Configure ISE 3.1 Through AWS Marketplace

Contents

Introduction

This document describes how to install Identity Services Engine (ISE) 3.1 via Amazon Machine Images (AMI) in Amazon Web Services (AWS). From version 3.1 ISE can be deployed as an Amazon Elastic Compute Cloud (EC2) instance with the help of CloudFormation Templates (CFT).

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of these topics:

- ISE
- AWS and its concepts like VPC, EC2, CloudFormation

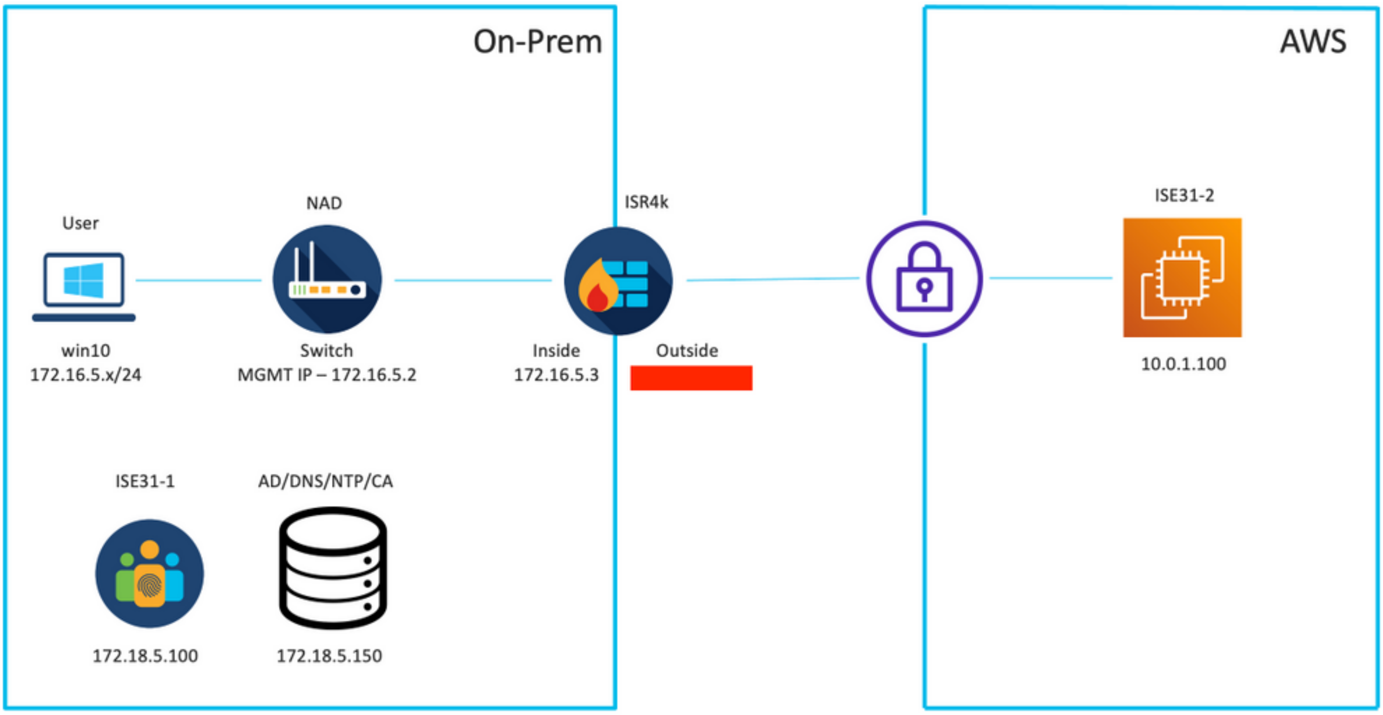
Components Used

The information in this document is based on Cisco ISE Version 3.1.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Topology

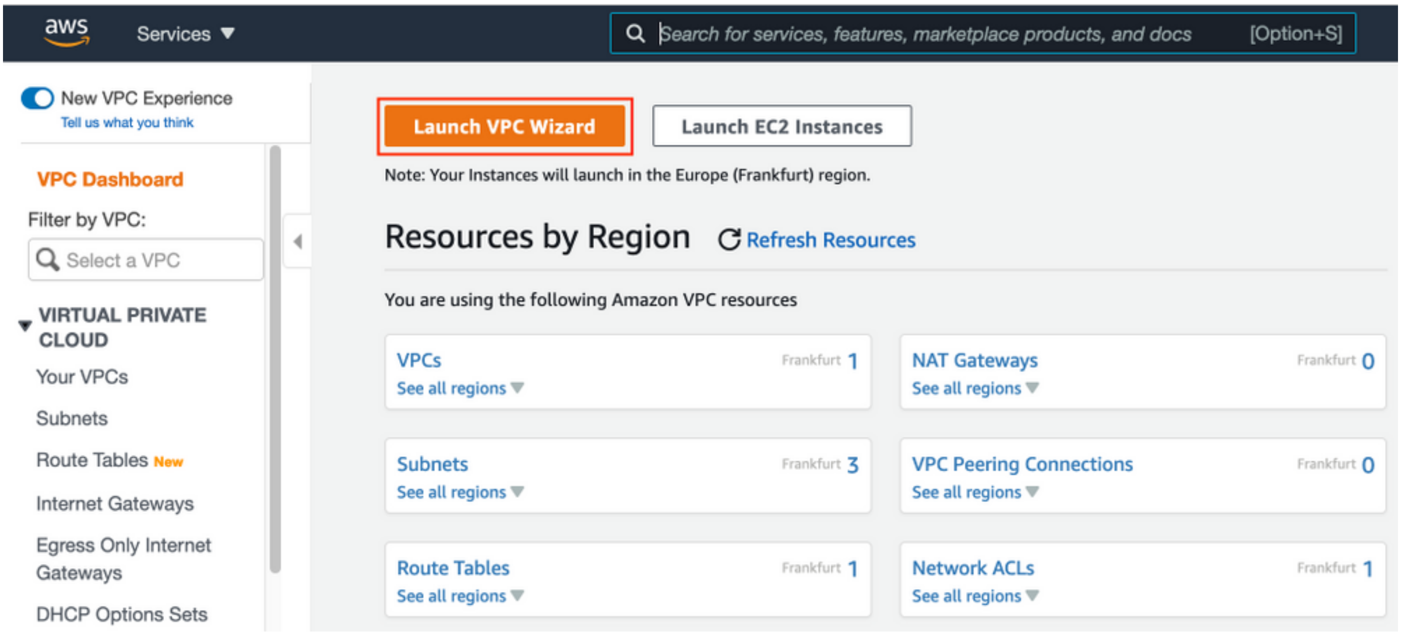


Configurations

If there is no VPC, Security Groups, Key Pairs and VPN tunnel configured yet, you need to follow Optional steps, otherwise, start with Step 1.

Optional Step A. Create VPC

Navigate to **VPC** AWS Service. Select **Launch VPC Wizard** as shown in the image.

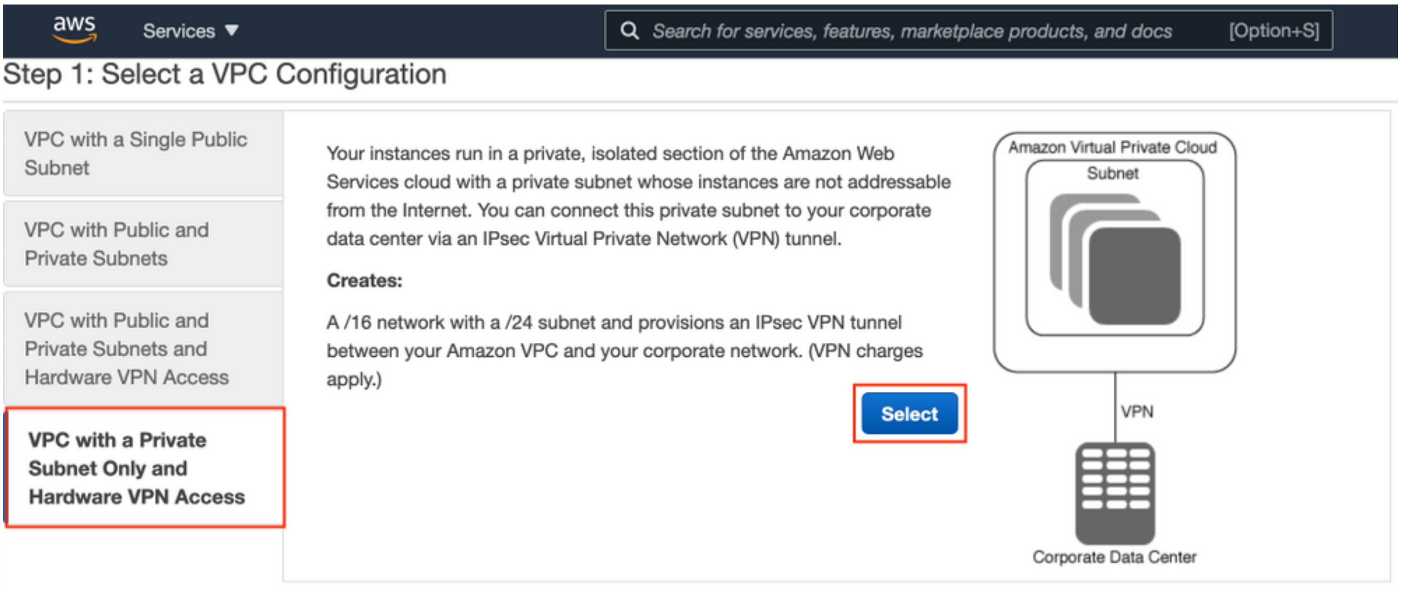


Note: Your Instances will launch in the Europe (Frankfurt) region.

You are using the following Amazon VPC resources

VPCs	See all regions ▼	Frankfurt 1
NAT Gateways	See all regions ▼	Frankfurt 0
Subnets	See all regions ▼	Frankfurt 3
VPC Peering Connections	See all regions ▼	Frankfurt 0
Route Tables	See all regions ▼	Frankfurt 1
Network ACLs	See all regions ▼	Frankfurt 1

Choose **VPC with Private Subnet Only and Hardware VPN Access** and click **Select** as shown in the image.


aws
Services ▼
Search for services, features, marketplace products, and docs [Option+S]
VPC with a Single Public Subnet
VPC with Public and Private Subnets
VPC with Public and Private Subnets and Hardware VPN Access
VPC with a Private Subnet Only and Hardware VPN Access
Select
Amazon Virtual Private Cloud
Subnet
VPN
Corporate Data Center

Step 1: Select a VPC Configuration

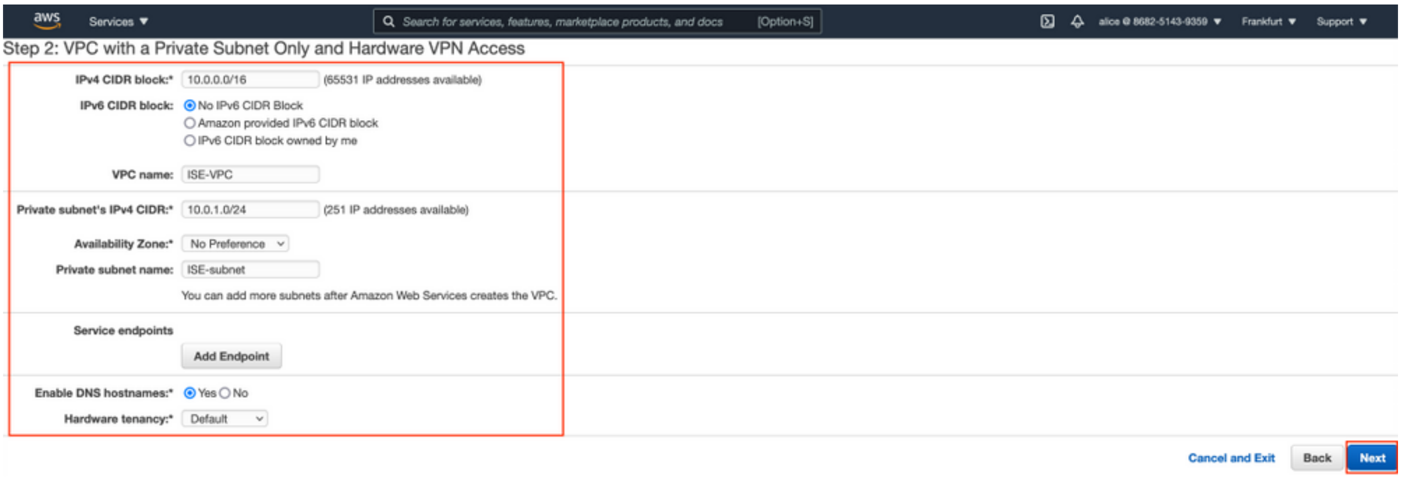
Your instances run in a private, isolated section of the Amazon Web Services cloud with a private subnet whose instances are not addressable from the Internet. You can connect this private subnet to your corporate data center via an IPsec Virtual Private Network (VPN) tunnel.

Creates:

A /16 network with a /24 subnet and provisions an IPsec VPN tunnel between your Amazon VPC and your corporate network. (VPN charges apply.)

> **Note**: The selection of VPC in Step 1. of the VPC wizard depends on the topology since ISE is not designed as Internet exposed server - VPN with private subnet only is used.

Configure VPC Private Subnet Settings as per your network design and Select **Next**.



Step 2: VPC with a Private Subnet Only and Hardware VPN Access

IPv4 CIDR block:* 10.0.0.0/16 (65531 IP addresses available)

IPv6 CIDR block: ● No IPv6 CIDR Block
○ Amazon provided IPv6 CIDR block
○ IPv6 CIDR block owned by me

VPC name: ISE-VPC

Private subnet's IPv4 CIDR:* 10.0.1.0/24 (251 IP addresses available)

Availability Zone:* No Preference

Private subnet name: ISE-subnet

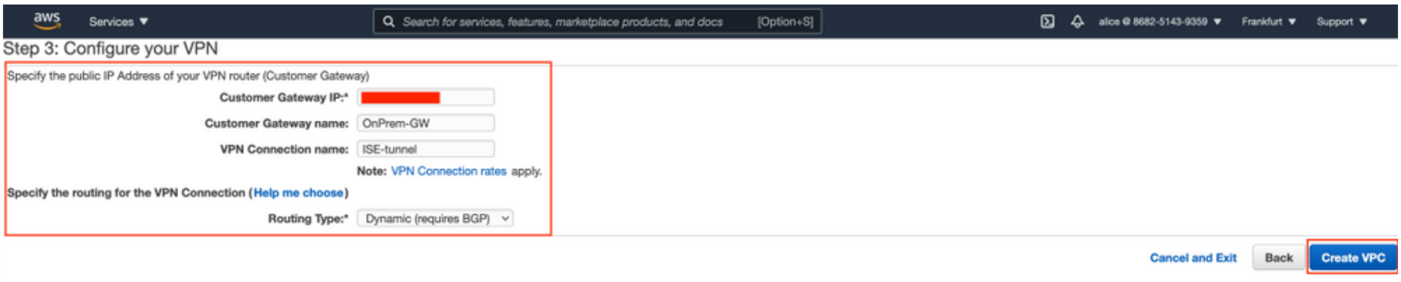
You can add more subnets after Amazon Web Services creates the VPC.

Service endpoints

Enable DNS hostnames:* ● Yes ○ No

Hardware tenancy:* Default

Configure your VPN as per your network design and Select **Create VPC**.



Step 3: Configure your VPN

Specify the public IP Address of your VPN router (Customer Gateway)

Customer Gateway IP:* [redacted]

Customer Gateway name: OnPrem-GW

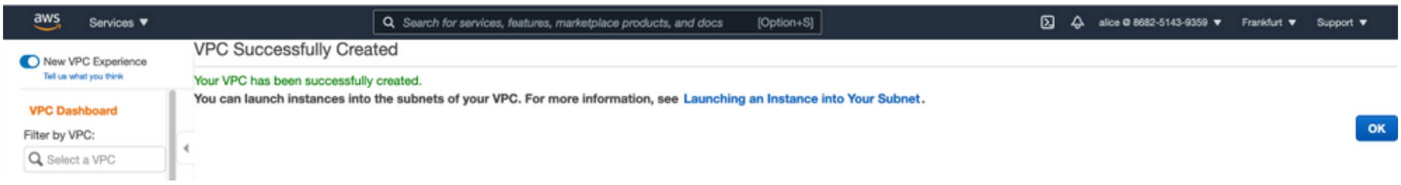
VPN Connection name: ISE-tunnel

Note: VPN Connection rates apply.

