CV1000-AWS Deployment Guide

Using the New **AWS Launch Instance Wizard**

SENETAS
Security without compromise

THALES

Firmware	v5.6.x
CM7 Management System	v7.11.0

The technology described in this document has been developed by Senetas Corporation and is distributed and supported world-wide by Thales.

Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Information

Address	**Phone**	
Arboretum Plaza II 9442 Capital of Texas Highway North Suite 400 Austin Texas 78759 USA	United States	+1 615 523 5530
	China	+86 10 8851 9191
	France	0825 341000
	Germany	01803 7246269
	United Kingdom	0870 7529200
	Australia, New Zealand, India or any other location worldwide	+1 410 931 7520
Email	**Customer Support Portal**	
technical.support.dis@thalesgroup.com	https://supportportal.thalesgroup.com/csm	

***Notice**: Senetas documentation is produced in English and may be subject to translation for use in the other geographies where Senetas products are installed. Senetas does not accept responsibility for any translation errors. All documentation remains the intellectual property of Senetas Corporation, must not be copied without permission and it or any translation, must not be used to reverse engineer Senetas products. (**This statement is to remain in English.**)*

Abstract

The purpose of this document is to explain how to deploy the CV1000-AWS in the AWS public cloud to encrypt/decrypt network traffic using the new AWS Launch Instance Wizard.

Table of Contents

Revision 0.10 (05/08/24)

Version History

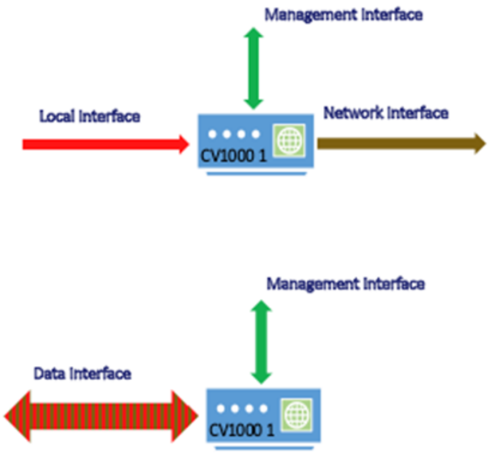
Revision	Author	Date	Description
0.0	RV	08-Apr-2020	Internal ETN that this guide is based on
0.1	BWS	03-Aug-2020	Initial release
0.2	BWS	26-Oct-2020	Update to explain AWS environment
0.3	BWS	24-Nov-2020	Complete revision of Instance creation
0.4	BWS	14-Nov-2021	Added CV1000-AWS-GWLB details
0.5	BWS	28-Apr-2023	Minor errors corrected
0.6	BWS	12-Feb-2024	Update to explain creating an Instance using the new AWS Launch Instance Wizard
0.7	BWS	13-May-2024	Removed RAW image use for AMI
0.8	RLT	22-Jun-2024	Restyled and new format
0.9	RLT	03-Jul-2024	Address details amended
0.10	NK	05-Aug-2024	Added SNMP over SSH details

Glossary of Terms

Term	Description
AMI	Amazon Machine Image
ARP	Address Resolution Protocol
AWS	Amazon Web Services
CLI	Command Line Interface
CM7	CypherManager 7
DPDK	Data Plane Development Kit
EC2	Elastic Cloud Compute
ETN	Engineering Technical Note
GENEVE	Generic Network Virtualisation Encapsulation
GWLB	Gateway Load Balancer
IAM	Identity and Access Management
JSON	JavaScript Object Notation
MAC	Media Access Control
NTP	Network Time Protocol
S3	Secure Storage Service
TIM	Transport Independent Mode
VNET	Virtual Network
VPC	Virtual Private Cloud

1 Introduction

There are two product variants of the CV1000 encryptor supported on AWS, the CV1000-AWS and CV1000-AWS-GWLB. The key differences between the two variants are shown in the figures below.



CV1000-AWS

- Three interfaces
- Cleartext ingress on **Local** interface Cyphertext ingress on **Network** Interface
- L3/L4 Encryption

CV1000-AWS-GWLB

- Two interfaces
- Cleartext/Cyphertext ingress/egress on **Data** interface
- Supports GENEVE encapsulation
- Responds to AWS GWLB health checks
- L3/L4 encryption

Figure 1 – CV1000 for AWS Variants

[Note: Details of Generic Network Virtualization Encapsulation (GENEVE) can be found here.]

This document covers the CV1000-AWS variant used in the AWS infrastructure. The purpose of this document is to explain how to create a CV1000-AWS Instance variant, deploy it in the AWS public cloud infrastructure and integrate it inline.

There are three different ways of creating a CV1000-AWS Instance for deployment:

- Using the old AWS Launch Instance Wizard, available in the AWS GovCloud (US) Region and AWS China Regions. The old wizard has a multi-page layout.
- Using the new AWS Launch Instance Wizard, available in all AWS Regions except AWS GovCloud (US) Region and AWS China Regions. The new wizard has a single-page layout with a summary side panel.
- Using the AWS CloudFormation Template for CV1000-AWS. The template has a single-page layout and creates most of the resources needed by an AMI to create an AWS Instance.

This document explains how to create a CV1000-AWS Instance from the CV1000-AWS AMI using the **new AWS Launch Wizard**. The CV1000-AWS AMI should eventually be available in the AWS Marketplace. CV1000-AWS is also available as a RAW image but its use is not covered in this document.

2 CV1000-AWS Technical Overview

This section describes some of the high-level changes present in the CV1000-AWS variant compared to the standard (non-cloud) CV1000-DPDK version.

2.1 CV1000-AWS Build Changes

AWS-related build changes from the CV1000-DPDK version are straightforward. They include the addition of AWS-specific networking drivers in DPDK, as well as the Linux kernel. The AWS-specific build ships as an AMI. It is also available as a raw format disk image file but this is not covered in this document.

2.2 CV1000-AWS Networking Changes

One major difference for this variant, compared to the existing CV1000 virtual encryptor, is that this variant doesn't operate as a traditional "bump-in-the-wire" encryptor deployment model. As the AWS infrastructure works with only Layer 3 network protocols, the Layer 2 model of encryption doesn't apply here. This also mandates the use of TIM (Layer 3 and Layer 4 encryption) in this product variant.

For the CV1000 encryptor to work with data being routed to and from an encryptor in the AWS cloud environment, this requires the networking to be setup in a specific manner. All packets exiting an encryptor need to be sent to the AWS gateway for that particular subnet. The gateway takes care of switching the frame to the right endpoint.

However, in AWS, the gateway doesn't have a fixed MAC address for each subnet. Therefore, the Local and Network adapters on an encryptor need to **arp** their respective gateway IP addresses. Once each **arp** is resolved, only then are these devices bound to the DPDK daemon, which then uses the resolved MAC address for each subnet's gateway for frames exiting that particular interface.

3 AWS Prerequisites

As a pre-requisite, an AWS subscription is required with a VPC with different subnets created for deploying the CV1000 VM. AWS has lot of documentation that can help in getting started with setting up a VPC with public and private subnets.

4 Obtain CV1000 AMI

An **Amazon Machine Image** (AMI) is a special type of virtual appliance that is used to create a virtual machine within the Amazon Elastic Compute Cloud (EC2). An AMI serves as the basic unit of deployment for services delivered using EC2. It is a template that contains such characteristics as the operating system, architecture (32-bit or 64-bit) and launch permissions. It does not contain resource information such as CPUs, RAM and Network Adapters.

Different types of AMIs are available, such as Public, Paid-For, Shared and Custom. To use CV1000 in an AWS EC2 environment, a CV1000 Instance needs to be created from an AMI.

To create a CV1000 for AWS Instance, the following high-level steps are required:

- Copy a CV1000 AMI from either the **AWS Marketplace** or from a **Shared AMI**.
- The new AMI should be listed in the **Images -> AMIs** section of the AWS **EC2 Dashboard**.
- Use the CV1000 AMI to create as many CV1000 AWS Instances as required.

The diagram below shows the high-level CV1000 Instance creation process.

