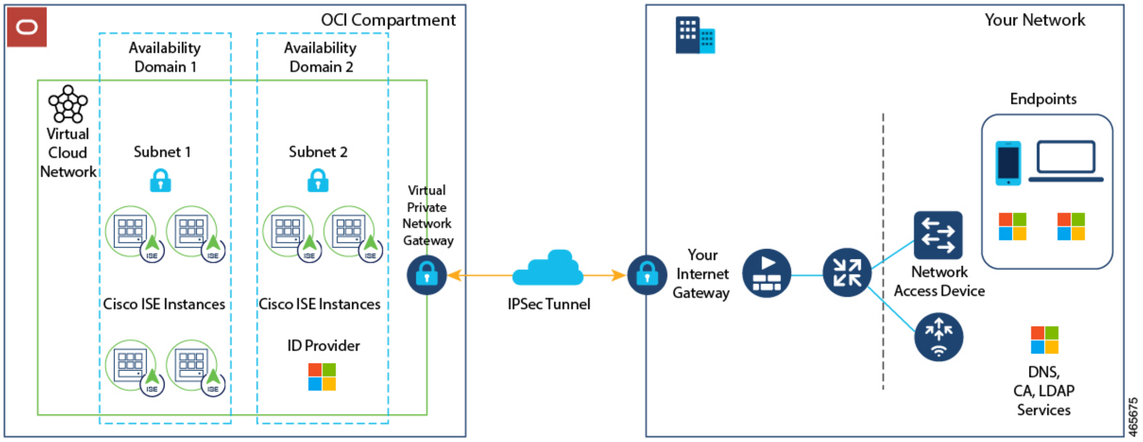
Cisco ISE on Oracle Cloud Infrastructure

Cisco ISE on Oracle Cloud Infrastructure

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

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



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

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

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

OCI instances supported by Cisco ISE

You can use these OCI instances with Cisco ISE.

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

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

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

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

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

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

Known limitations of using Cisco ISE on OCI

- The Cisco ISE upgrade workflow is not supported for OCI. Only fresh installs are supported. However, you can back up and restore configuration data. For information on upgrading hybrid Cisco ISE deployments, see Upgrade Guidelines for Hybrid Deployments.
- The public cloud supports only Layer 3 features. Cisco ISE nodes on OCI do not support functions that depend on Layer 2 capabilities. For example, DHCP SPAN profiler probes and CDP protocol functions that are accessed through the Cisco ISE CLI are not supported.
- To enable IPv6 addresses in Cisco ISE, configure an IPv6 address in the OCI portal for Cisco ISE and restart interface Gigabit Ethernet 0. Log in as an administrator in the Cisco ISE Serial Console and run these commands:

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

- When you carry out the restore and backup function of configuration data, after the backup operation is complete, first restart Cisco ISE through the CLI. Then, initiate the restore operation from the Cisco ISE GUI. For more information on the Cisco ISE backup and restore processes, 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 lose your Private Key (or PEM) file, you cannot access the Cisco ISE CLI.

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

Create a Cisco ISE instance in OCI

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

Before you begin

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

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

Note From Cisco ISE Release 3.4, OpenAPI services are enabled automatically. You do not need to include OpenAPI-related options when launching an instance.

Procedure

Step 1 Navigate to the Cisco ISE option on the OCI console, on page 4.

Step 2 Configure instance details, on page 4.

Step 3 Configure advanced options for a Cisco ISE instance, on page 5.

Navigate to the Cisco ISE option on the OCI console

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

Procedure

Step 1 Log in to your OCI account.

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

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

Configure instance details

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

Procedure

Step 1 Click the Cisco ISE option that is of **Image** type.

Step 2 Click **Launch Instance**.

Step 3 In the **List Scope** area, from the **Compartment** drop-down list, choose a compartment.

Step 4 Click **Create Instance**.

Step 5 In the **Create Compute Instance** window, enter a name for your Cisco ISE instance.

Step 6 From the **Create in compartment** drop-down list, choose the compartment for the Cisco ISE instance.

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

Step 7 In the **Placement** area, click an availability domain.

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

Step 8 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 and click **Select Shape**.