Specify the routing for the VPN Connection (Help me choose)

Routing Type:* Dynamic (requires BGP)

Once the VPC is created, the message **"Your VPC has been successfully created"** is displayed. Click **OK** as shown in the image.



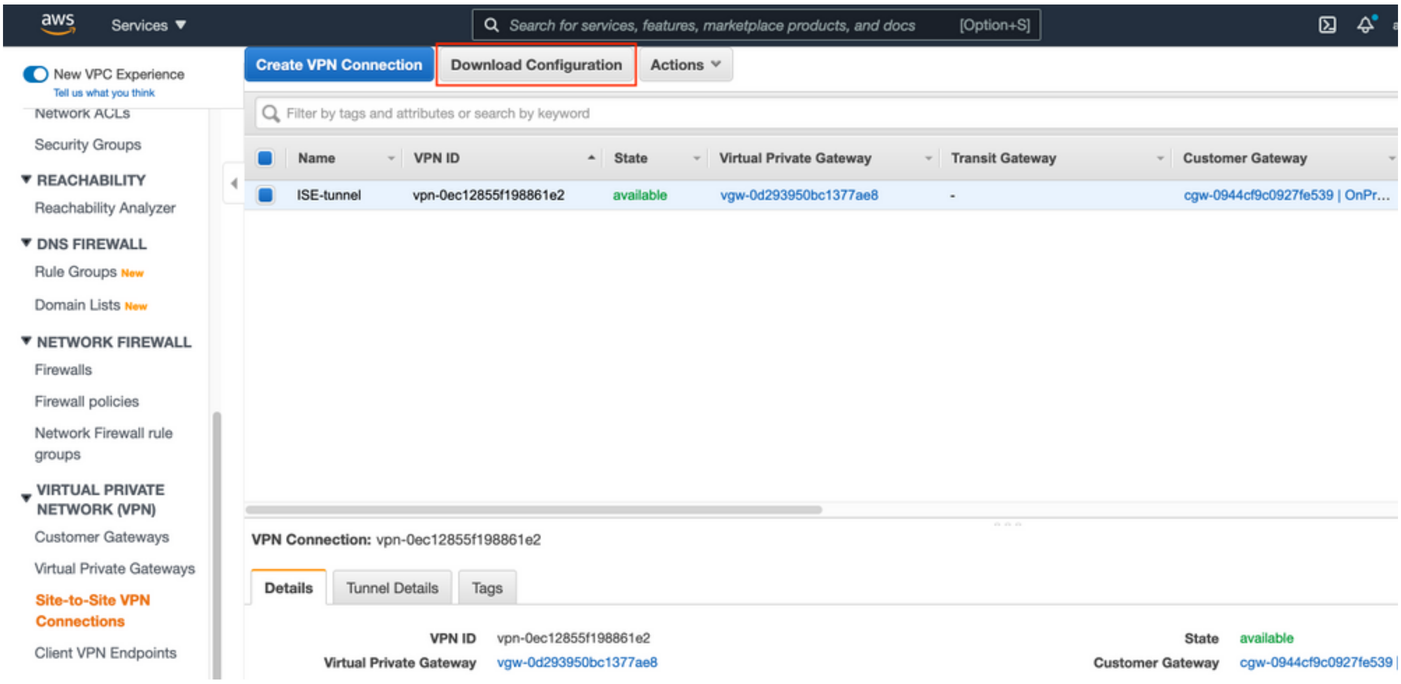
VPC Successfully Created

Your VPC has been successfully created.

You can launch instances into the subnets of your VPC. For more information, see Launching an Instance into Your Subnet.

Optional Step B. Configure On-Prem VPN Headend Device

Navigate to **VPC** AWS Service. Choose **Site-to-Site VPN connections**, select newly created VPN tunnel and Select **Download Configuration** as shown in the image.



	Name	VPN ID	State	Virtual Private Gateway	Transit Gateway	Customer Gateway
■	ISE-tunnel	vpn-0ec12855f198861e2	available	vgw-0d293950bc1377ae8	-	cgw-0944cf9c0927fe539 | OnPr...

VPN Connection: vpn-0ec12855f198861e2

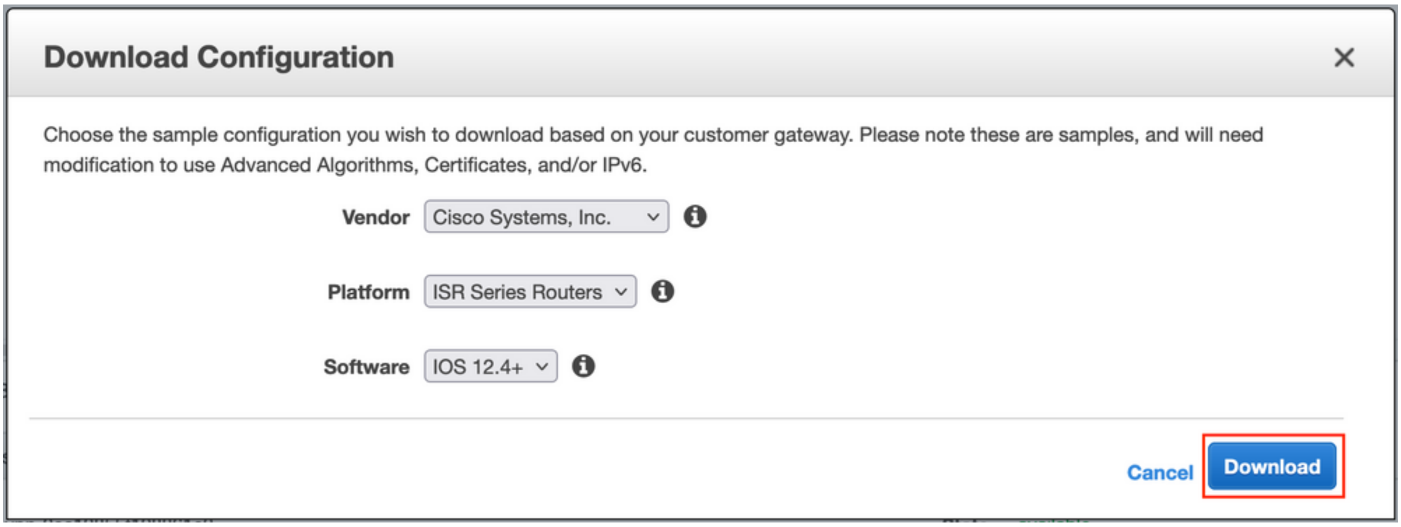
VPN ID vpn-0ec12855f198861e2

Virtual Private Gateway vgw-0d293950bc1377ae8

State available

Customer Gateway cgw-0944cf9c0927fe539 |

Choose **Vendor**, **Platform** and **Software**, Select **Download** as shown in the image.



Choose the sample configuration you wish to download based on your customer gateway. Please note these are samples, and will need modification to use Advanced Algorithms, Certificates, and/or IPv6.

Vendor: Cisco Systems, Inc.

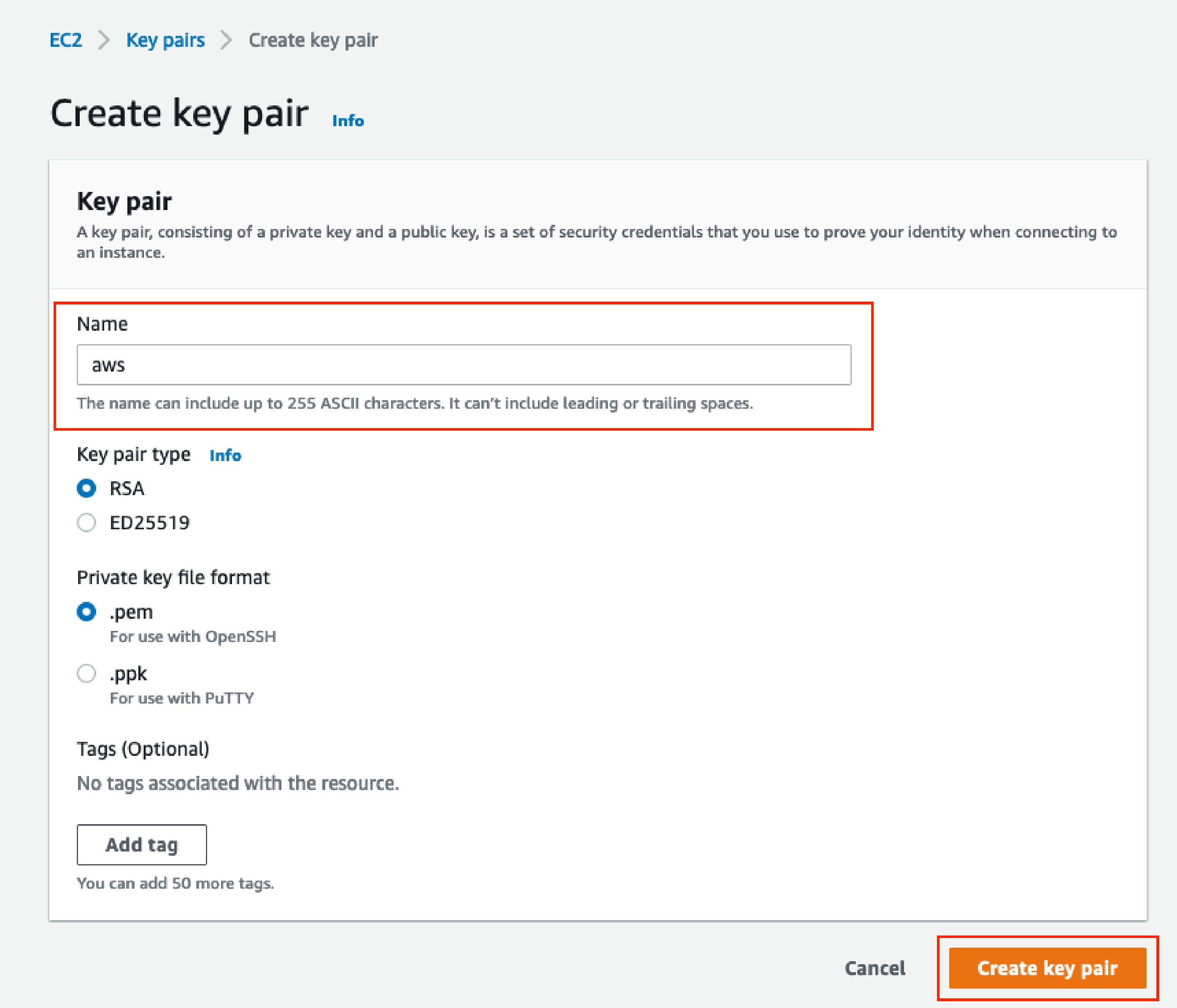
Platform: ISR Series Routers

Software: IOS 12.4+

Apply downloaded configuration on On-Prem VPN headend device.

Optional Step C. Create Custom Key Pair

AWS EC2 instances are accessed with the help of key pairs. In order to create a key pair, navigate to **EC2** Service. Select **Key Pairs** menu under **Network & Security.** Select **Create Key Pair**, give it a **Name,** leave other values as default and Select **Create Key Pair** again.



EC2 > Key pairs > Create key pair

Create key pair Info

Key pair

A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name

aws

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type Info

● RSA

○ ED25519

Private key file format

● .pem
For use with OpenSSH

○ .ppk
For use with PuTTY

Tags (Optional)

No tags associated with the resource.

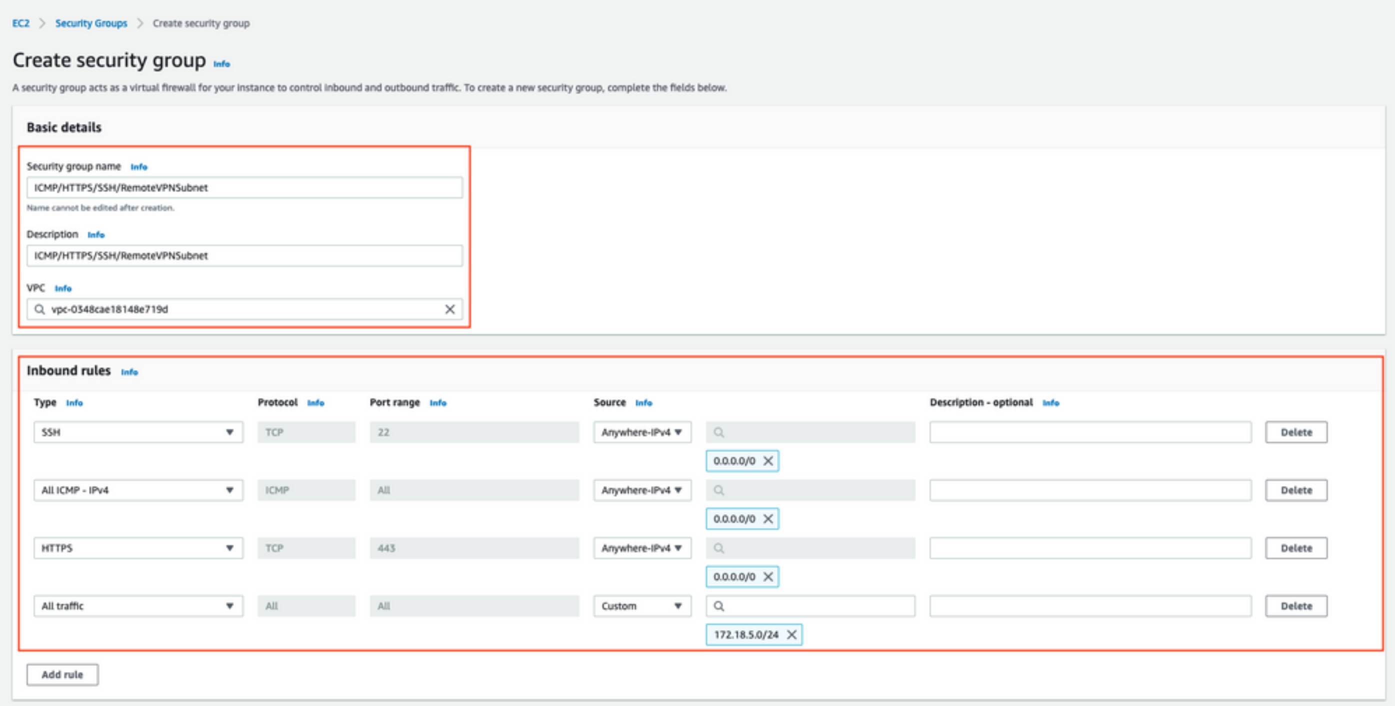
Add tag

You can add 50 more tags.

Cancel | Create key pair

Optional Step D. Create custom Security Group

AWS EC2 instances access is protected by **Security Groups**, in order to configure **Security Group**, navigate to **EC2** Service. Select **Security Groups** menu under **Network & Security.** Select **Create Security Group,** configure a **Name**, **Description,** in the **VPC** field select newly configured **VPC**. Configure **Inbound Rules** to allow communication to ISE. Select **Create Security Group** as shown in the image.



EC2 > Security Groups > Create security group

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name: ICMP/HTTPS/SSH/RemoteVPNSubnet

Name cannot be edited after creation.

Description: ICMP/HTTPS/SSH/RemoteVPNSubnet

VPC: vpc-0348cae18148e719d

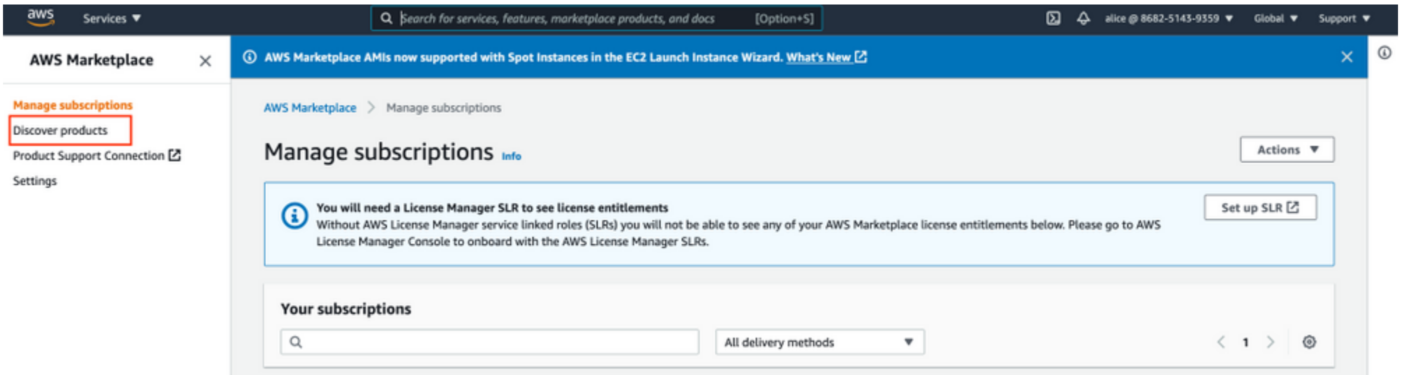
Inbound rules

Type	Protocol	Port range	Source		Description - optional
SSH	TCP	22	Anywhere-IPv4	0.0.0.0/0	
All ICMP - IPv4	ICMP	All	Anywhere-IPv4	0.0.0.0/0	
HTTPS	TCP	443	Anywhere-IPv4	0.0.0.0/0	
All traffic	All	All	Custom	172.18.5.0/24	

Note: The Security Group configured allows SSH, ICMP, HTTPS access to ISE and all protocols access from On-Prem subnet.