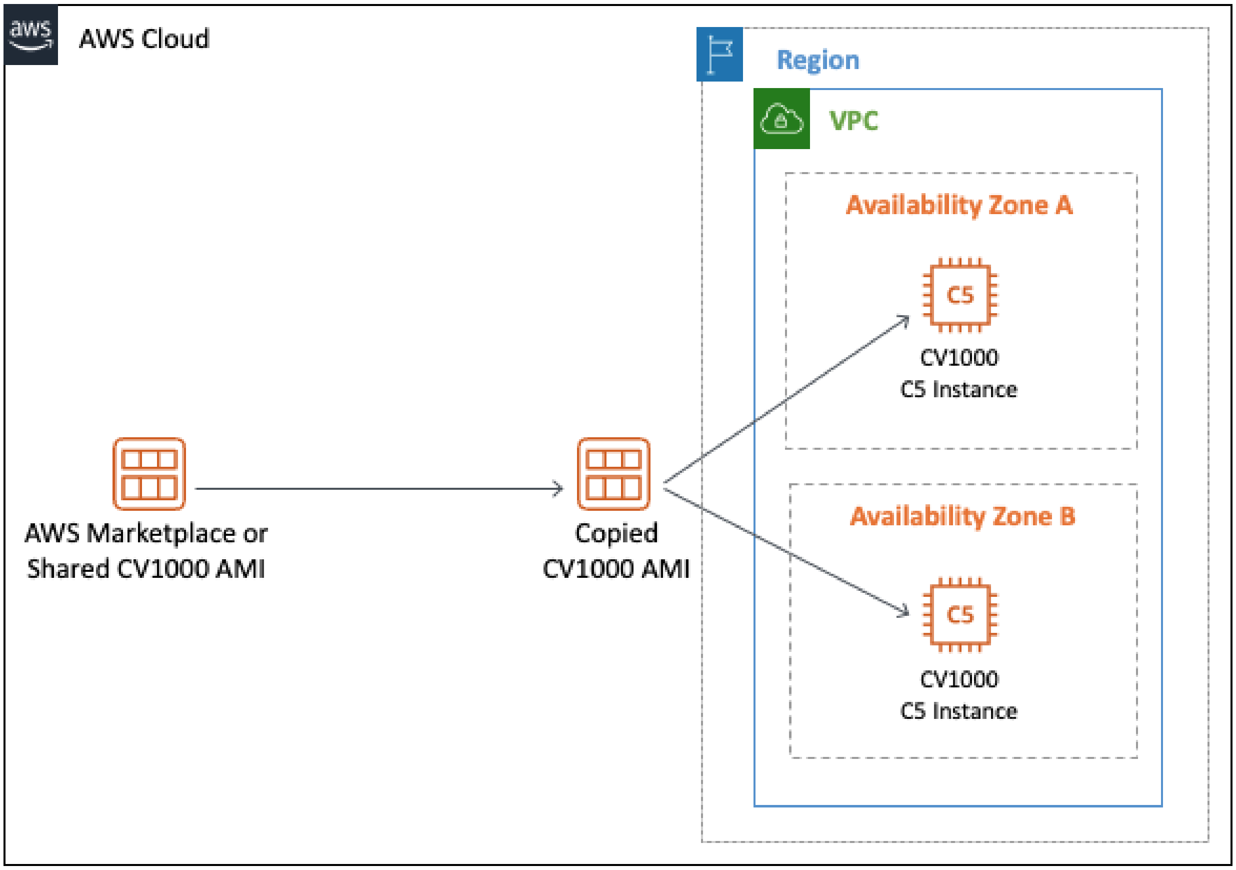
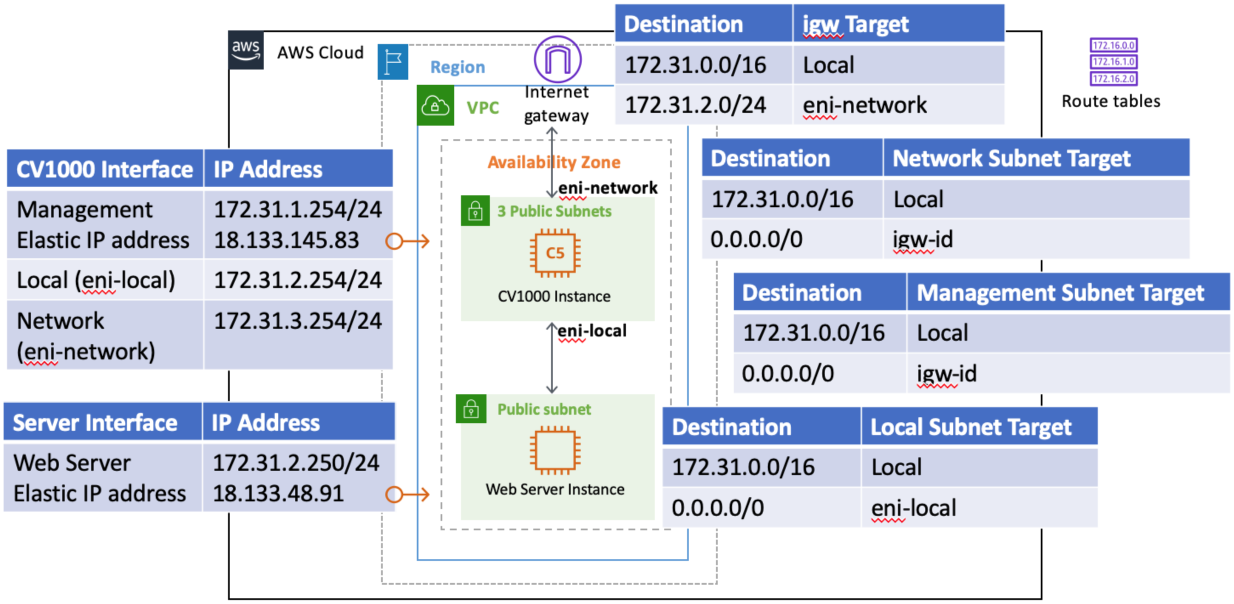


Figure 2 – CV1000 Instance Creation Process

5 Configure VPC Network for CV1000 Instance

Prior to creating a CV1000 Instance, various VPC network environment components need to be created and configured. The instructions below are based on an inline CV1000 being used to protect a Web server listening on TCP port 80. It is assumed that this Web server is being accessed from hosts at remote sites and via other encryptors.



Destination	igw Target
172.31.0.0/16	Local
172.31.2.0/24	eni-network

CV1000 Interface	IP Address
Management Elastic IP address	172.31.1.254/24 18.133.145.83
Local (eni-local)	172.31.2.254/24
Network (eni-network)	172.31.3.254/24

Destination	Network Subnet Target
172.31.0.0/16	Local
0.0.0.0/0	igw-id

Destination	Management Subnet Target
172.31.0.0/16	Local
0.0.0.0/0	igw-id

Server Interface	IP Address
Web Server Elastic IP address	172.31.2.250/24 18.133.48.91

