

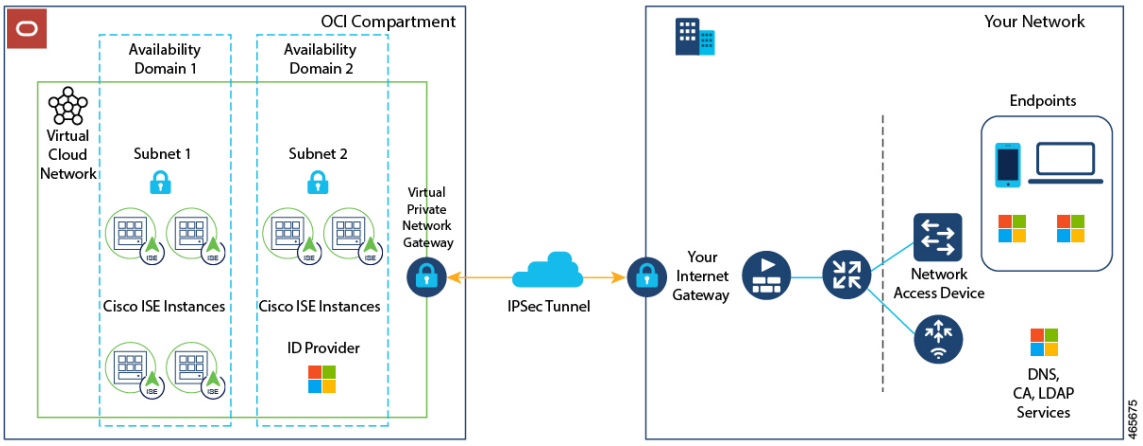
Cisco ISE on Oracle Cloud Infrastructure

- Cisco ISE on Oracle Cloud Infrastructure, on page 1
- OCI instances supported by Cisco ISE, on page 2
- Known limitations of using Cisco ISE on OCI, on page 2
- Create a Cisco ISE instance in OCI, on page 3
- Create a Cisco ISE instance in OCI using a Terraform Stack file, on page 11
- Postinstallation tasks, on page 12
- Compatibility information for Cisco ISE on OCI, on page 13
- Password recovery and reset on OCI, on page 13

Cisco ISE on Oracle Cloud Infrastructure

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

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



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

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

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

OCI instances supported by Cisco ISE

You can use these OCI instances with Cisco ISE.

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

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

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

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

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

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

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

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

Known limitations of using Cisco ISE on OCI

- The Cisco ISE upgrade workflow is not supported for OCI. Only fresh installs are supported. However, you can back up and restore configuration data. For information on upgrading hybrid Cisco ISE deployments, refer to "Upgrade Guidelines for Hybrid Deployments".

- The public cloud supports only Layer 3 features. Cisco ISE nodes on OCI do not support functions that depend on Layer 2 capabilities. For example, DHCP SPAN profiler probes and CDP protocol functions that are accessed through the Cisco ISE CLI are not supported.
- To enable IPv6 addresses in Cisco ISE, configure an IPv6 address in the OCI portal for Cisco ISE and restart interface Gigabit Ethernet 0. Log in as an administrator in the Cisco ISE Serial Console and run these commands:

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

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

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

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

Create a Cisco ISE instance in OCI

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

Before you begin

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

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

Procedure

Step 1 Navigate to the Cisco ISE option on the OCI console, on page 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 and click **Launch Instance**.

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

a) Click **Create Instance**.

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

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

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

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

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

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

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

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

A list of available shapes is displayed.

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

Step 6 In the **Networking** area:

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

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

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

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

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

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

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

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

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

Configure advanced options for a Cisco ISE instance

To configure the advanced options, follow these steps.

Procedure

Step 1 Click **Show advanced options**.

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

Note
Cisco ISE on OCI does not support IMDSv2.

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

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

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

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

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

Table 1: Configuration guidelines for User Data field

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

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

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

Step 6 Click **Create**.

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

User data parameters

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

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

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

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

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

Parameter syntax requirements

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

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

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

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

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

Before you begin

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

Procedure

Step 1 Create a Cisco ISE stack in OCI, on page 11.

Step 2 Configure variables for Cisco ISE instance, on page 12.

Step 3 Review configurations and create a Cisco ISE instance in OCI, on page 12.

Create a Cisco ISE stack in OCI

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

Procedure

Step 1 Log in to your OCI account.

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

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

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

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

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

a) Click **My Configuration**.

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

Configure variables for Cisco ISE instance

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

Procedure

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

Step 2 Click **Next**.

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

Review configurations and create a Cisco ISE instance in OCI

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

Procedure

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

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

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

Step 3 Click **Create**.

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

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

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

Postinstallation tasks

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

Compatibility information for Cisco ISE on OCI

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

Load balancer integration support

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

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

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

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

NIC jumbo frame support

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

Password recovery and reset on OCI

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

Reset Cisco ISE GUI password through serial console

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

Procedure

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

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

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

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

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

Step 5 Log in to the serial console.

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

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

Create a new public key pair in OCI

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

Procedure

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

Step 2 Log in to the OCI serial console.

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

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

Step 4 Import the new public key using this command:

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

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

Password recovery

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

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