Step 1. Subscribe to AWS ISE Marketplace Product

Navigate to **AWS Marketplace Subscriptions** AWS Service. Select **Discover Products** as shown in the image.



AWS Marketplace AMIs now supported with Spot Instances in the EC2 Launch Instance Wizard. What's New

AWS Marketplace > Manage subscriptions

Manage subscriptions Info

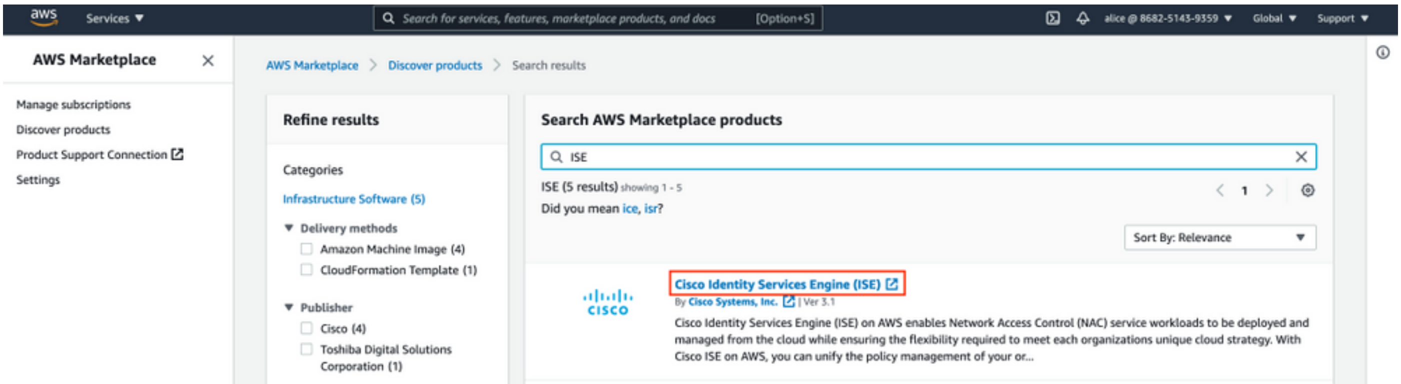
You will need a License Manager SLR to see license entitlements

Without AWS License Manager service linked roles (SLRs) you will not be able to see any of your AWS Marketplace license entitlements below. Please go to AWS License Manager Console to onboard with the AWS License Manager SLRs.

Your subscriptions

All delivery methods

Search for **ISE** product and Select **Cisco Identity Services Engine (ISE)** as shown in the image.



AWS Marketplace > Discover products > Search results

Refine results

Categories

Infrastructure Software (5)

Delivery methods

□ Amazon Machine Image (4)

□ CloudFormation Template (1)

Publisher

□ Cisco (4)

□ Toshiba Digital Solutions Corporation (1)

Search AWS Marketplace products

ISE

ISE (5 results) showing 1 - 5

Did you mean ice, isr?

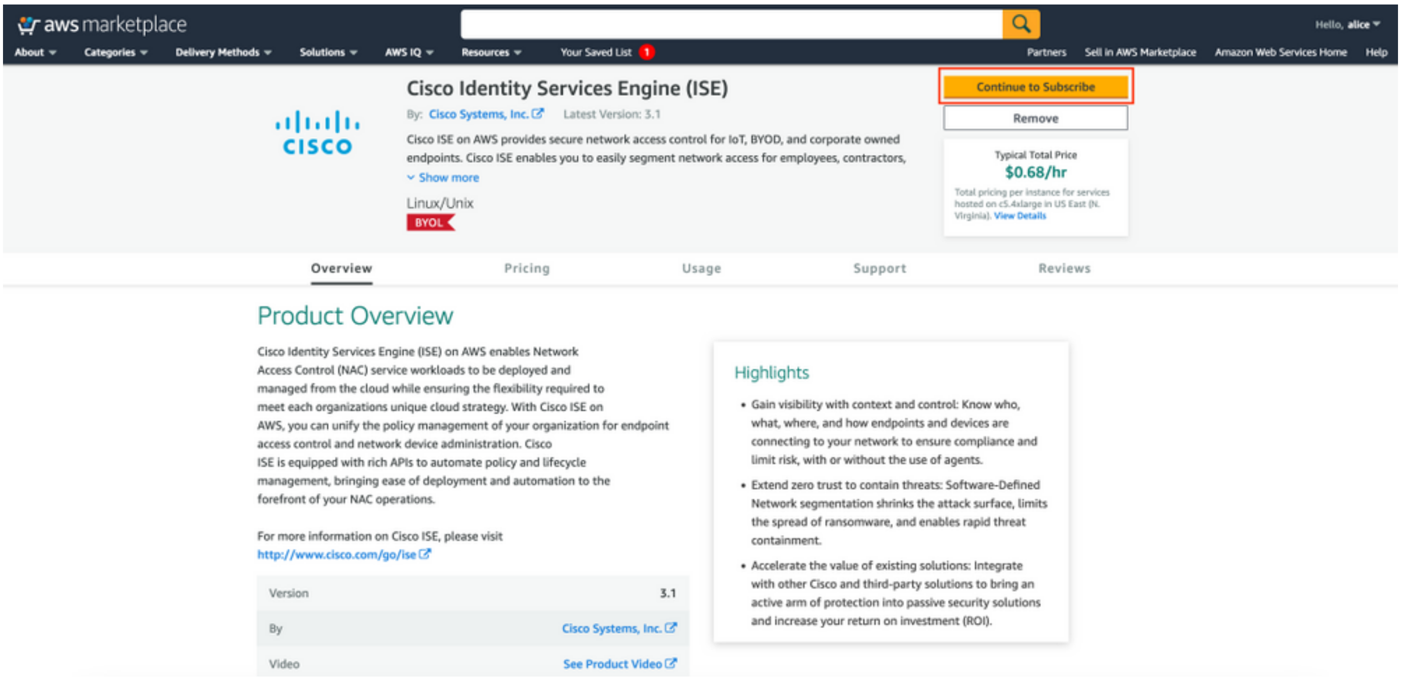
Sort By: Relevance

Cisco Identity Services Engine (ISE)

By Cisco Systems, Inc. | Ver 3.1

Cisco Identity Services Engine (ISE) on AWS enables Network Access Control (NAC) service workloads to be deployed and managed from the cloud while ensuring the flexibility required to meet each organizations unique cloud strategy. With Cisco ISE on AWS, you can unify the policy management of your or...

Select **Continue to Subscribe** button



Cisco Identity Services Engine (ISE)

By: Cisco Systems, Inc. Latest Version: 3.1

Cisco ISE on AWS provides secure network access control for IoT, BYOD, and corporate owned endpoints. Cisco ISE enables you to easily segment network access for employees, contractors,

Show more

Linux/Unix

BYOL

Typical Total Price
$0.68/hr
Total pricing per instance for services hosted on c5.4xlarge in US East (N. Virginia). View Details

Product Overview

Cisco Identity Services Engine (ISE) on AWS enables Network Access Control (NAC) service workloads to be deployed and managed from the cloud while ensuring the flexibility required to meet each organizations unique cloud strategy. With Cisco ISE on AWS, you can unify the policy management of your organization for endpoint access control and network device administration. Cisco ISE is equipped with rich APIs to automate policy and lifecycle management, bringing ease of deployment and automation to the forefront of your NAC operations.

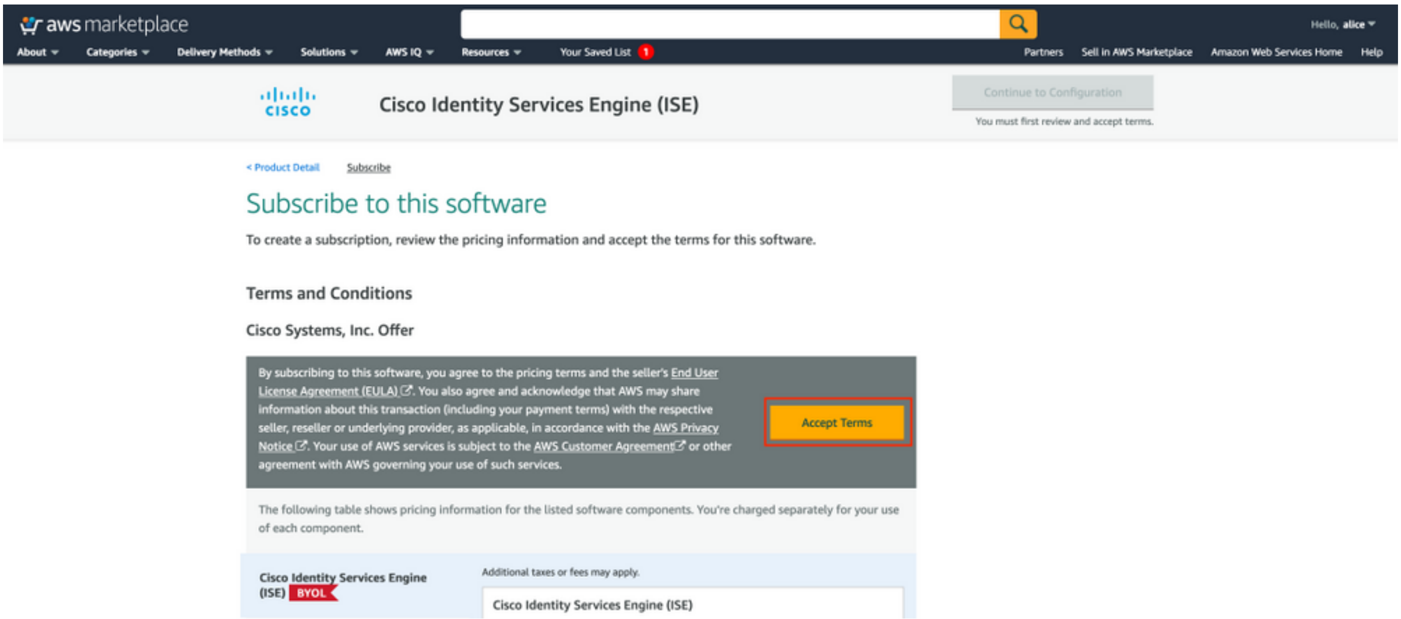
For more information on Cisco ISE, please visit http://www.cisco.com/go/ise

Version	3.1
By	Cisco Systems, Inc.
Video	See Product Video

Highlights

- Gain visibility with context and control: Know who, what, where, and how endpoints and devices are connecting to your network to ensure compliance and limit risk, with or without the use of agents.
- Extend zero trust to contain threats: Software-Defined Network segmentation shrinks the attack surface, limits the spread of ransomware, and enables rapid threat containment.
- Accelerate the value of existing solutions: Integrate with other Cisco and third-party solutions to bring an active arm of protection into passive security solutions and increase your return on investment (ROI).

Select **Accept Terms** button as shown in the image.



Cisco Identity Services Engine (ISE)

You must first review and accept terms.

Subscribe to this software

To create a subscription, review the pricing information and accept the terms for this software.

Terms and Conditions

Cisco Systems, Inc. Offer

By subscribing to this software, you agree to the pricing terms and the seller's End User License Agreement (EULA). You also agree and acknowledge that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the AWS Privacy Notice. Your use of AWS services is subject to the AWS Customer Agreement or other agreement with AWS governing your use of such services.

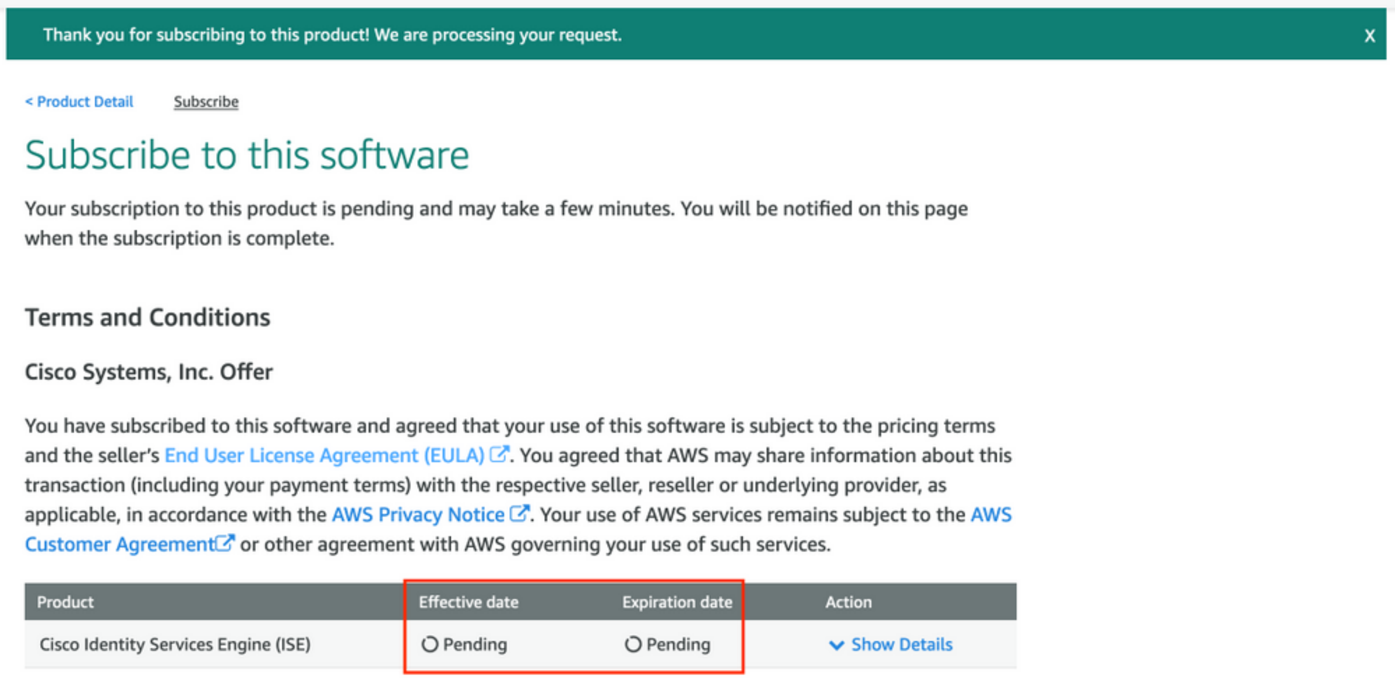
The following table shows pricing information for the listed software components. You're charged separately for your use of each component.

Cisco Identity Services Engine (ISE) BYOL

Additional taxes or fees may apply.

Cisco Identity Services Engine (ISE)

Once subscribed the status of **Effective** and **Expiration date** with change to **Pending** as shown in the image.



Thank you for subscribing to this product! We are processing your request. X

< Product Detail Subscribe

Subscribe to this software

Your subscription to this product is pending and may take a few minutes. You will be notified on this page when the subscription is complete.