Destination	Local Subnet Target
172.31.0.0/16	Local
0.0.0.0/0	eni-local

Figure 3 – Inline CV1000 Protecting a Web Server

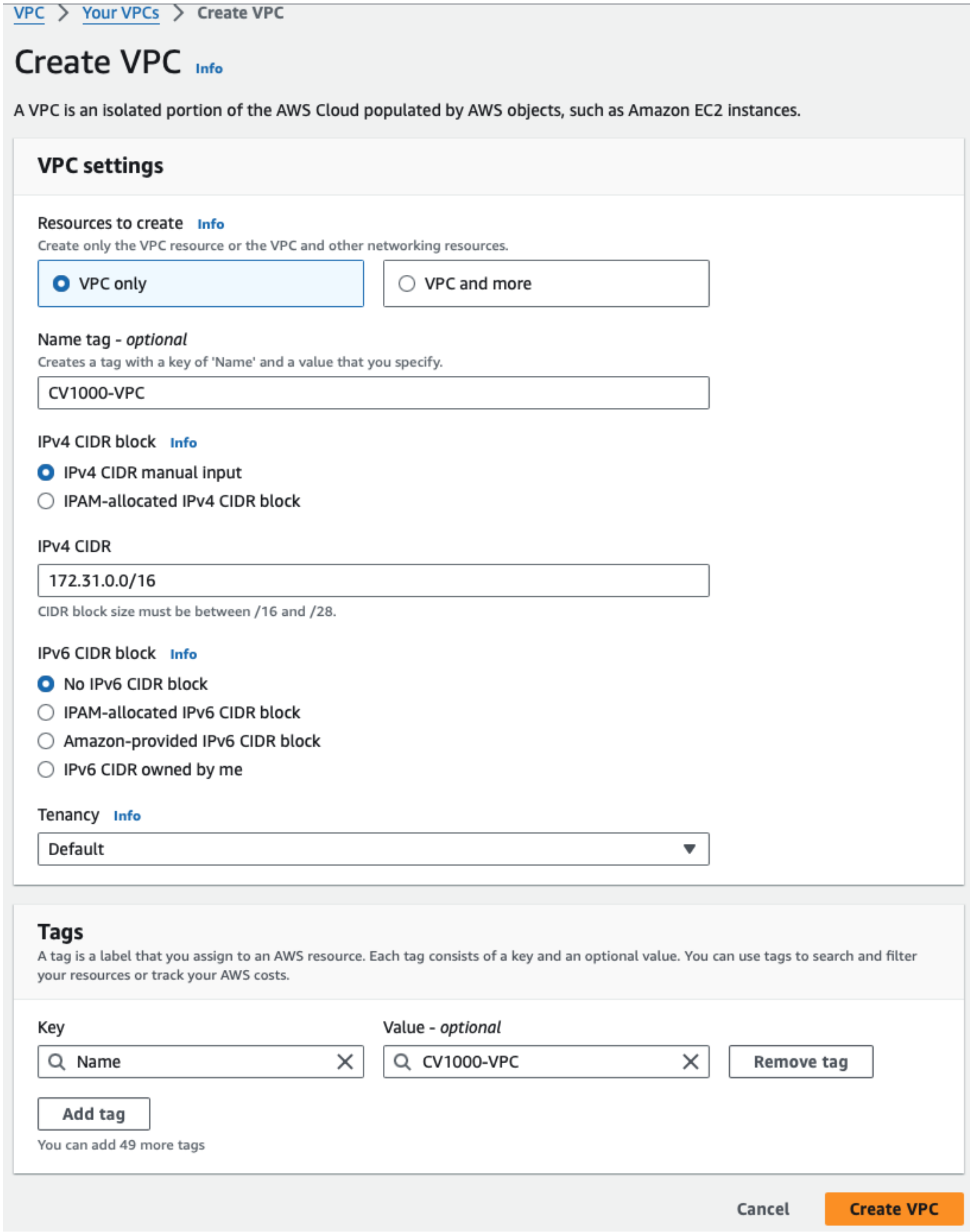
5.1 Create a VPC

If a VPC doesn’t already exist or a new one needs to be created, then create one. From the AWS Web console, in the **Your VPCs** section, click on **Create a VPC**:

- **VPC** > **Create VPC**

The screenshot below shows the creation of a VPC.

The **Name** and **IPv4 CIDR** fields (e.g., 172.31.0.0/16) need to be entered.



VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.

● VPC only ○ VPC and more

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
CV1000-VPC

IPv4 CIDR block Info
● IPv4 CIDR manual input
○ IPAM-allocated IPv4 CIDR block

IPv4 CIDR
172.31.0.0/16
CIDR block size must be between /16 and /28.

IPv6 CIDR block Info
● No IPv6 CIDR block
○ IPAM-allocated IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block
○ IPv6 CIDR owned by me

Tenancy Info
Default

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

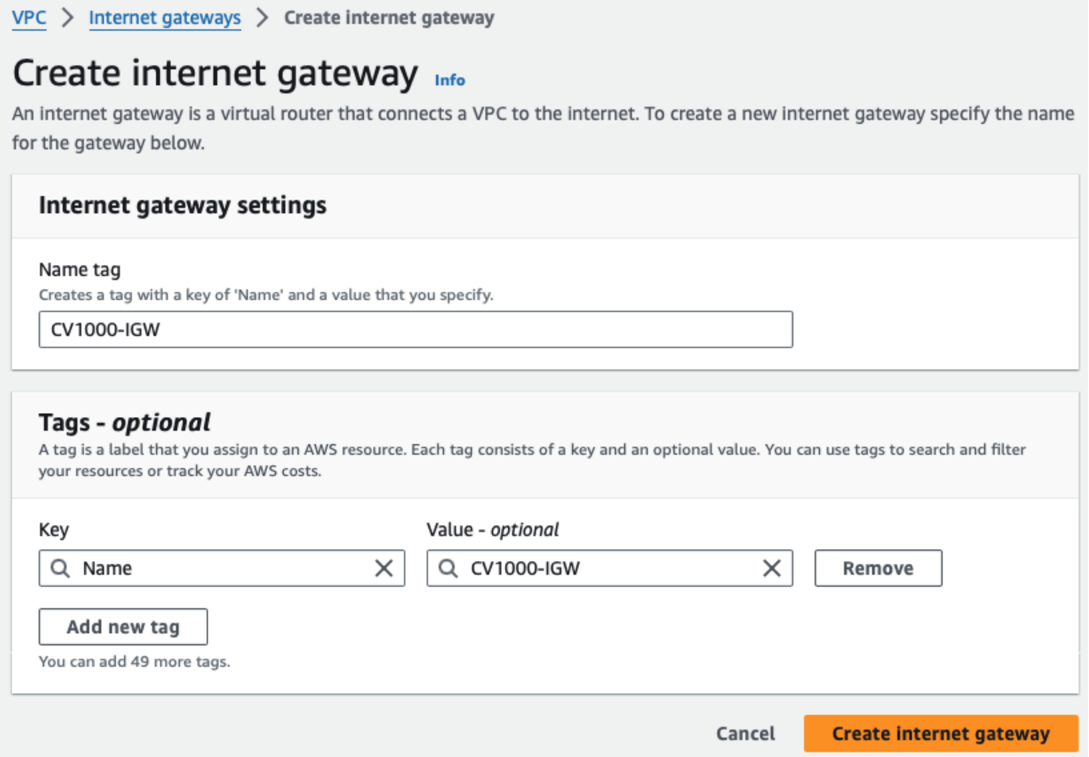
Key	Value - *optional*	
Name	CV1000-VPC	Remove tag

Add tag
You can add 49 more tags

5.2 Create and Attach an Internet Gateway to a VPC

From the AWS Web console, go to the VPC section, create an Internet gateway and then attach it to a VPC.

1. **Create an Internet Gateway**
   - In the AWS console, under **VPC > Internet gateways and** click on the **Create Internet gateway** button. This will bring up the screen below.



VPC > Internet gateways > Create internet gateway

Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.
CV1000-IGW

Tags - *optional*
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*	
Name	CV1000-IGW	Remove

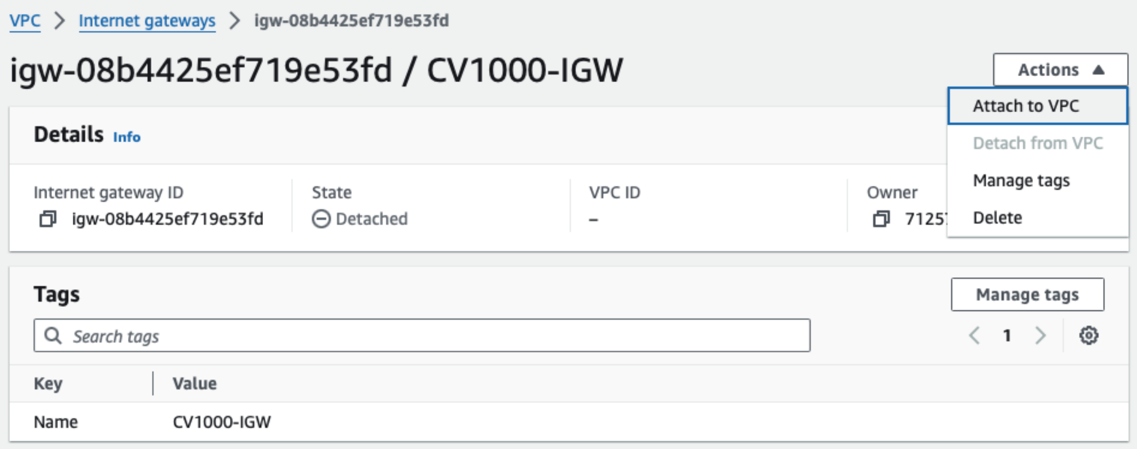
Add new tag
You can add 49 more tags.

Cancel | Create internet gateway

- ○ Enter a suitable **Name tag** and click on **Create Internet gateway**.

2. Attach to a VPC

- ○ The screen below will then appear. Click the **Actions > Attach to VPC** drop-down menu option.



VPC > Internet gateways > igw-08b4425ef719e53fd

igw-08b4425ef719e53fd / CV1000-IGW

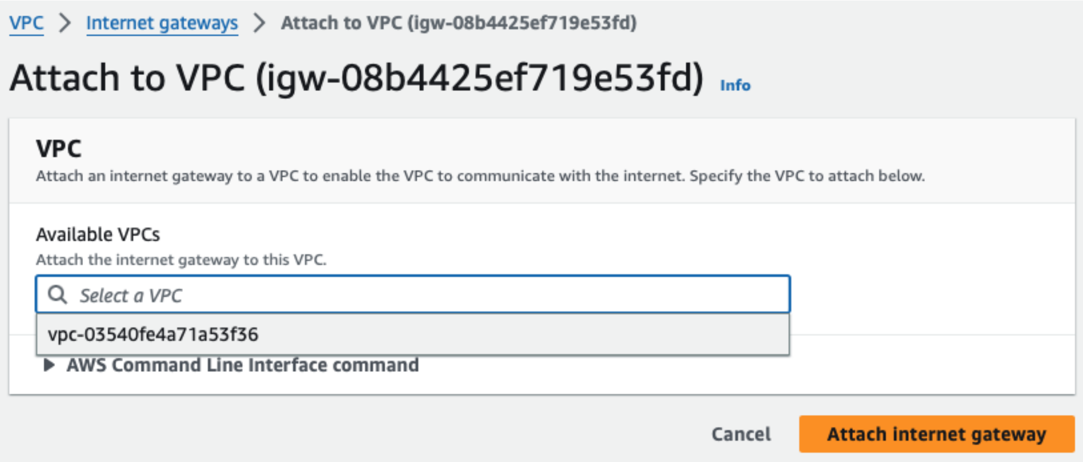
Details Info

Internet gateway ID	State	VPC ID	Owner
igw-08b4425ef719e53fd	Detached	–	7125

Tags

Key	Value
Name	CV1000-IGW

- ○ The screen below will then appear. Select the VPC to attach the Internet gateway to and click on the **Attach Internet gateway** button.