Step 9 In the **Networking** area:

a) In the **Primary Network** area, click the **Select existing virtual cloud network** radio button.
b) Choose a virtual cloud network from the drop-down list.
c) In the **Subnet** area, click **Select existing subnet**.

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

The subnets that are created in the same compartment are displayed.

Step 10 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 11 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.

Configure advanced options for a Cisco ISE instance

Follow these steps to configure the advanced options.

Procedure

Step 1 Click **Show advanced options**.

Step 2 In the **Management** tab, click **Paste cloud-init script**.

Step 3 In the **Cloud-init script** text box, enter the required user data.

Step 4 In the **User data** field, enter these details:

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. If you use incorrect syntax, Cisco ISE services might not start when you launch the image.

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

- 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. Set all Cisco ISE nodes to the Coordinated Universal Time (UTC) timezone, especially for distributed deployments. 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, 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 when the instance launches.

Step 5 Click **Create**.

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

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

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

Before you begin

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

Note From Cisco ISE release 3.4, OpenAPI services are enabled automatically. Hence, you do not need to include OpenAPI-related options when you launch an instance.

Procedure

Step 1 Create a Cisco ISE stack in OCI, on page 7.

Step 2 Configure variables for Cisco ISE instance, on page 8.

Step 3 Review configurations and create a Cisco ISE instance in OCI, on page 9.

Create a Cisco ISE stack in OCI

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

Procedure

Step 1 Log in to your OCI account.

Step 2 Use the search field to search for **Marketplace**.

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

Step 4 Click **Cisco Identity Services Engine (ISE) Stack**.

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

Step 6 In the **Stack Information** window:

a) Click **My Configuration**.

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

Configure variables for Cisco ISE instance

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

Procedure

Step 1 In the **Configure Variables** 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 select **VM.Optimized3.Flex**, choose the required value from the **Flex OCPUs** drop-down list. The **Flex Memory in GB** field displays the corresponding value. For the other shapes, these values are preconfigured and 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 Key Management.

d) In the **SSH Key** area, upload an SSH key file or paste an SSH key code.

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 selected earlier.

h) From the **Subnet** drop-down list, choose an option from the list of subnets associated with the selected VCN.

i) (Optional) From the **Network Security Group** drop-down list, select the security group associated with the component you selected earlier.

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.

j) In the **Private IP Address** field, enter an IP address within the range defined for the selected subnet.

If this field is left blank, the OCI DHCP server assigns an IP address to Cisco ISE.

k) In the **DNS Name** field, enter the domain name.

l) 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
If any entered IP addresses are unavailable or not reachable, Cisco ISE services might not start.

m) 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. 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. 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 any entered IP addresses are unavailable or not reachable, Cisco ISE services might not start.

n) From the **ERS** drop-down list, choose **Yes** or **No**.
o) From the **Open API** drop-down list, choose **Yes** or **No**.
p) From the **pxGrid** drop-down list, choose **Yes** or **No**.
q) From the **pxGrid Cloud** drop-down list, choose **Yes** or **No**.
r) 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 2 Click **Next**.

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

Review configurations and create a Cisco ISE instance in OCI

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

Procedure

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

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

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

Step 3 Click **Create**.

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

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

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

Postinstallation tasks

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

Compatibility information for Cisco ISE on OCI

This section provides compatibility information that is unique to Cisco ISE on OCI. For general compatibility details for Cisco ISE, 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 with Cisco ISE for load balancing RADIUS traffic. However, these caveats are applicable:

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

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

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

NIC jumbo frame support

Cisco ISE supports jumbo frames. The Maximum Transmission Unit (MTU) for Cisco ISE is 9,001 bytes, while the MTU of Network Access Devices is typically 1,500 bytes. Cisco ISE supports both standard and jumbo frames. You can reconfigure the MTU for Cisco ISE as required through the CLI in configuration mode.

Password recovery and reset on OCI

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

Reset Cisco ISE GUI password through serial console

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

Procedure

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

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

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

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

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

Step 5 Log in to the serial console.

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

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

Create a new public key pair in OCI

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

Procedure

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

Step 2 Log in to the OCI serial console.

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

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

Step 4 Import the new public key using this command:

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

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

Password recovery

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

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