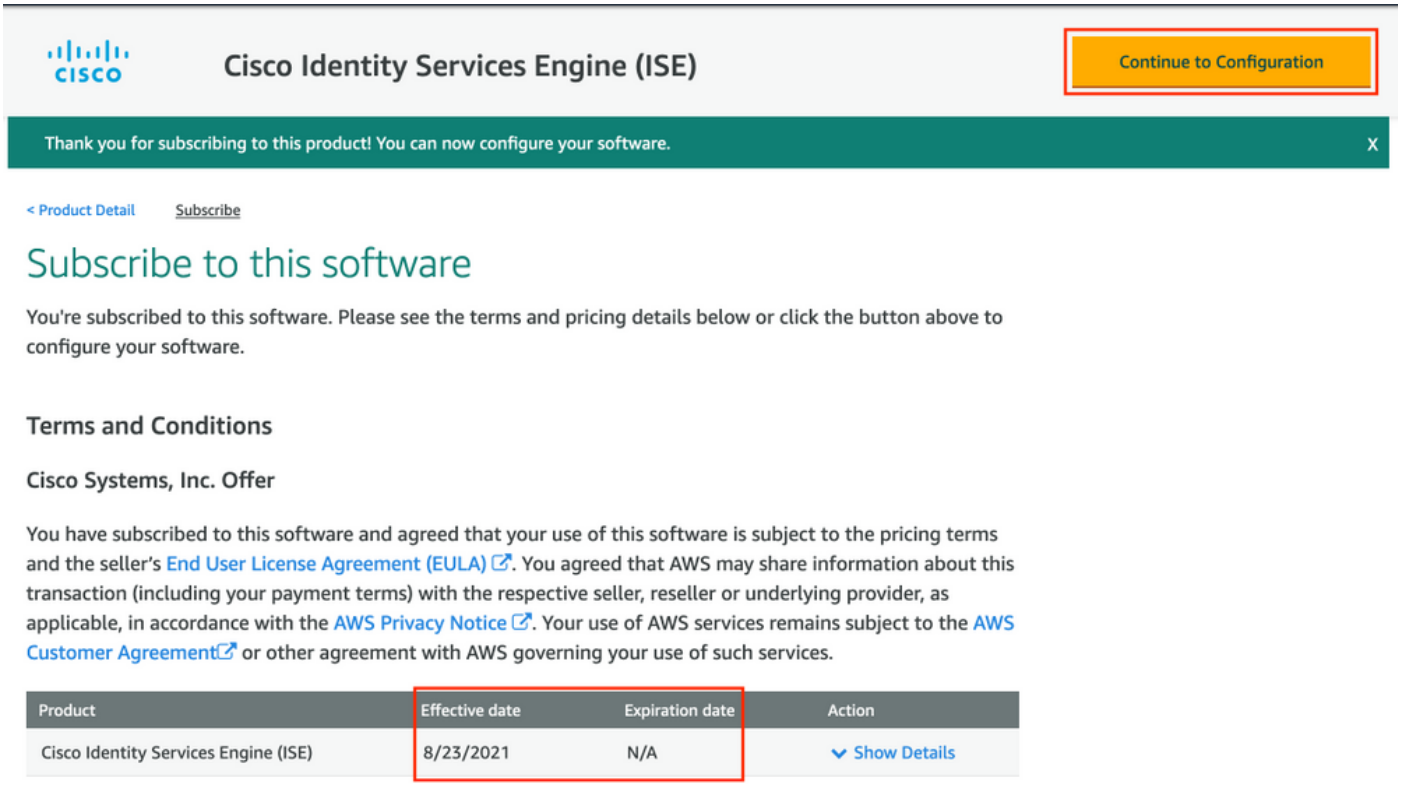
Terms and Conditions

Cisco Systems, Inc. Offer

You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA). You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the AWS Privacy Notice. Your use of AWS services remains subject to the AWS Customer Agreement or other agreement with AWS governing your use of such services.

Product	Effective date	Expiration date	Action
Cisco Identity Services Engine (ISE)	○ Pending	○ Pending	Show Details

Shortly after the **Effective date** changes to the date of Subscription and the **Expiration date** changes to **N/A.** Select **Continue to Configuration** as shown in the ima



Cisco Identity Services Engine (ISE)

Thank you for subscribing to this product! You can now configure your software. X

< Product Detail Subscribe

Subscribe to this software

You're subscribed to this software. Please see the terms and pricing details below or click the button above to configure your software.

Terms and Conditions

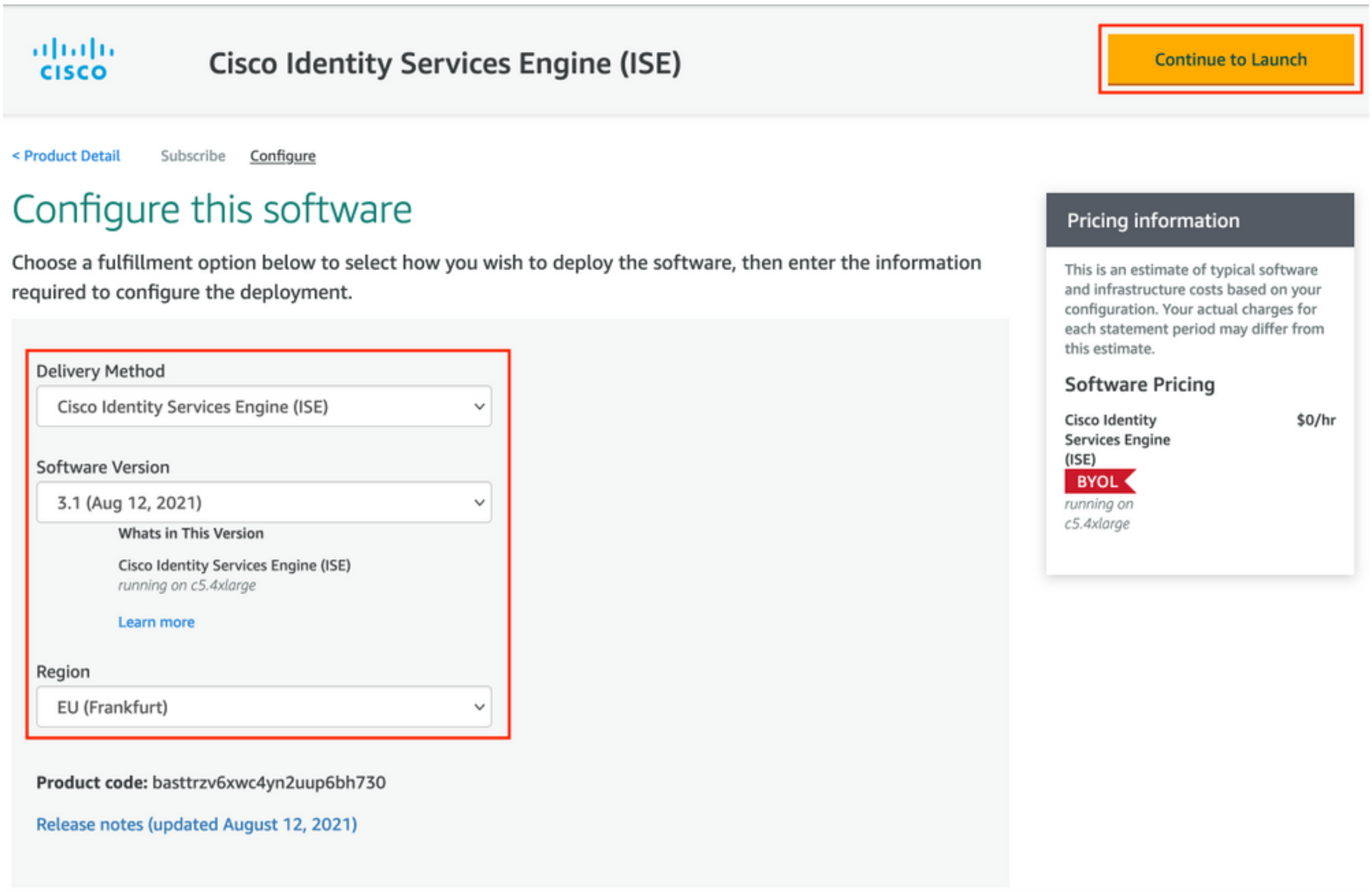
Cisco Systems, Inc. Offer

You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA). You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the AWS Privacy Notice. Your use of AWS services remains subject to the AWS Customer Agreement or other agreement with AWS governing your use of such services.

Product	Effective date	Expiration date	Action
Cisco Identity Services Engine (ISE)	8/23/2021	N/A	Show Details

Step 2. Configure ISE on AWS

In the Delivery Method menu of the **Configure this software screen** select **Cisco Identity Services Engine (ISE).** In the **Software Version** select **3.1 (Aug 12, 2021)**. Select the **Region**, where ISE is planned to be deployed. Select **Continue to Launch.**



Configure this software

Choose a fulfillment option below to select how you wish to deploy the software, then enter the information required to configure the deployment.

Delivery Method: Cisco Identity Services Engine (ISE)

Software Version: 3.1 (Aug 12, 2021)

Whats in This Version

Cisco Identity Services Engine (ISE)
running on c5.4xlarge

Learn more

Region: EU (Frankfurt)

Product code: basttrzv6xwc4yn2uup6bh730

Release notes (updated August 12, 2021)

Pricing information

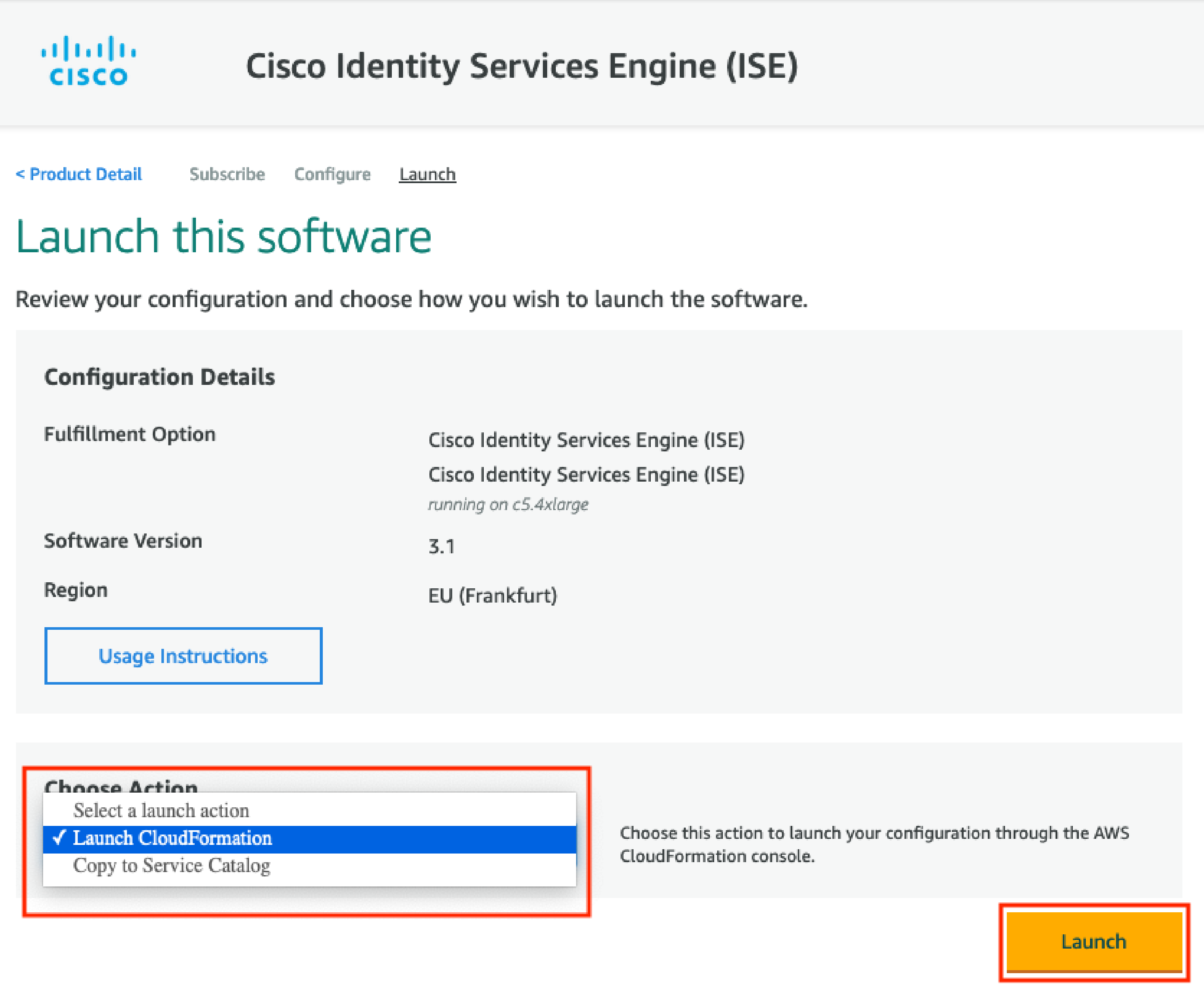
This is an estimate of typical software and infrastructure costs based on your configuration. Your actual charges for each statement period may differ from this estimate.

Software Pricing

Cisco Identity Services Engine (ISE) BYOL *running on c5.4xlarge* $0/hr

Step 3. Launch ISE on AWS

From the Actions drop-down menu of the **Launch this Software** screen, select **Launch CloudFormation**.



Cisco Identity Services Engine (ISE)

< Product Detail   Subscribe   Configure   Launch

Launch this software

Review your configuration and choose how you wish to launch the software.

Configuration Details

Fulfillment Option	Cisco Identity Services Engine (ISE) Cisco Identity Services Engine (ISE) *running on c5.4xlarge*
Software Version	3.1
Region	EU (Frankfurt)

Usage Instructions

Choose Action

Select a launch action
✓ Launch CloudFormation
Copy to Service Catalog

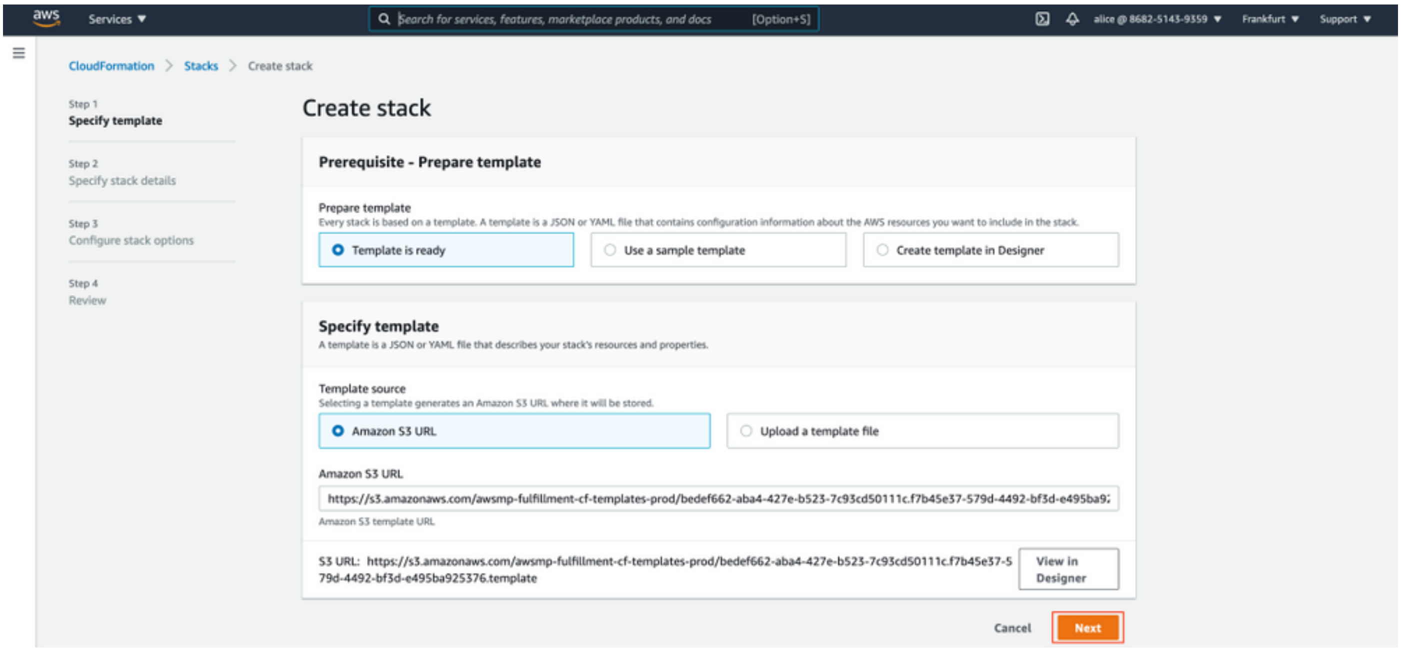
Choose this action to launch your configuration through the AWS CloudFormation console.

Launch

(Optional) Select **Usage instructions** to make yourself familiar with them. Select **Launch**.

Step 4. Configure CloudFormation Stack for ISE on AWS

Launch button redirects you to the **CloudFormation Stack** setup screen. There is a prebuilt template that must be used to set up ISE. Keep default settings and select **Next**.



aws
Services ▼
Search for services, features, marketplace products, and docs [Option+S]
alice @ 8682-5143-9359 ▼
Frankfurt ▼
Support ▼

CloudFormation > Stacks > Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Create stack

Prerequisite - Prepare template

Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

● Template is ready ○ Use a sample template ○ Create template in Designer

Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.