VPC > Internet gateways > Attach to VPC (igw-08b4425ef719e53fd)

Attach to VPC (igw-08b4425ef719e53fd) Info

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

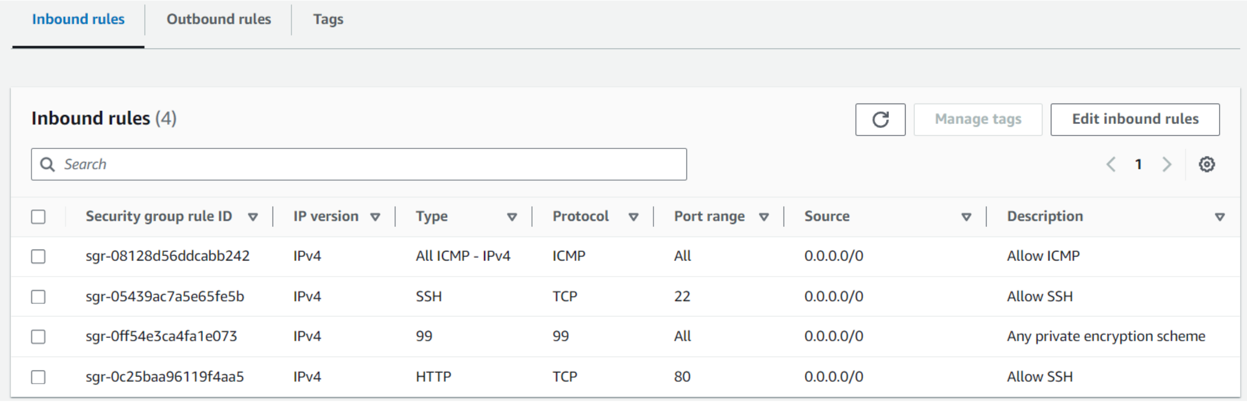
Select a VPC

vpc-03540fe4a71a53f36

▶ AWS Command Line Interface command

5.3 Create a Security Group

Security Groups are assigned to Instances and Network Interfaces. It’s possible to create and use separate Security Groups but a single Security Group or the default Security Group, as shown below, is sufficient in most cases. Limit the **Source** to known IP address if possible.



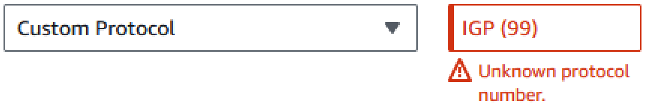
Inbound rules (4)

□	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
□	sgr-08128d56ddcabb242	IPv4	All ICMP - IPv4	ICMP	All	0.0.0.0/0	Allow ICMP
□	sgr-05439ac7a5e65fe5b	IPv4	SSH	TCP	22	0.0.0.0/0	Allow SSH
□	sgr-0ff54e3ca4fa1e073	IPv4	99	99	All	0.0.0.0/0	Any private encryption scheme
□	sgr-0c25baa96119f4aa5	IPv4	HTTP	TCP	80	0.0.0.0/0	Allow SSH

By default, everything inbound is implicitly denied. The above rules are used as follows:

- TCP/80 – allows HTTP access (e.g., for a Web server instance)
- 99/All* – allows Layer 3 encrypted traffic (e.g., ICMP/ping in encrypted mode)
- TCP/22 – allows SSH access for remote CLI access & for SNMP over SSH
- ICMP/All – allows ping testing in bypass mode

[Note *: There appears to be a bug in the AWS web GUI when trying to enter protocol 99. It changes 99 to IGP (99) and displays the error message Unknown protocol number.

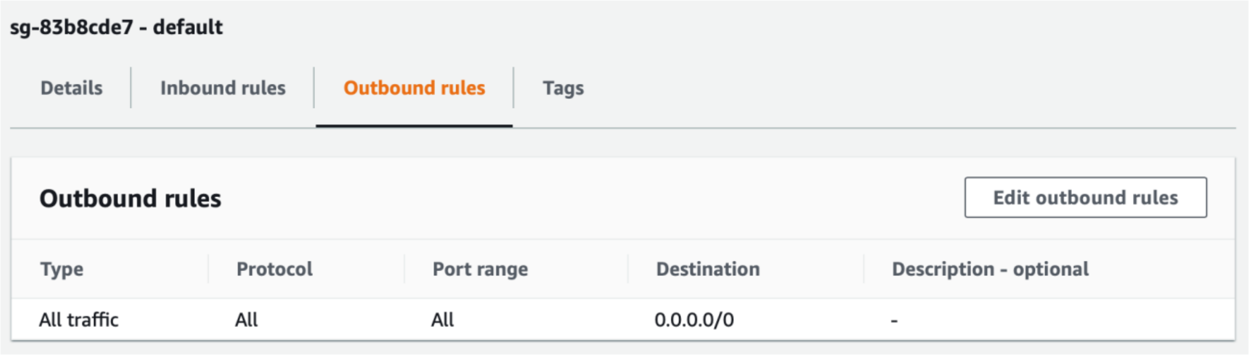


Custom Protocol

IGP (99)

Unknown protocol number.

To resolve this problem, edit this field and remove IGP and the braces.]



sg-83b8cde7 - default

Outbound rules

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	0.0.0.0/0	-

By default, a security group includes an outbound rule that allows all outbound traffic. We recommend removing this default rule and adding outbound rules that allow specific outbound traffic only (e.g., to specific destinations).

5.4 Create CV1000 Network Subnets

From the AWS Web console, create three subnets that will be assigned to the **Management**, **Local** and **Network** interfaces:

- **VPC** > **Subnets** > **Create subnet**

For example, for a VPC with an IPv4 CIDR of 172.31.0.0/16, the following subnets could be created:

- 172.31.1.0/24 – **Management** subnet
- 172.31.2.0/24 – **Local** subnet (the unencrypted application subnet)
- 172.31.3.0/24 – **Network** subnet (the encrypted subnet)

These subnets should be in the same VPC and Availability Zone that the CV1000 for AWS instance will reside in.

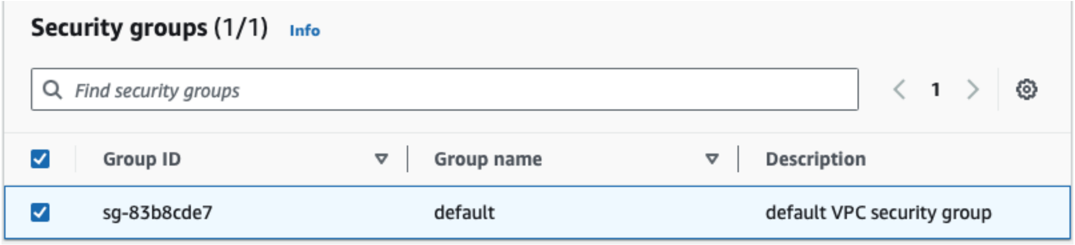
5.5 Create CV1000 Network Interfaces

Create the required interfaces that will be used for the **Management**, **Local** and **Network** ports of the CV1000 VM (they will be assigned to the encryptor at a later stage):

1. Go to the **Network Interfaces** section of EC2 service in the AWS Web console and create three network interfaces for the respective subnets of the CV1000 encryptor.

   The recommended practice is to assign separate subnets to the three interfaces:
   - **Management** – a subnet that will eventually be assigned to **eth0**
   - **Local** – a subnet that will eventually be assigned to **eth1** (contains protected resources, e.g., a Web server)
   - **Network** – a subnet that will eventually be assigned to **eth2**

In the **Create network interface** screen, once a **Subnet** has been assigned to the network interface, a **Security groups** section will appear. Assign appropriate security groups for that interface and subnet. The default security group can be used if desired.