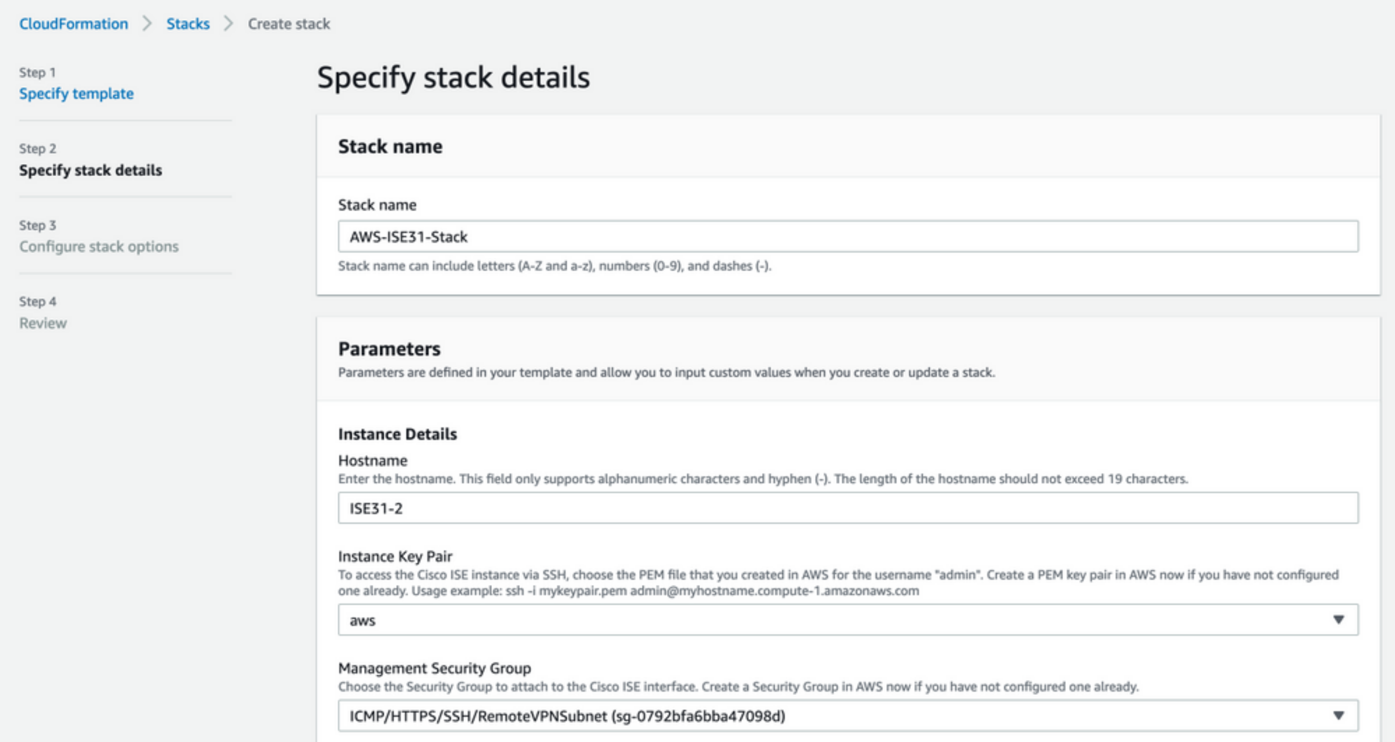
Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

● Amazon S3 URL ○ Upload a template file

Amazon S3 URL
https://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/bedef662-aba4-427e-b523-7c93cd50111c.f7b45e37-579d-4492-bf3d-e495ba9
Amazon S3 template URL

S3 URL: https://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/bedef662-aba4-427e-b523-7c93cd50111c.f7b45e37-579d-4492-bf3d-e495ba925376.template

Populate CloudFormation Stack data with **Stack Name**. Configure Instance Details like **Hostname**, select Instance **Key Pair** and **Management Security Group.**



CloudFormation > Stacks > Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Specify stack details

Stack name

Stack name
AWS-ISE31-Stack
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.

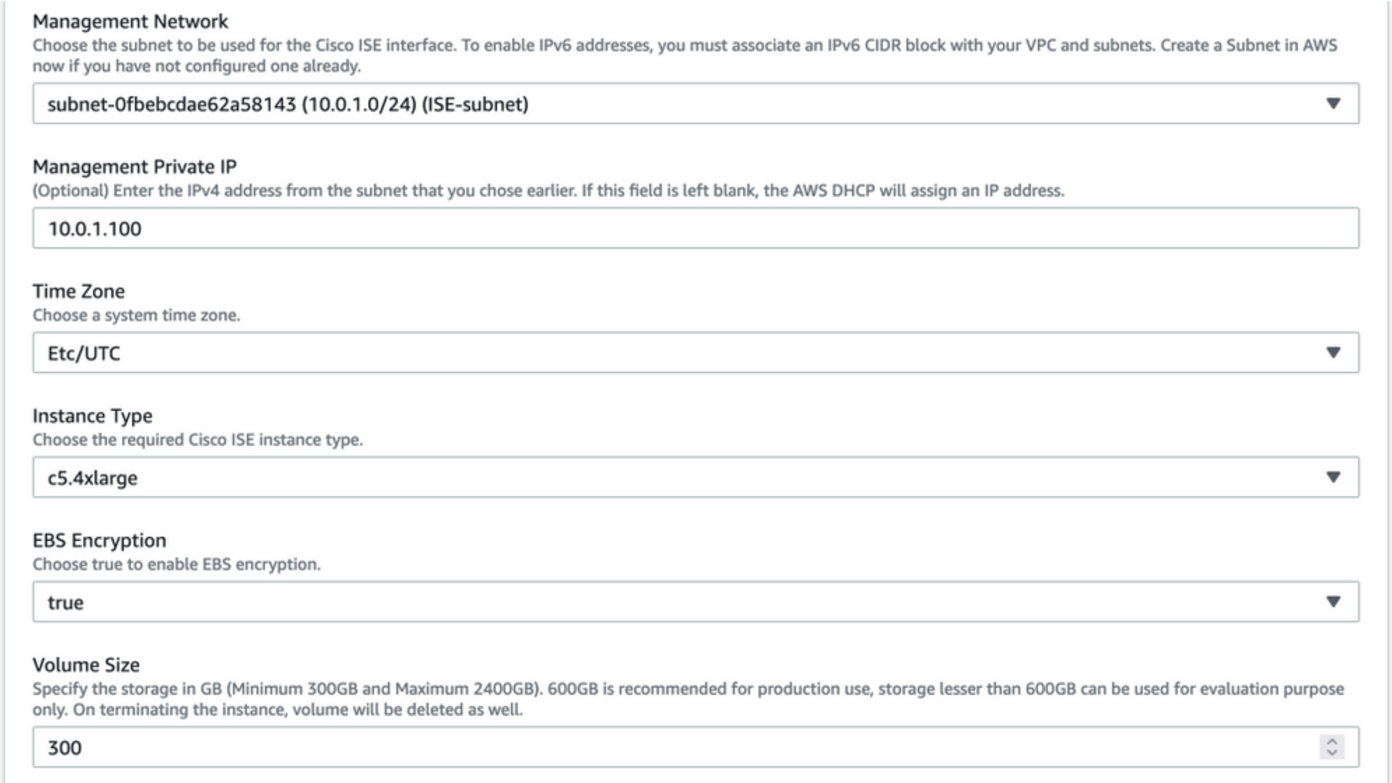
Instance Details

Hostname
Enter the hostname. This field only supports alphanumeric characters and hyphen (-). The length of the hostname should not exceed 19 characters.
ISE31-2

Instance Key Pair
To access the Cisco ISE instance via 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. Usage example: ssh -i mykeypair.pem admin@myhostname.compute-1.amazonaws.com
aws ▼

Management Security Group
Choose the Security Group to attach to the Cisco ISE interface. Create a Security Group in AWS now if you have not configured one already.
ICMP/HTTPS/SSH/RemoteVPNSubnet (sg-0792bfa6bba47098d) ▼

Continue Instance Details configuration with **Management Network, Management Private IP, Time Zone**, **Instance Type, EBS Encryption** and **Volume Size.**



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.

subnet-0fbebcdae62a58143 (10.0.1.0/24) (ISE-subnet) ▼

Management Private IP

(Optional) Enter the IPv4 address from the subnet that you chose earlier. If this field is left blank, the AWS DHCP will assign an IP address.

10.0.1.100

Time Zone

Choose a system time zone.

Etc/UTC ▼

Instance Type

Choose the required Cisco ISE instance type.

c5.4xlarge ▼

EBS Encryption

Choose true to enable EBS encryption.

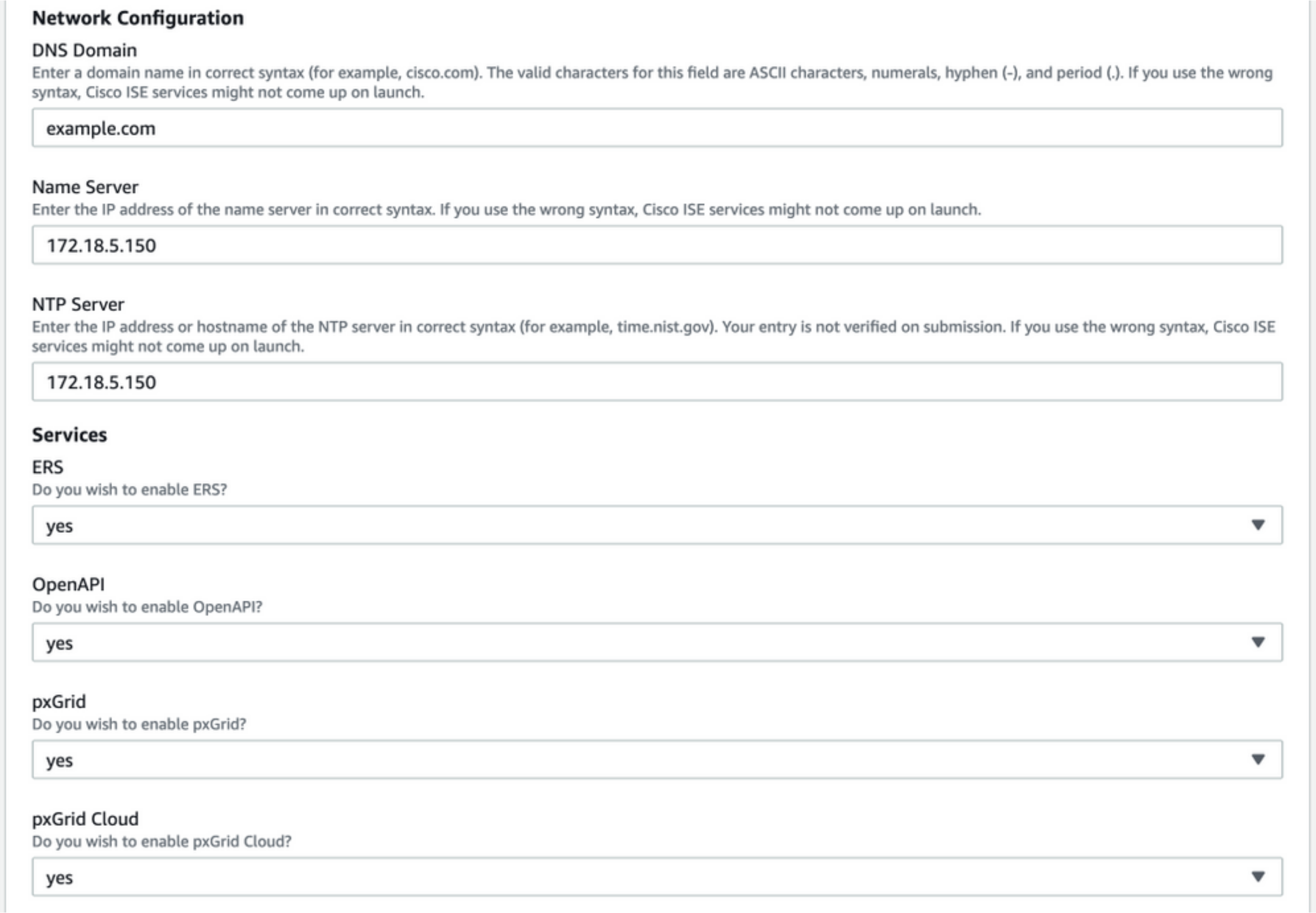
true ▼

Volume Size

Specify the storage in GB (Minimum 300GB and Maximum 2400GB). 600GB is recommended for production use, storage lesser than 600GB can be used for evaluation purpose only. On terminating the instance, volume will be deleted as well.

300

Continue Instance Details configuration with **DNS Domain, Name Server, NTP Service** and **Services**.



Network Configuration

DNS Domain

Enter a domain name in correct syntax (for example, cisco.com). The valid characters for this field are ASCII characters, numerals, hyphen (-), and period (.). If you use the wrong syntax, Cisco ISE services might not come up on launch.

example.com

Name Server

Enter the IP address of the name server in correct syntax. If you use the wrong syntax, Cisco ISE services might not come up on launch.

172.18.5.150

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.

172.18.5.150

Services

ERS

Do you wish to enable ERS?

yes ▼

OpenAPI

Do you wish to enable OpenAPI?

yes ▼

pxGrid

Do you wish to enable pxGrid?

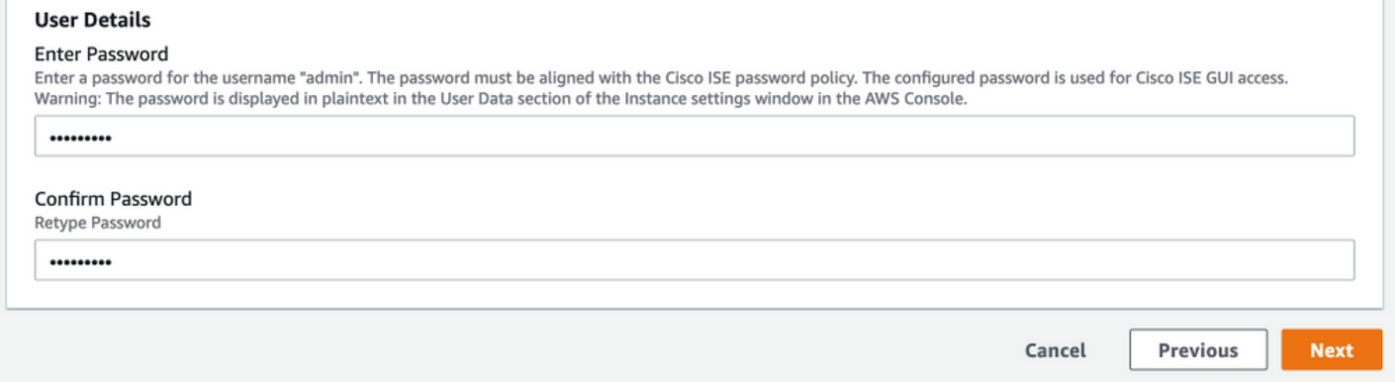
yes ▼

pxGrid Cloud

Do you wish to enable pxGrid Cloud?

yes ▼

Configure GUI user password and select **Next**.



User Details

Enter Password

Enter a password for the username "admin". The password must be aligned with the Cisco ISE password policy. The configured password is used for Cisco ISE GUI access.
Warning: The password is displayed in plaintext in the User Data section of the Instance settings window in the AWS Console.

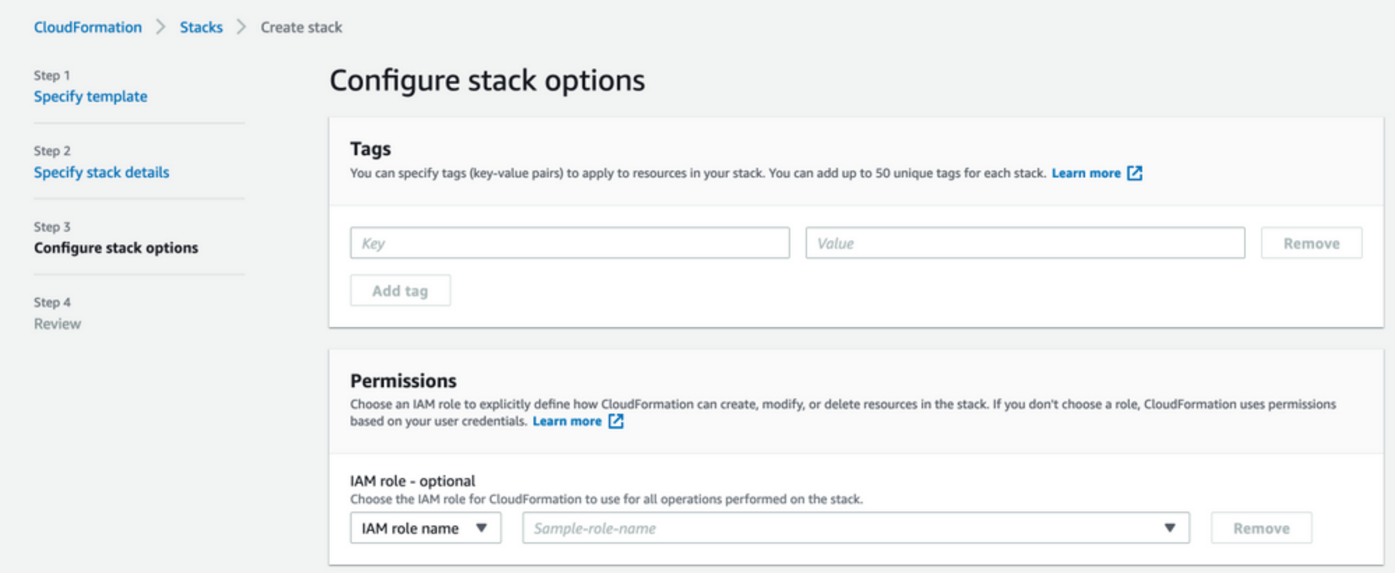
•••••••••

Confirm Password

Retype Password

•••••••••

No changes are required on the next screen. Select **Next**.