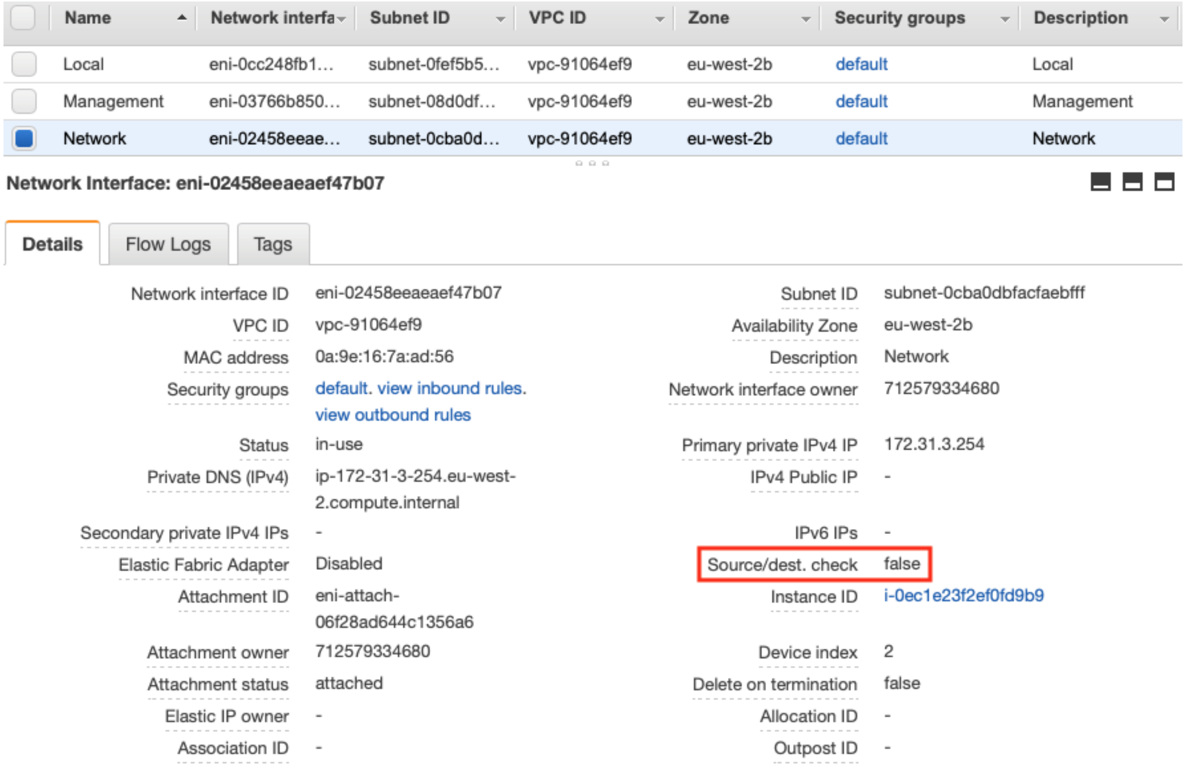


Security groups (1/1) Info

Find security groups

☑	Group ID	Group name	Description
☑	sg-83b8cde7	default	default VPC security group

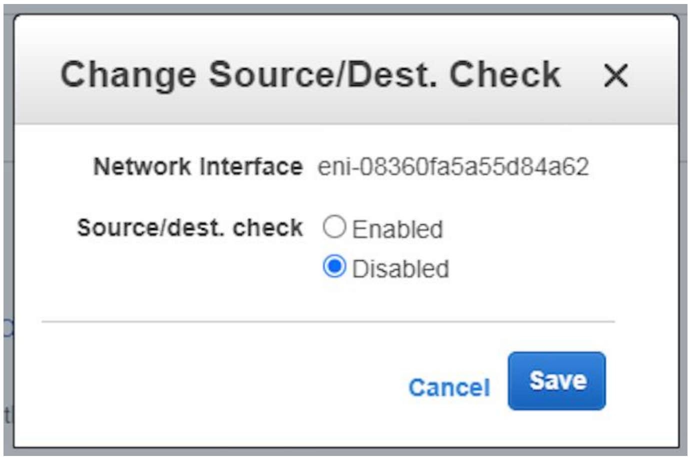
For the **Local** and **Network** interfaces, Disable the **Source/Dest** check. This is required to allow routing to/from the encryptor's interfaces to work.



□	Name	Network interfa	Subnet ID	VPC ID	Zone	Security groups	Description
□	Local	eni-0cc248fb1…	subnet-0fef5b5…	vpc-91064ef9	eu-west-2b	default	Local
□	Management	eni-03766b850…	subnet-08d0df…	vpc-91064ef9	eu-west-2b	default	Management
■	Network	eni-02458eeae…	subnet-0cba0d…	vpc-91064ef9	eu-west-2b	default	Network

Network Interface: eni-02458eeaeaef47b07

Network interface ID	eni-02458eeaeaef47b07	Subnet ID	subnet-0cba0dbfacfaebfff
VPC ID	vpc-91064ef9	Availability Zone	eu-west-2b
MAC address	0a:9e:16:7a:ad:56	Description	Network
Security groups	default. view inbound rules. view outbound rules	Network interface owner	712579334680
Status	in-use	Primary private IPv4 IP	172.31.3.254
Private DNS (IPv4)	ip-172-31-3-254.eu-west-2.compute.internal	IPv4 Public IP	-
Secondary private IPv4 IPs	-	IPv6 IPs	-
Elastic Fabric Adapter	Disabled	Source/dest. check	false
Attachment ID	eni-attach-06f28ad644c1356a6	Instance ID	i-0ec1e23f2ef0fd9b9
Attachment owner	712579334680	Device index	2
Attachment status	attached	Delete on termination	false
Elastic IP owner	-	Allocation ID	-
Association ID	-	Outpost ID	-



Change Source/Dest. Check

Network Interface eni-08360fa5a55d84a62

Source/dest. check ○ Enabled ● Disabled

2. From the AWS Web console, **Allocate Elastic IP address** and then **Associate** it with the **Management** interface:
   - **EC2** > **Elastic IPs** > **Allocate Elastic IP address**
   - **EC2** > **Elastic IPs** > **Actions** > **Associate Elastic IP address**

   This Elastic IP address is a public-facing IP address that has a 1-1 mapping to the internal IP address of the Management interface. The protected resources in the Local subnet may also require an Elastic IP address (e.g., a Web server).

5.6 Create Route Tables

From the AWS Web console, create route tables for the Management subnet, Local subnet, Network subnet and the Internet Gateway:

- **VPC** > **Route Tables** > **Create route table**

A **Route** and **Subnet Association** needs to be created for the Management, Local and Network subnets. A **Route** and **Edge Association** needs to be created for the Internet Gateway.

Using the following example subnets

- 172.31.1.0/24 – **Management** subnet
- 172.31.2.0/24 – **Local** subnet
- 172.31.3.0/24 – **Network** subnet (containing a Web server)

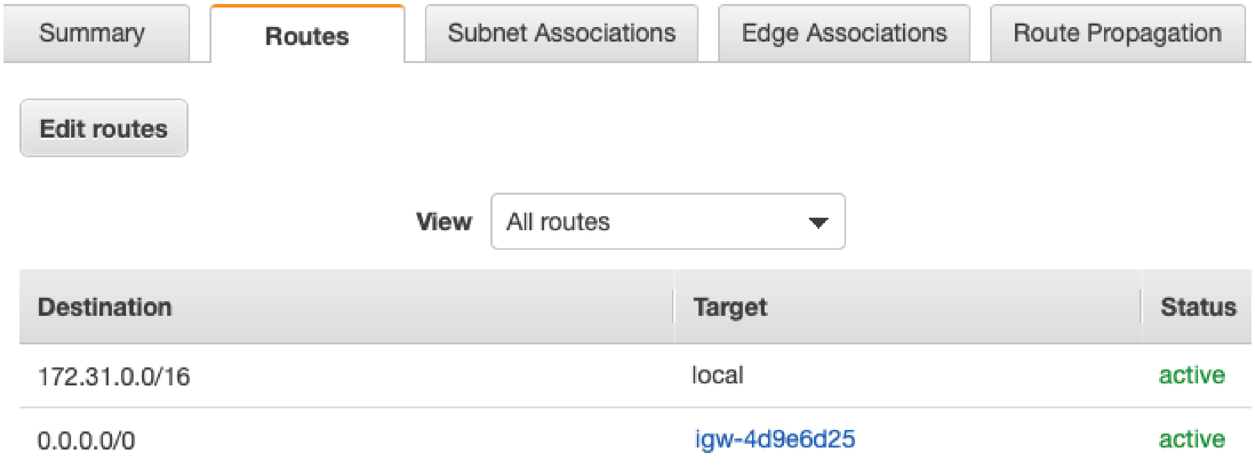
Route tables need to be created to

- allow the **Management** subnet to be accessible from the Internet via the **Internet Gateway**
- force the CV1000 to be inline between the **Network** subnet and **Local** subnet via the **Internet Gateway**

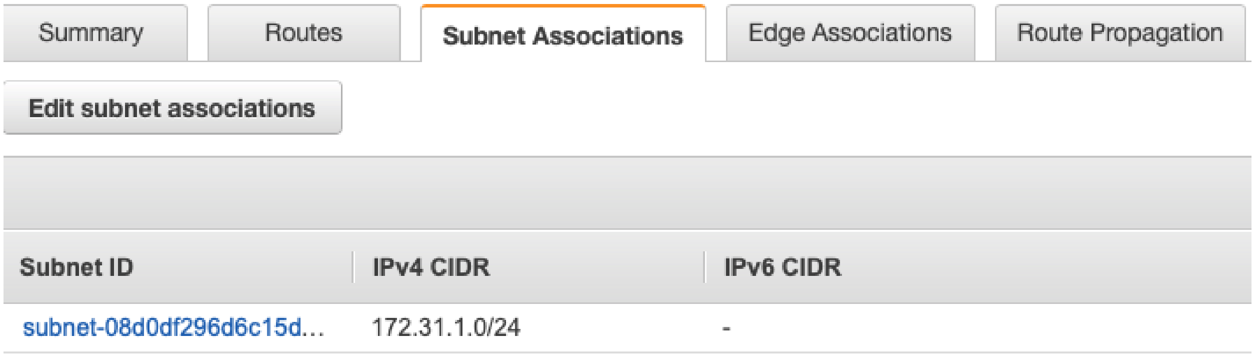
The route tables are defined below.

5.6.1 Management Subnet Route Table

The **igw Target** refers to the **Internet Gateway**.



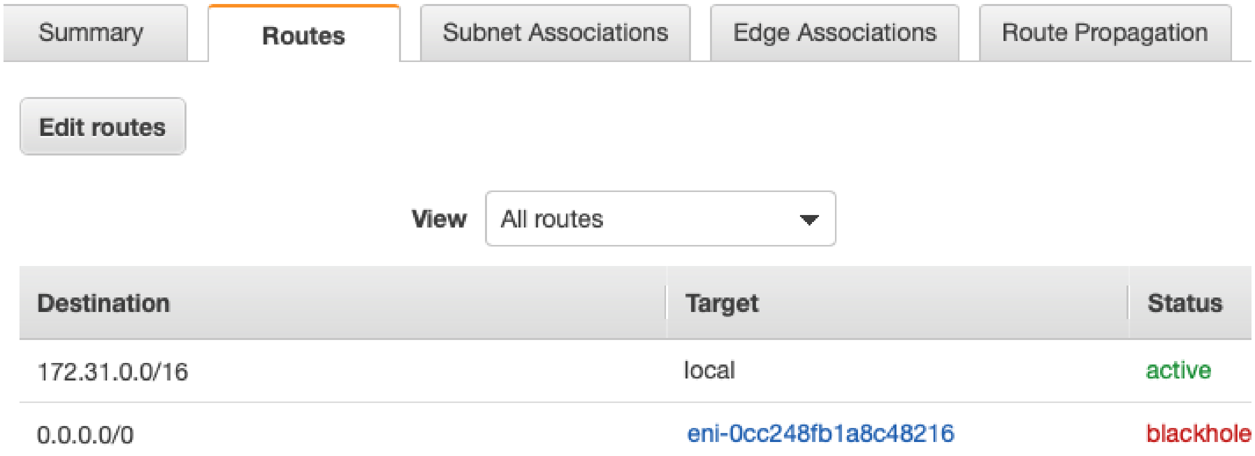
Destination	Target	Status
172.31.0.0/16	local	active
0.0.0.0/0	igw-4d9e6d25	active



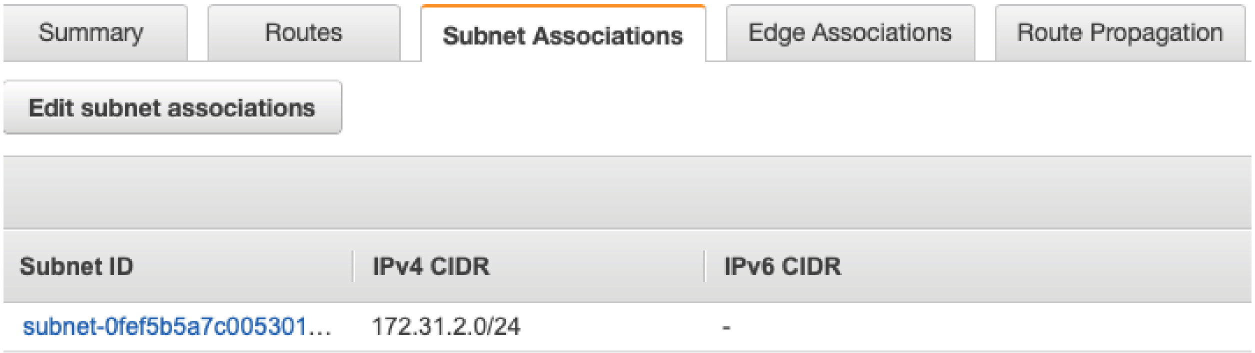
Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-08d0df296d6c15d...	172.31.1.0/24	-

5.6.2 Local Subnet Route Table

The **eni Target** refers to the **CV1000 Local network interface**.



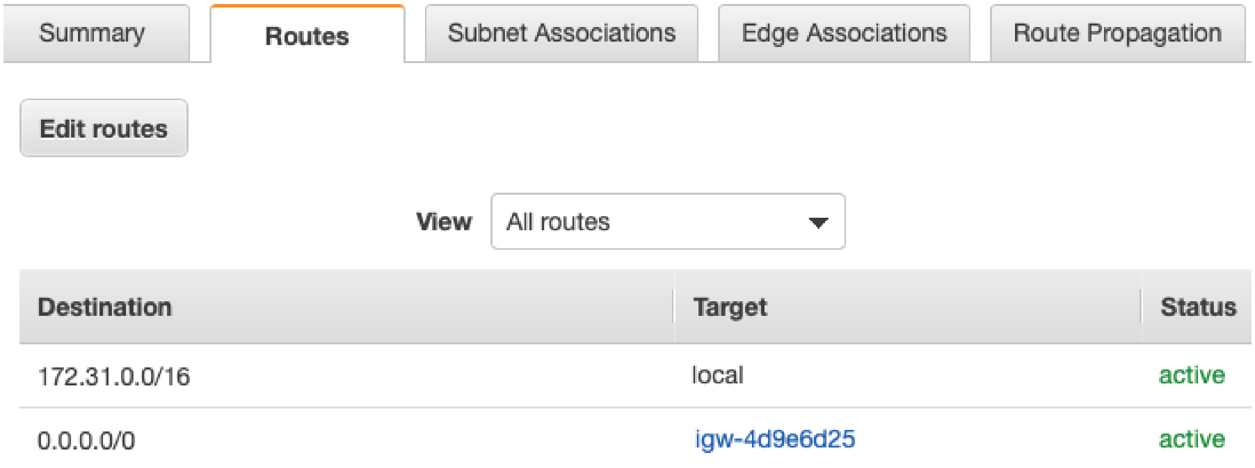
Destination	Target	Status
172.31.0.0/16	local	active
0.0.0.0/0	eni-0cc248fb1a8c48216	blackhole



Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-0fef5b5a7c005301…	172.31.2.0/24	-

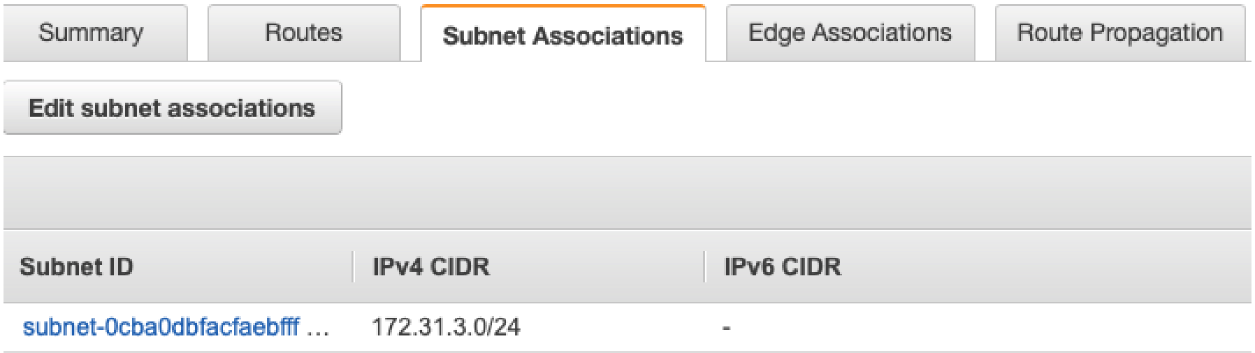
5.6.3 Network Subnet Route Table

The **igw Target** refers to the **Internet Gateway**.