Configure stack options

Tags

You can specify tags (key-value pairs) to apply to resources in your stack. You can add up to 50 unique tags for each stack. Learn more

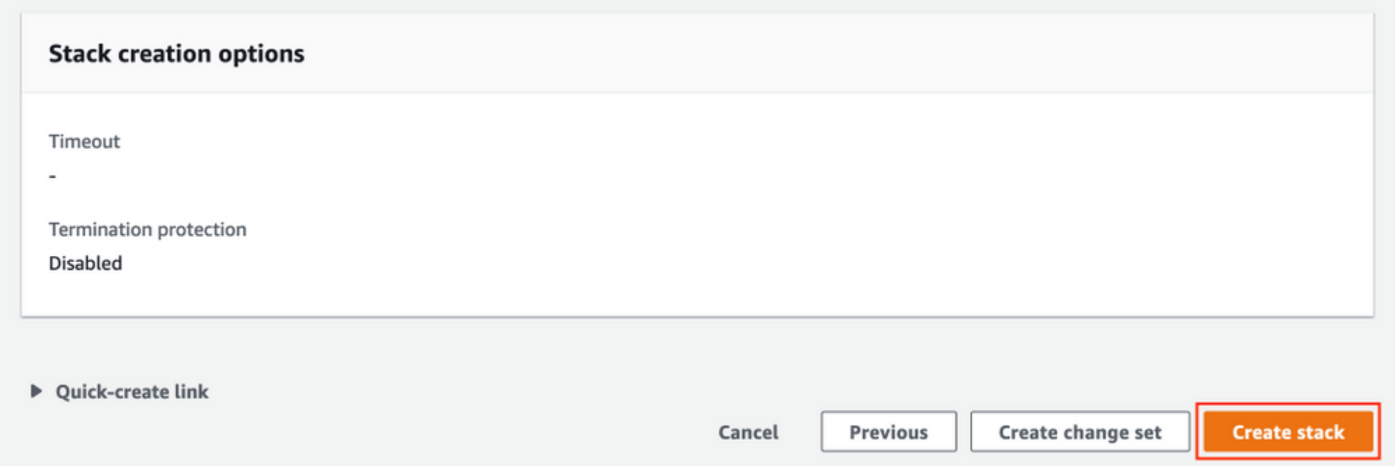
Permissions

Choose an IAM role to explicitly define how CloudFormation can create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses permissions based on your user credentials. Learn more

IAM role - optional

Choose the IAM role for CloudFormation to use for all operations performed on the stack.

Go over the **Review Stack** screen, scroll down and Select **Create stack**.



Stack creation options

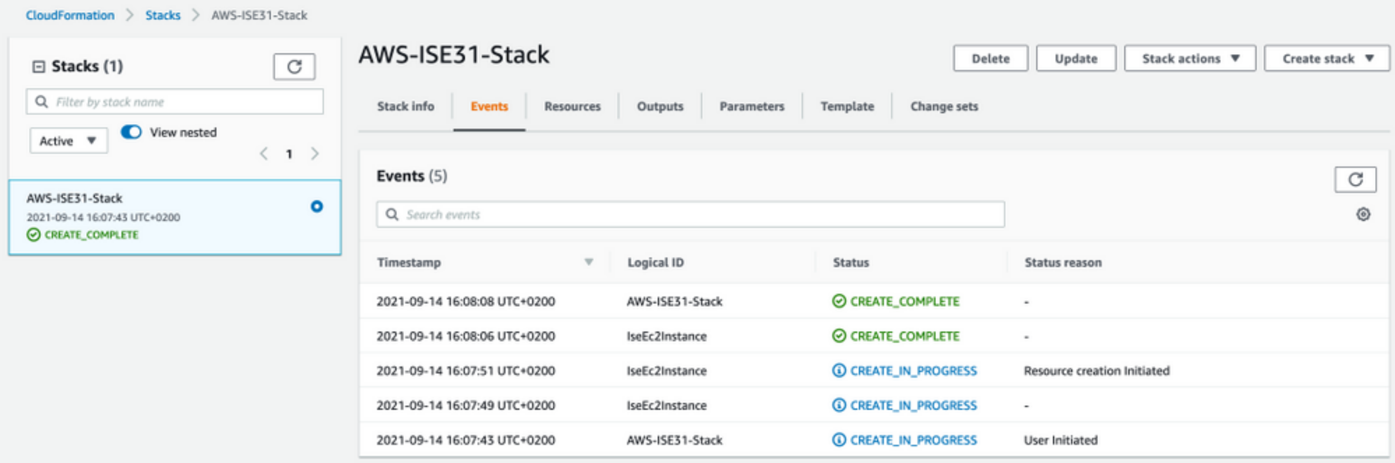
Timeout

-

Termination protection

Disabled

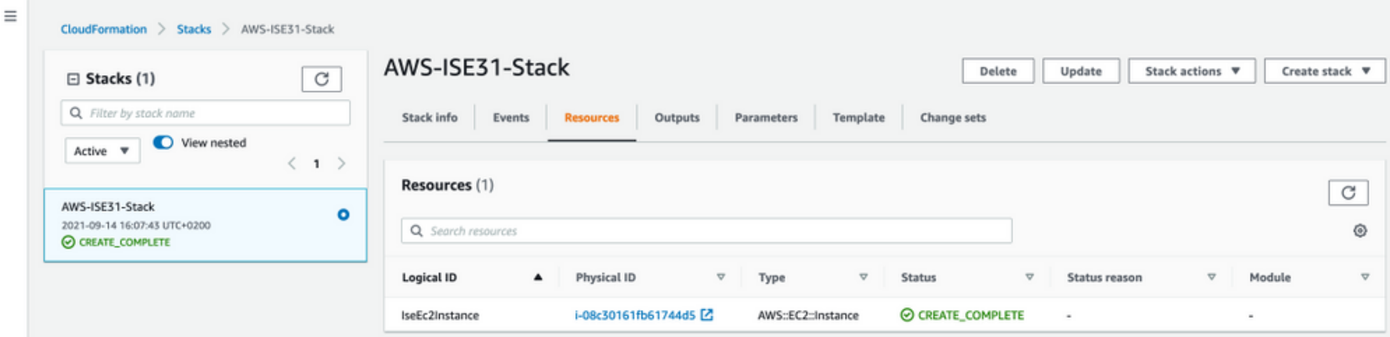
Once the Stack is deployed **CREATE_COMPLETE** status must be seen.



Timestamp	Logical ID	Status	Status reason
2021-09-14 16:08:08 UTC+0200	AWS-ISE31-Stack	CREATE_COMPLETE	-
2021-09-14 16:08:06 UTC+0200	IseEc2Instance	CREATE_COMPLETE	-
2021-09-14 16:07:51 UTC+0200	IseEc2Instance	CREATE_IN_PROGRESS	Resource creation Initiated
2021-09-14 16:07:49 UTC+0200	IseEc2Instance	CREATE_IN_PROGRESS	-
2021-09-14 16:07:43 UTC+0200	AWS-ISE31-Stack	CREATE_IN_PROGRESS	User Initiated

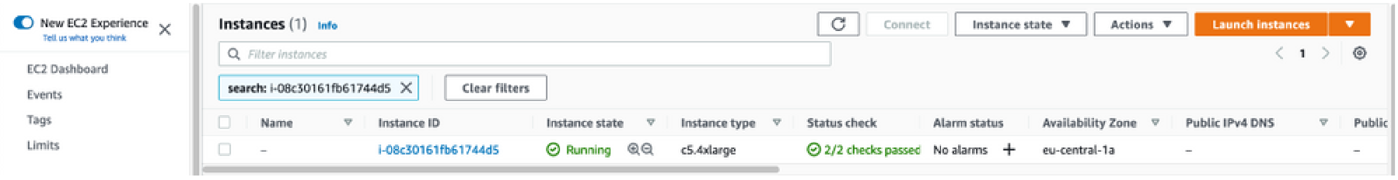
Step 5. Access ISE on AWS

In order to access ISE instance, navigate to the **Resources** tab to view the EC2 instance created from CloudForms (Alternatively navigate to **Services > EC2 > Instances** in order to view the EC2 instances) as shown in the image.



Logical ID	Physical ID	Type	Status	Status reason	Module
IseEc2Instance	i-08c30161fb61744d5	AWS::EC2::Instance	CREATE_COMPLETE	-	-

Select **Physical ID** in order to open **EC2 Instances** menu. Ensure the **Status check** has **2/2 checks passed** status.



Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public
–	i-08c30161fb61744d5	Running	c5.4xlarge	2/2 checks passed	No alarms	eu-central-1a	–	–

Select **Instance ID**. ISE can be accessed via **Private IPv4 address/Private IPv4 DNS** with SSH or HTTPS protocol.

> **Note**: If you access ISE via **Private IPv4 address/Private IPv4 DNS** ensure that there is network connectivity towards ISE private address.

Example of ISE accessed via **Private IPv4 Address** via SSH:

```
[centos@ip-172-31-42-104 ~]$ ssh -i aws.pem admin@10.0.1.100
The authenticity of host '10.0.1.100 (10.0.1.100)' can't be established.
ECDSA key fingerprint is SHA256:G5NdGZ1rgPYnjnldPcXOLcJg9VICLSxnZA0kn0CfMPs.
ECDSA key fingerprint is MD5:aa:e1:7f:8f:35:e8:44:13:f3:48:be:d3:4f:5f:05:f8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.1.100' (ECDSA) to the list of known hosts.
Last login: Tue Sep 14 14:36:39 2021 from 172.31.42.104
```

```
Failed to log in 0 time(s)
ISE31-2/admin#
```

> **Note**: It takes around 20 minutes for ISE to be accessible via SSH. Till that time connectivity to ISE fails with "**Permission denied (publickey).**" error message.

Use **show application status ise** in order to verify that services are running:

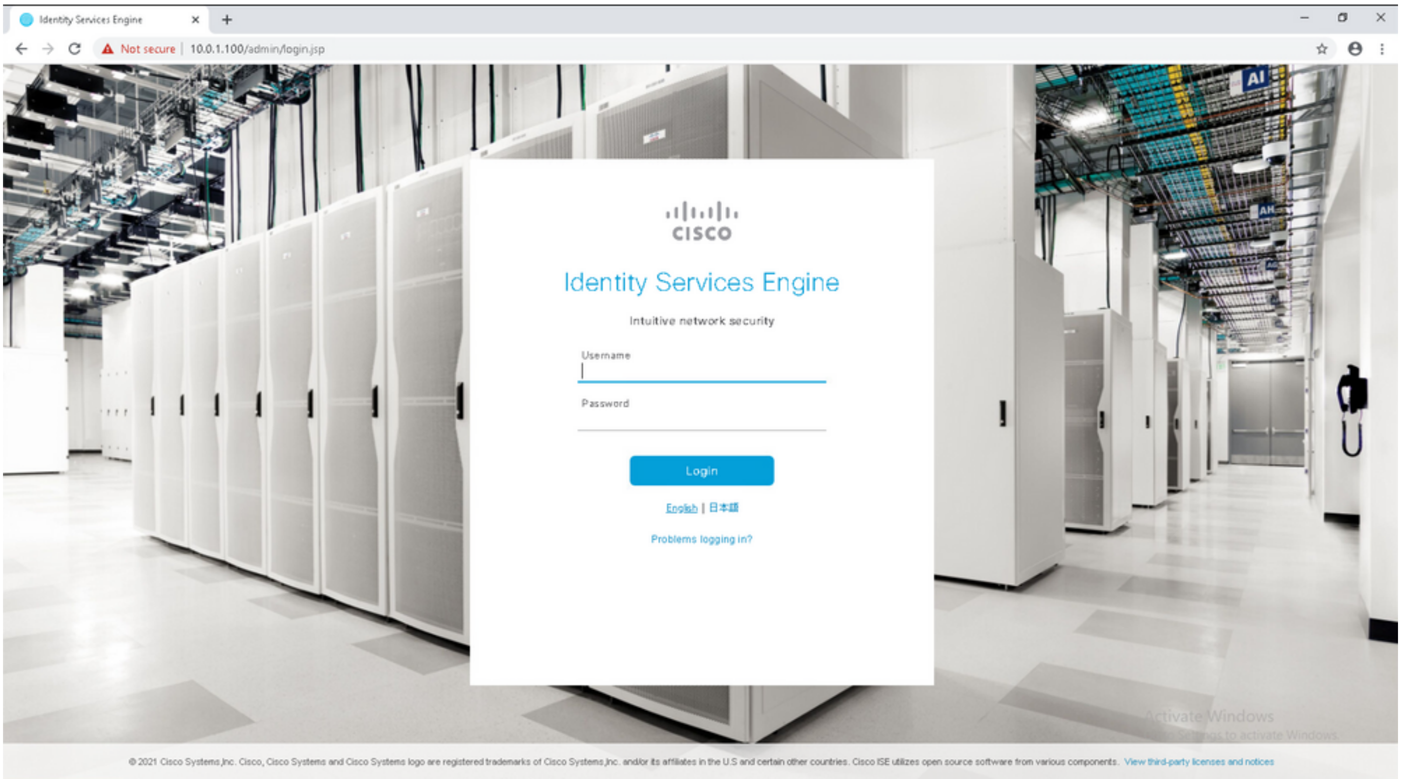
```
ISE31-2/admin# show application status ise

ISE PROCESS NAME STATE PROCESS ID
--------------------------------------------------------------------
Database Listener running 27703
Database Server running 127 PROCESSES
Application Server                      running         47142
Profiler Database running 38593
ISE Indexing Engine running 48309
AD Connector running 56223
M&T Session Database running 37058
M&T Log Processor running 47400
Certificate Authority Service running 55683
EST Service running
SXP Engine Service disabled
TC-NAC Service disabled
PassiveID WMI Service disabled
PassiveID Syslog Service disabled
PassiveID API Service disabled
PassiveID Agent Service disabled
PassiveID Endpoint Service disabled
PassiveID SPAN Service disabled
DHCP Server (dhcpd) disabled
DNS Server (named) disabled
ISE Messaging Service running 30760
ISE API Gateway Database Service running 35316
ISE API Gateway Service running 44900
Segmentation Policy Service disabled
REST Auth Service disabled
SSE Connector disabled
Hermes (pxGrid Cloud Agent) Service disabled

ISE31-2/admin#
```

> **Note**: It takes around 10-15 minutes since SSH is available for ISE services to transition to a running state.

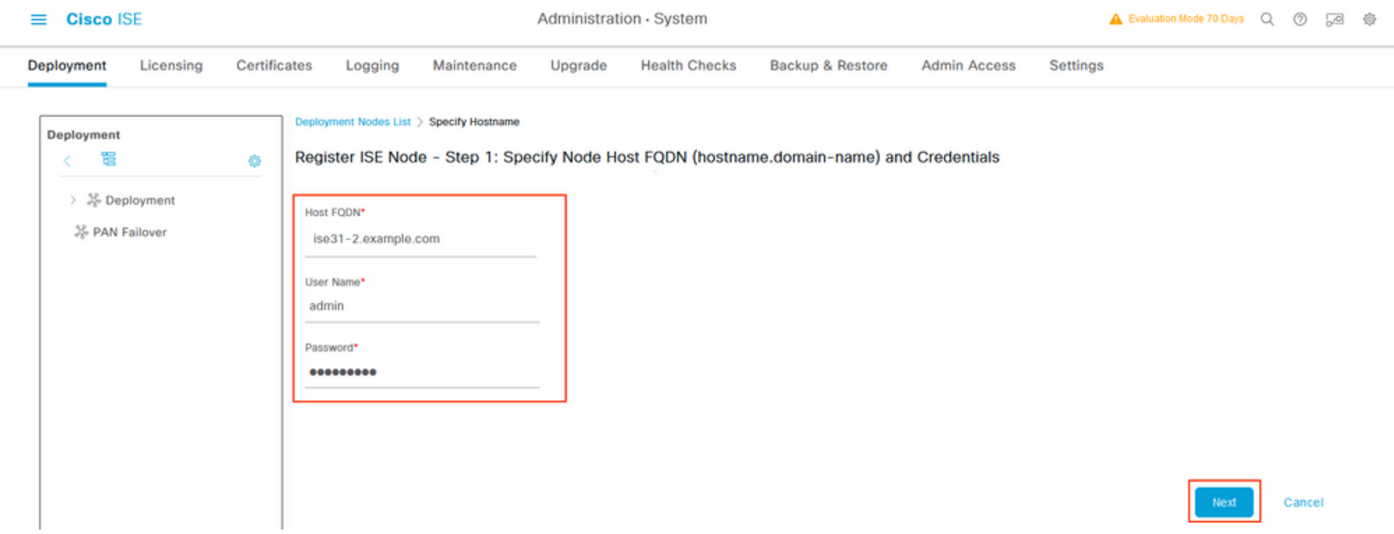
Once the **Application Server** is in **running State**, you can access ISE via GUI as shown in the image.



© 2021 Cisco Systems,Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems,Inc. and/or its affiliates in the U.S and certain other countries. Cisco ISE utilizes open source software from various components. View third-party licenses and notices

Step 6. Configure Distributed Deployment between On-Prem ISE and ISE on AWS

Log in to On-Prem ISE and navigate to **Administration > System > Deployment.** Select the node and Select **Make Primary.** Navigate back to **Administration > System > Deployment**, Select **Register**. Configure **Host FQDN** of ISE on AWS, GUI **Username** and **Password.** Click **Next.**



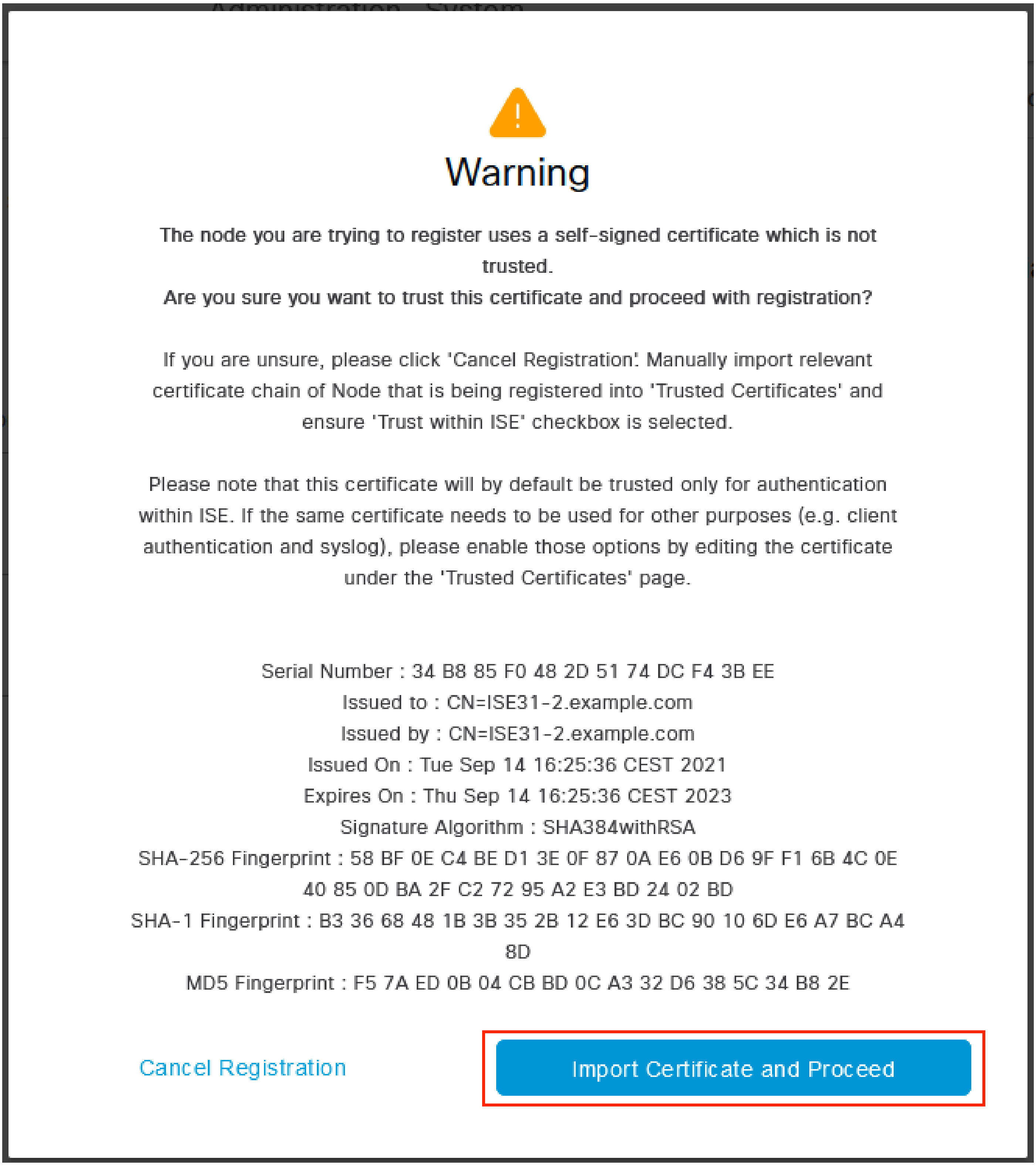
Register ISE Node - Step 1: Specify Node Host FQDN (hostname.domain-name) and Credentials

Host FQDN*: ise31-2.example.com

User Name*: admin

Password*: ●●●●●●●●●

Since Self-signed certificates are used in this topology, to cross import admin certificates to the Trusted Store Select **Import Certificate and Proceed.**



Warning

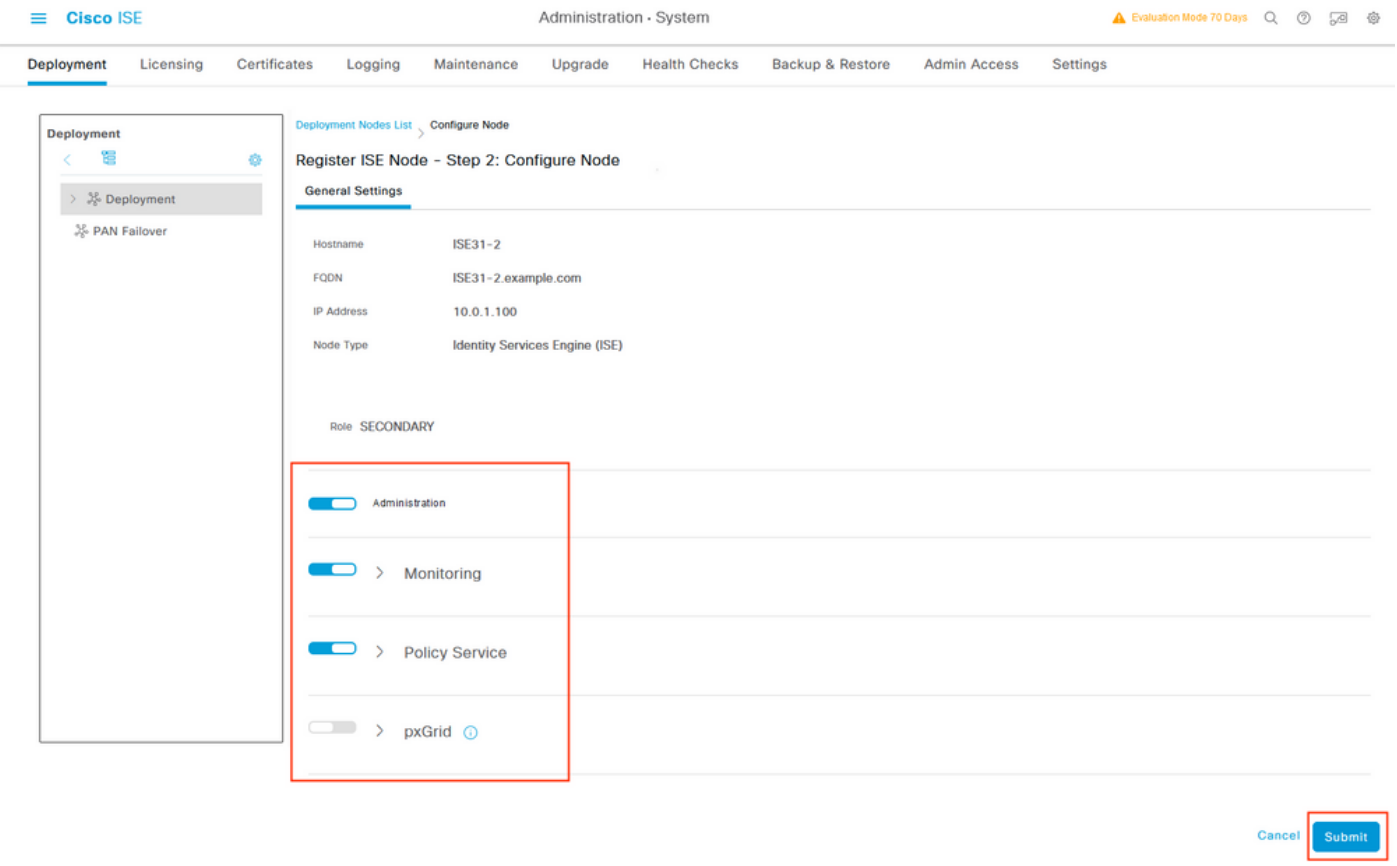
The node you are trying to register uses a self-signed certificate which is not trusted.
Are you sure you want to trust this certificate and proceed with registration?

If you are unsure, please click 'Cancel Registration'. Manually import relevant certificate chain of Node that is being registered into 'Trusted Certificates' and ensure 'Trust within ISE' checkbox is selected.

Please note that this certificate will by default be trusted only for authentication within ISE. If the same certificate needs to be used for other purposes (e.g. client authentication and syslog), please enable those options by editing the certificate under the 'Trusted Certificates' page.

Serial Number : 34 B8 85 F0 48 2D 51 74 DC F4 3B EE
Issued to : CN=ISE31-2.example.com
Issued by : CN=ISE31-2.example.com
Issued On : Tue Sep 14 16:25:36 CEST 2021
Expires On : Thu Sep 14 16:25:36 CEST 2023
Signature Algorithm : SHA384withRSA
SHA-256 Fingerprint : 58 BF 0E C4 BE D1 3E 0F 87 0A E6 0B D6 9F F1 6B 4C 0E 40 85 0D BA 2F C2 72 95 A2 E3 BD 24 02 BD
SHA-1 Fingerprint : B3 36 68 48 1B 3B 35 2B 12 E6 3D BC 90 10 6D E6 A7 BC A4 8D
MD5 Fingerprint : F5 7A ED 0B 04 CB BD 0C A3 32 D6 38 5C 34 B8 2E

Select the Personas of your choice and click **Submit**.



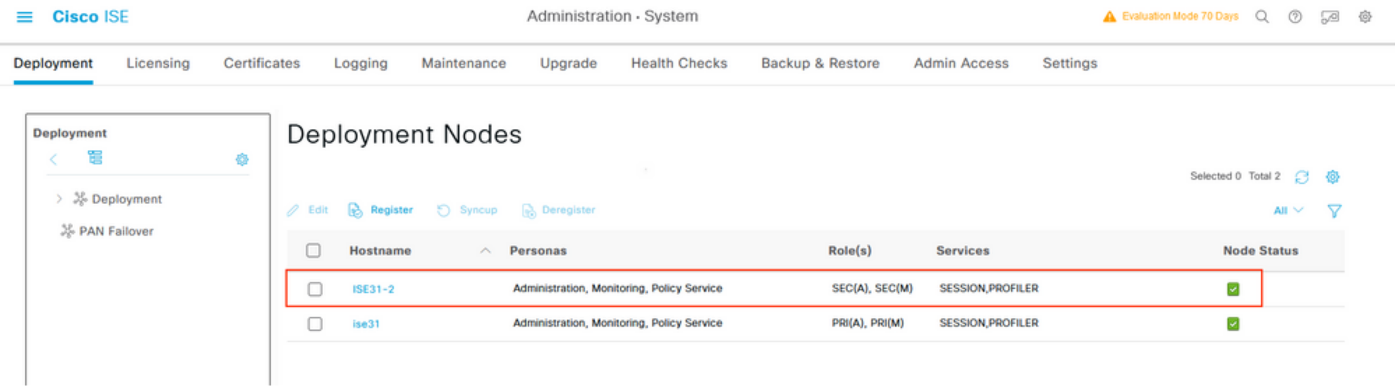
Register ISE Node - Step 2: Configure Node

Hostname	ISE31-2
FQDN	ISE31-2.example.com
IP Address	10.0.1.100
Node Type	Identity Services Engine (ISE)

Role SECONDARY

- Administration: on
- Monitoring: on
- Policy Service: on
- pxGrid: off

Once the synchronization completes, the node transitions to the connected state, the green checkbox is displayed against it.



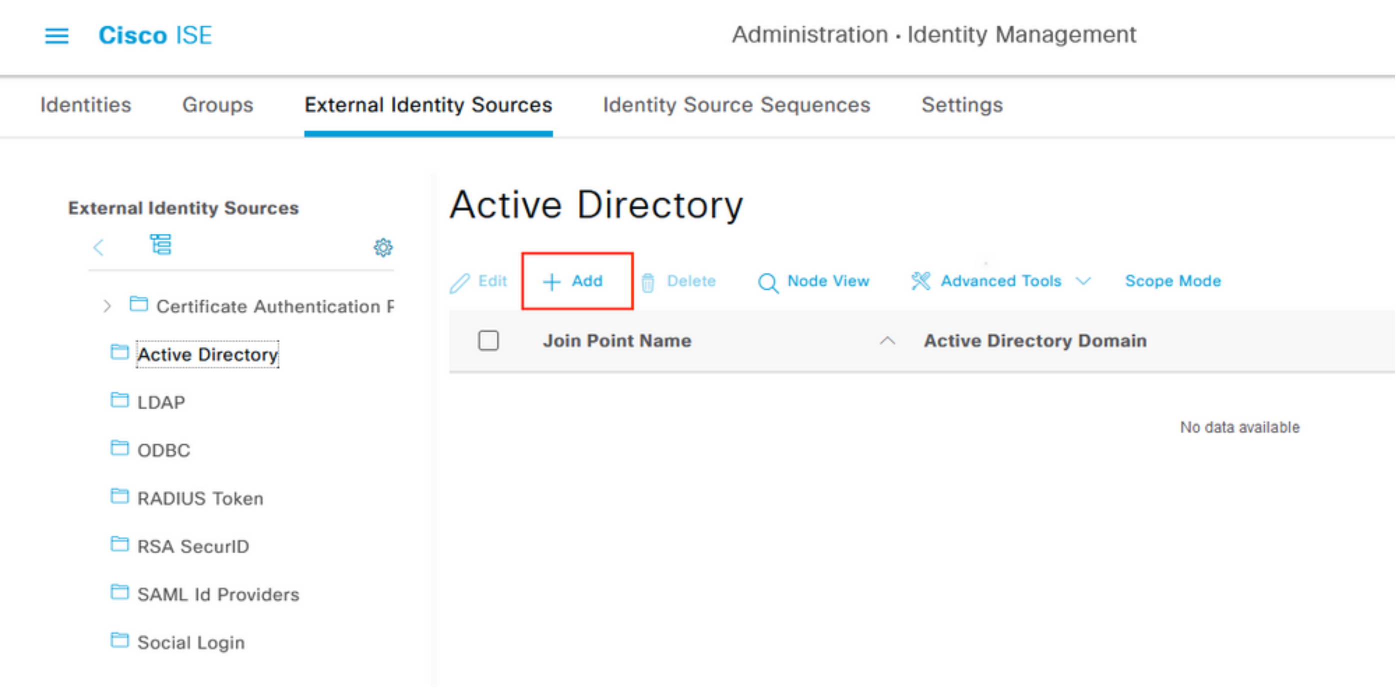
Deployment Nodes

Selected 0 Total 2

□	Hostname	Personas	Role(s)	Services	Node Status
□	ISE31-2	Administration, Monitoring, Policy Service	SEC(A), SEC(M)	SESSION,PROFILER	✓
□	ise31	Administration, Monitoring, Policy Service	PRI(A), PRI(M)	SESSION,PROFILER	✓