View: All routes

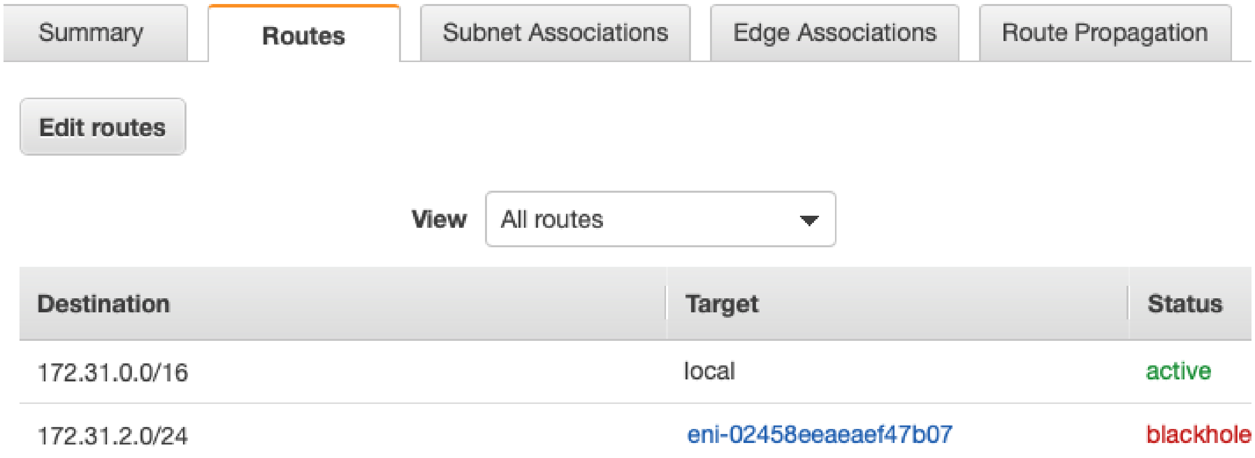
Destination	Target	Status
172.31.0.0/16	local	active
0.0.0.0/0	igw-4d9e6d25	active



Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-0cba0dbfacfaebfff …	172.31.3.0/24	-

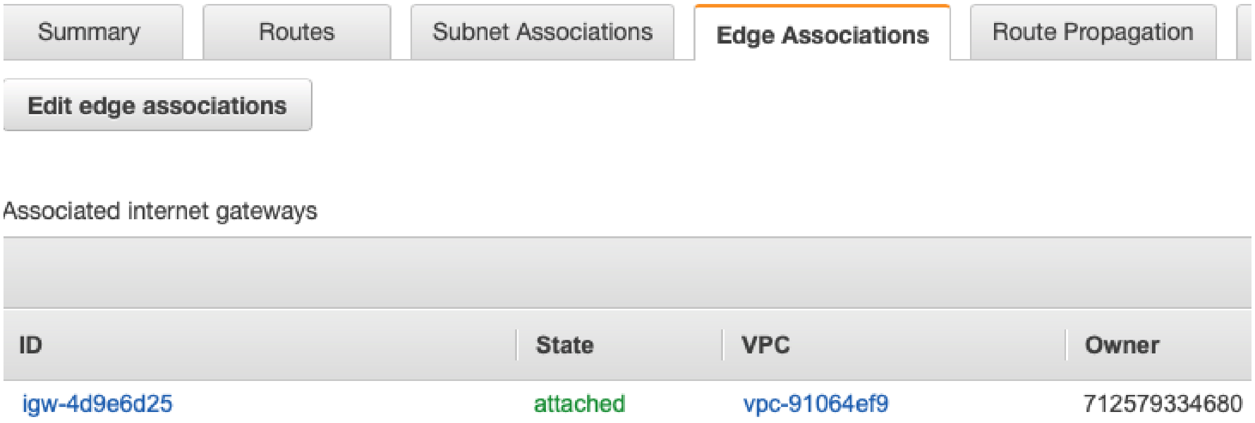
5.6.4 Internet Gateway Route Table

The **Destination** 172.31.2.0/24 refers to the **CV1000 Local subnet** and the **eni Target** refers to the **CV1000 Network interface** (i.e., the first network interface hop to get to the Destination).



Destination	Target	Status
172.31.0.0/16	local	active
172.31.2.0/24	eni-02458eeaeaef47b07	blackhole

The **igw Edge Association** refers to the **Internet Gateway** available with the current VPC.



Associated internet gateways

ID	State	VPC	Owner
igw-4d9e6d25	attached	vpc-91064ef9	712579334680

6 Create and Configure a CV1000 Instance

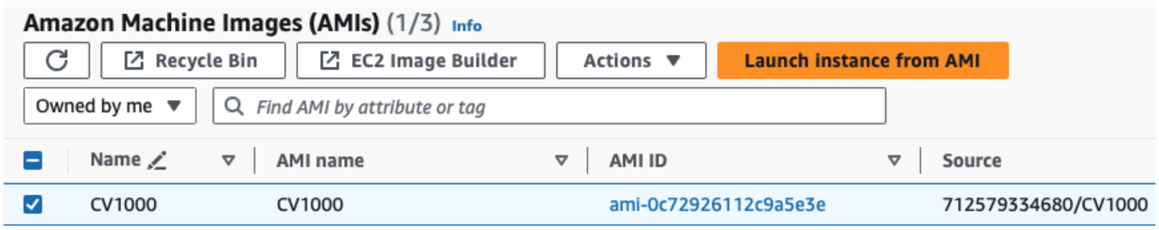
Once the CV1000 AMI is ready, it can be launched to create a virtual encryptor **Instance**. The following steps are performed as part of the Instance creation process:

- Assign VM resources (e.g., CPUs, RAM)
- Assign network adapters (Management, Local, Network)

6.1 Assign Resources and Network Adapters to CV1000 Instance

The following steps show how to create a virtual encryptor instance and assign resources and network adapters to it:

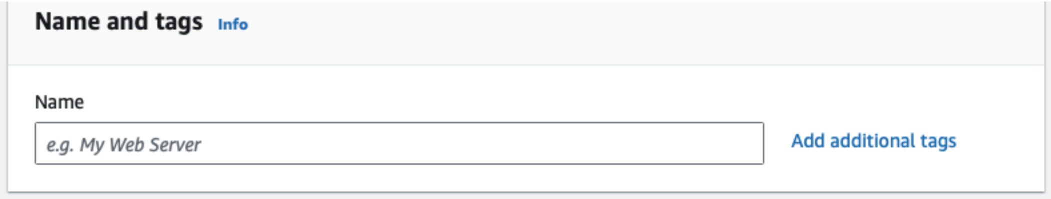
1. **Select and Launch an AMI**
   In the AWS console, under **EC2 > Images > AMIs** select the CV1000 AMI and click on **Launch instance from AMI**. This will initiate the creation of a virtual encryptor instance.



	Name	AMI name	AMI ID	Source
☑	CV1000	CV1000	ami-0c72926112c9a5e3e	712579334680/CV1000

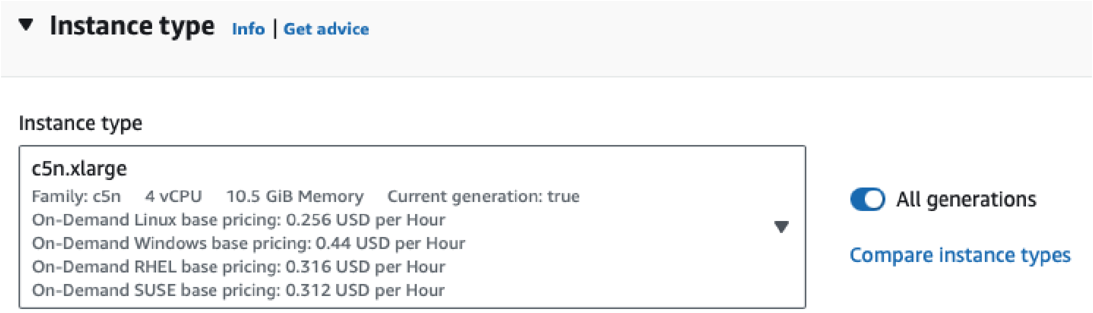
   Unlike the old AWS Launch Instance Wizard, all the settings required to create and launch an Instance are now entered on a single **Launch an instance** page. The separate sections are listed below.

2. **Name and tags**
   In the **Name and tags** section, give the Instance a name (e.g., CV1000).



3. **Application and OS Images (Amazon Machine Image)**
   In the **Application and OS Images** section, the AMI selected in step 1 above should be listed. However, if the CV1000 AMI is available in the AMI Marketplace, it can be selected from there instead.

4. **Instance type**
   Select a **Compute Optimized** instance type with minimum 4 vCPUs and 2 GB RAM. Make sure that the instance type selected supports at least **three NICs**, since the number of NICs supported is tied to the instance type.



▼ Instance type Info | Get advice

Instance type

c5n.xlarge
Family: c5n   4 vCPU   10.5 GiB Memory   Current generation: true
On-Demand Linux base pricing: 0.256 USD per Hour
On-Demand Windows base pricing: 0.44 USD per Hour
On-Demand RHEL base pricing: 0.316 USD per Hour
On-Demand SUSE base pricing: 0.312 USD per Hour

Table 1 lists some suitable instance types.