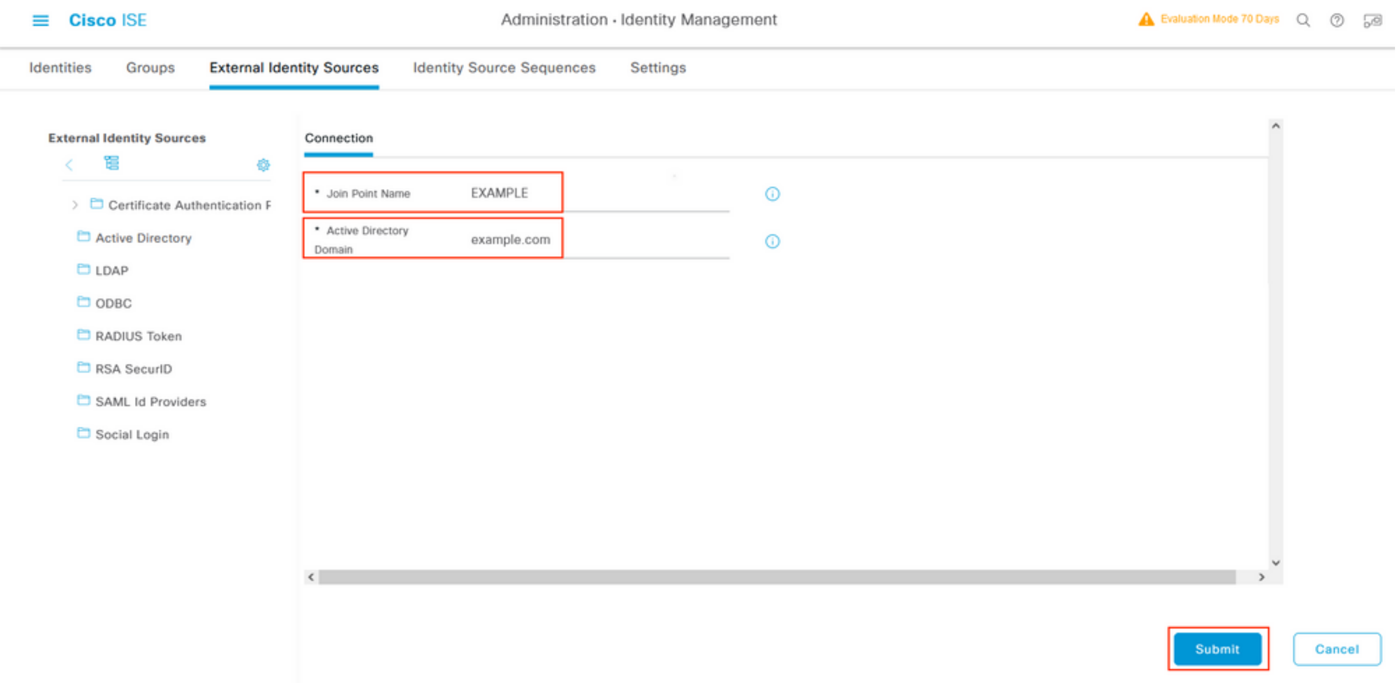
Step 7. Integrate ISE Deployment with On-Prem AD

Navigate to **Administration > Identity Management > External Identity Sources**. Select **Active Directory**, Select **Add**.



No data available

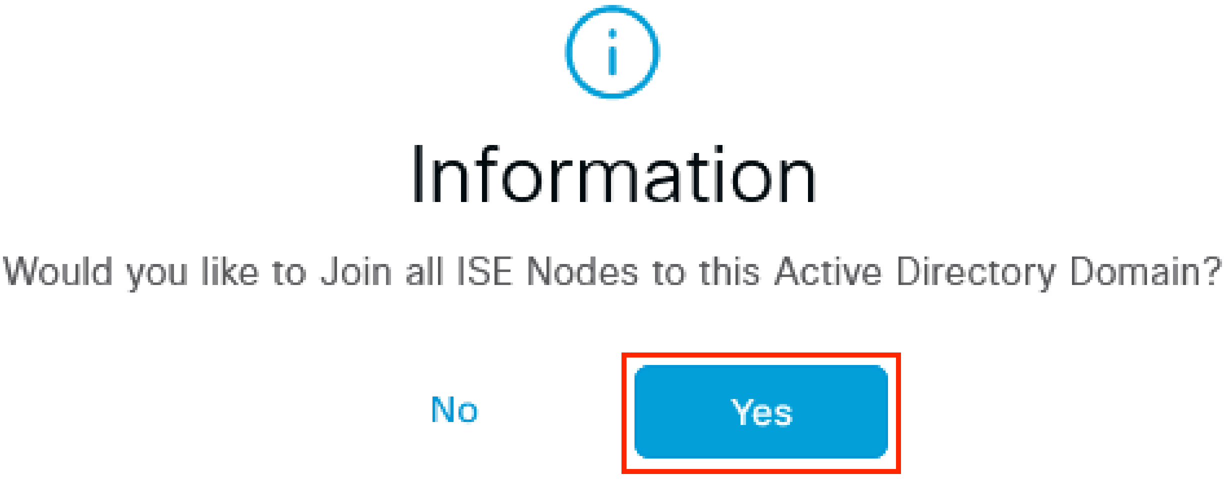
Configure **Joint Point Name** and **Active Directory Domain**, Select **Submit**.



* Join Point Name EXAMPLE

* Active Directory Domain example.com

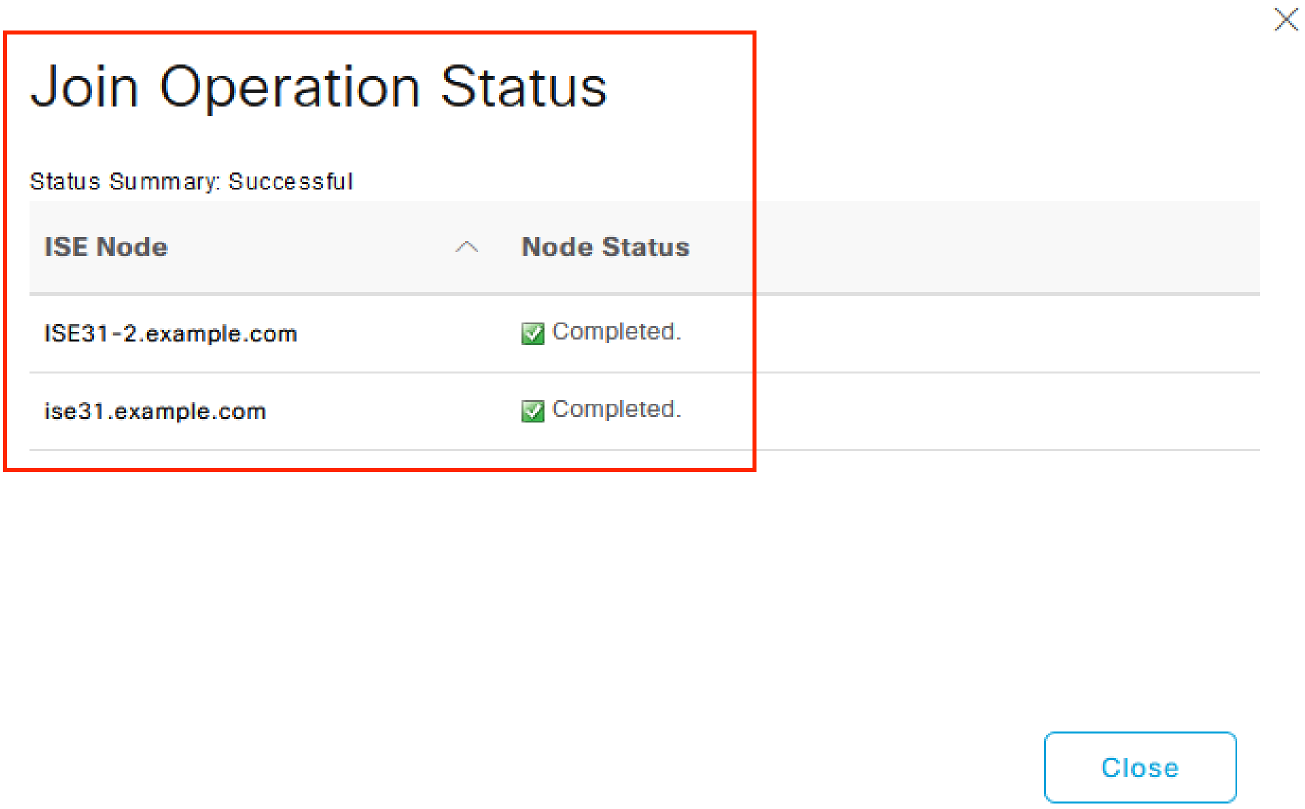
To integrate both nodes with Active Directory Select **Yes**.



Information

Would you like to Join all ISE Nodes to this Active Directory Domain?

Enter **AD User Name** and **Password**, click **OK**. Once the ISE Nodes are successfully integrated with Active Directory, Node Status changes to Completed.



Join Operation Status

Status Summary: Successful

ISE Node	Node Status
ISE31-2.example.com	✓ Completed.
ise31.example.com	✓ Completed.

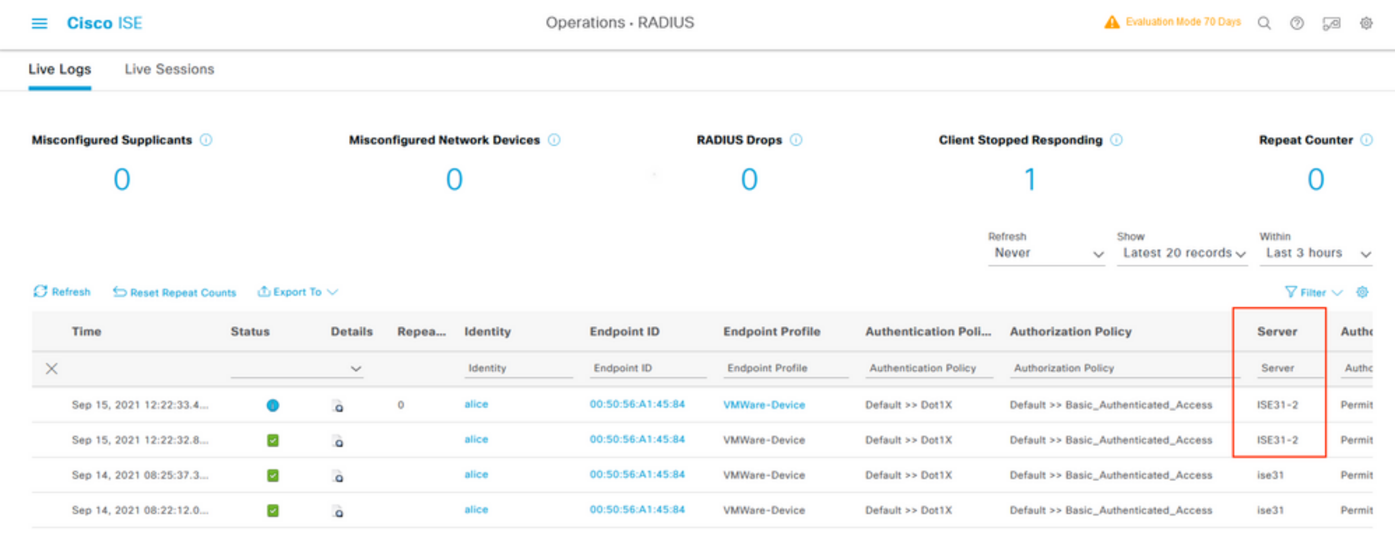
Limitations

For ISE on AWS limitations please refer to the Known Limitations section of the ISE Admin Guide.

Verify

Use this section in order to confirm that your configuration works properly.

In order to verify authentication is performed on the ISE PSN located on AWS, navigate to **Operations > Radius > Live Logs**, and confirm in the **Server** column ISE on AWS PSN is observed.



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	1	0

Refresh: Never
Show: Latest 20 records
Within: Last 3 hours

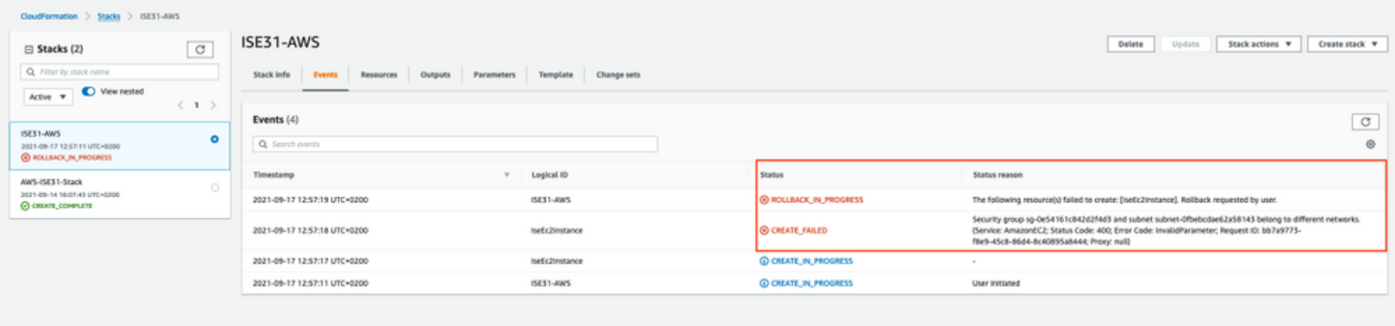
Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Profile	Authentication Poli...	Authorization Policy	Server	Authc
Sep 15, 2021 12:22:33.4...	●		0	alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ISE31-2	Permit
Sep 15, 2021 12:22:32.8...	✓			alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ISE31-2	Permit
Sep 14, 2021 08:25:37.3...	✓			alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ise31	Permit
Sep 14, 2021 08:22:12.0...	✓			alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ise31	Permit

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

CloudFormation Stack Creation Failed

CloudFormation Stack Creation can fail due to multiple reasons, one of them is when you select that Security Group from the VPN which is different from the Management network of ISE. The Error looks like the one in the image.



Timestamp	Logical ID	Status	Status reason
2021-09-17 12:57:19 UTC+0200	ISE31-AWS	ROLLBACK_IN_PROGRESS	The following resource(s) failed to create: [IseEc2Instance]. Rollback requested by user.
2021-09-17 12:57:18 UTC+0200	IseEc2Instance	CREATE_FAILED	Security group sg-0e54161c842d2f4d3 and subnet subnet-0fbebcdae62a58143 belong to different networks. (Service: AmazonEC2; Status Code: 400; Error Code: InvalidParameter; Request ID: bb7a9773-f8e9-45c8-86d4-8c40895a8444; Proxy: null)
2021-09-17 12:57:17 UTC+0200	IseEc2Instance	CREATE_IN_PROGRESS	-
2021-09-17 12:57:11 UTC+0200	ISE31-AWS	CREATE_IN_PROGRESS	User initiated

Solution:

Ensure to pick up the Security Group from the Same VPC. Navigate to **Security Groups** under **VPC** Service, and note the **Security Group ID**, ensure it corresponds to the right VPC (where ISE resides), verify **VPC ID**.

Connectivity issues

There can be multiple issues that can cause connectivity to ISE on AWS not to work.

1. Connectivity issue due to misconfigured **Security Groups.**

Solution: ISE can be not reachable from the On-Prem network or even within AWS networks if **Security Groups** are misconfigured. Ensure that the required protocols and ports are allowed in the **Security Group** associated with the ISE network. Refer to ISE Ports Reference for Required ports to be opened.

2. Connectivity issues due to misconfigured Routing.

Solution: Due to the complexity of the topology, it is easy to miss some routes between the On-Prem network and AWS. Before you can use ISE features, ensure end-to-end connectivity is in place.

Appendix

Switch AAA/Radius Related Configuration

```
aaa new-model
!
!
aaa group server radius ISE-Group
server name ISE31-2
server name ISE31-1
!
aaa authentication dot1x default group ISE-Group
aaa authorization network default group ISE-Group
aaa accounting dot1x default start-stop group ISE-Group
!
aaa server radius dynamic-author
client 172.18.5.100 server-key cisco
client 10.0.1.100 server-key cisco
!
aaa session-id common
!
dot1x system-auth-control
!
vlan 1805
!
interface GigabitEthernet1/0/2
description VMWIN10
switchport access vlan 1805
switchport mode access
authentication host-mode multi-auth
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
mab
dot1x pae authenticator
!
interface Vlan1805
ip address 172.18.5.3 255.255.255.0
!
!
radius server ISE31-1
address ipv4 172.18.5.100 auth-port 1645 acct-port 1646
key cisco
!
radius server ISE31-2
address ipv4 10.0.1.100 auth-port 1645 acct-port 1646
key cisco
```