Instance Type	vCPUs	GB RAM	Max NICs	Bandwidth
c5n.xlarge	4	10.5	4	25 Gbps
c5n.2xlarge	8	21	4	25 Gbps
c5n.4xlarge	16	42	8	25 Gbps

Table 1 – CV1000 Suitable IAM Instance Types

The c5n instance types aren’t available in every AWS region, in which case a c5 instance type should be used instead.

5. **Key pair (login)**
   In the **Key pair login** section, no entry is required.

6. **Network settings**
   In the **Network settings** section, click on the Edit button.

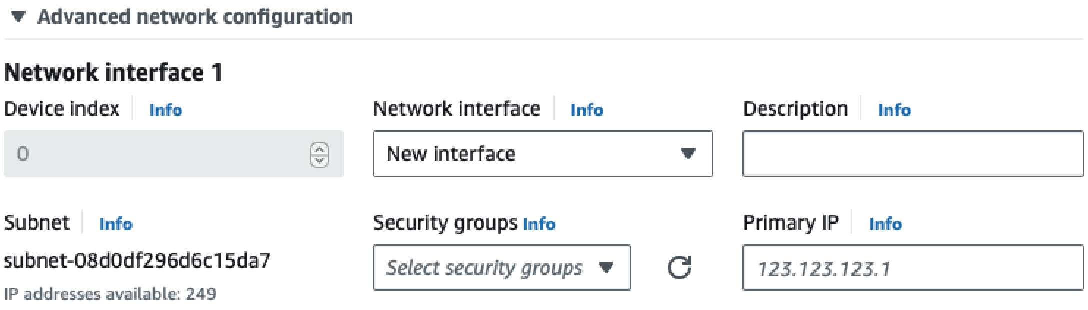
   - In the **VPC** sub-section, select the VPC.

   - In the **Subnet** sub-section, select the **Management** subnet.

   - In the **Auto-assign public IP** sub-section, leave this as **Disable**. An elastic IP address was previously assigned in section 5.5 above.

- In the **Firewall (security groups)** sub-section, enable the **Select existing security group** radio button. However, do not select any security groups, as these were previously assigned in section 5.5 above.

- Click on the **Advanced network configuration** icon to expand this sub-section and display the options for **Network interface 1** (the Management network interface).



▼ Advanced network configuration

Network interface 1

Device index Info: 0

Network interface Info: New interface

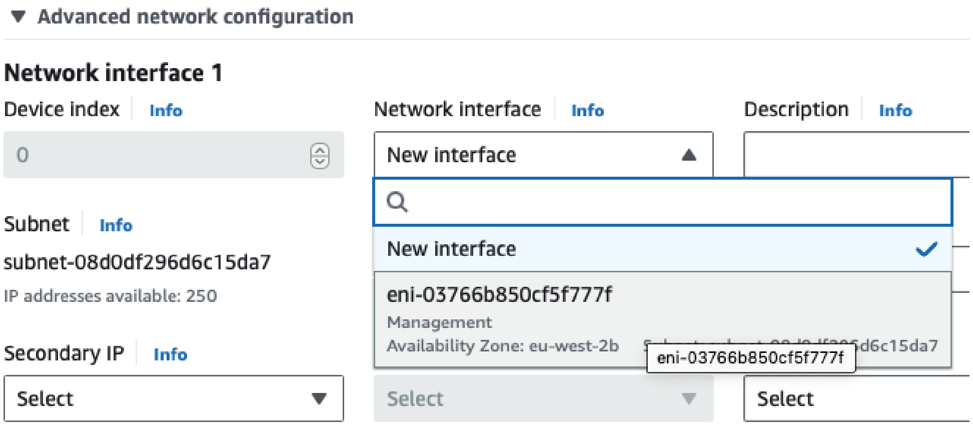
Description Info:

Subnet Info: subnet-08d0df296d6c15da7
IP addresses available: 249

Security groups Info: *Select security groups*

Primary IP Info: *123.123.123.1*

- In the **Network interface** drop down menu, select the **Management** interface. Leave all other entries as-is.



▼ Advanced network configuration

Network interface 1

Device index Info: 0

Network interface Info: New interface

Description Info:

Subnet Info: subnet-08d0df296d6c15da7
IP addresses available: 250

New interface ✓

eni-03766b850cf5f777f
Management
Availability Zone: eu-west-2b d6c15da7

eni-03766b850cf5f777f

Secondary IP Info: Select

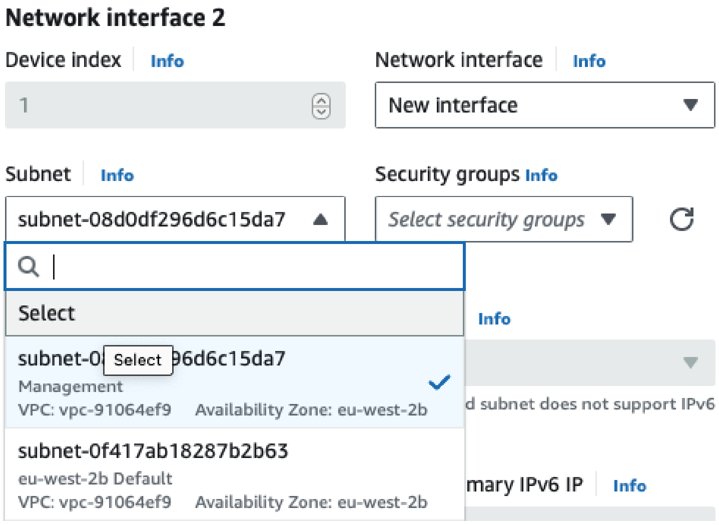
Select

Select

- Click on the **Add network interface** button to add the **Local** network interface next.

Add network interface

- In **Network Interfaces 2** click on the **Subnet** drop-down menu and choose the **Select** option at the top. This has the effect of not selecting any subnet, as this was previously assigned in section 5.5 above.



Network interface 2

Device index: 1

Network interface: New interface

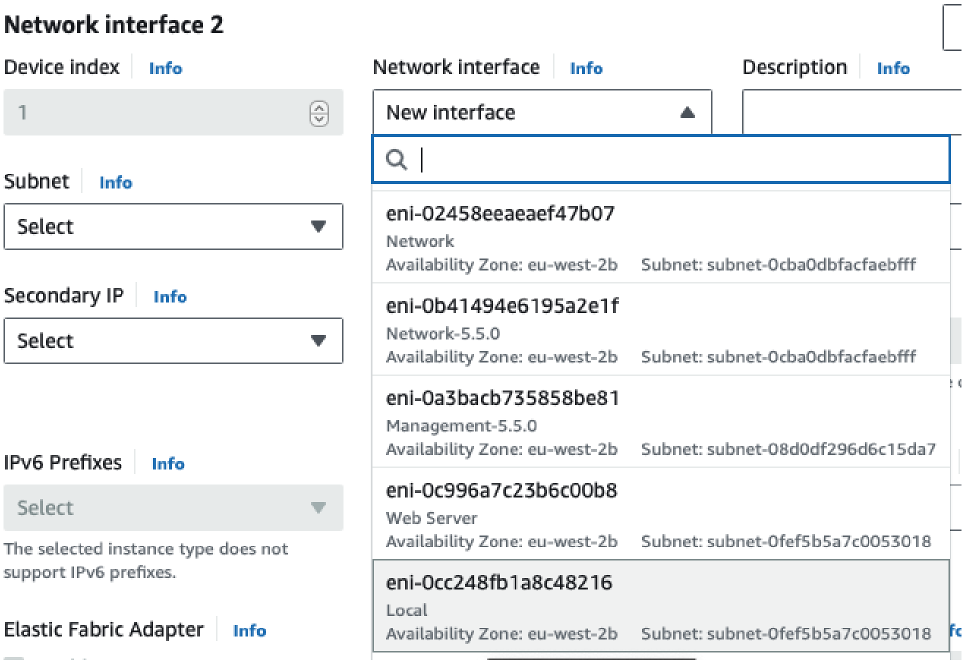
Subnet: subnet-08d0df296d6c15da7

Security groups: Select security groups

subnet-08d0df296d6c15da7
Management
VPC: vpc-91064ef9 Availability Zone: eu-west-2b

subnet-0f417ab18287b2b63
eu-west-2b Default
VPC: vpc-91064ef9 Availability Zone: eu-west-2b

- In **Network Interfaces 2** click on the **Network interface** drop-down menu and choose the **Local** (plaintext) interface. Leave all other entries as-is.



Network interface 2

Device index: 1

Network interface: New interface

Description

Subnet: Select

Secondary IP: Select

IPv6 Prefixes: Select

The selected instance type does not support IPv6 prefixes.

Elastic Fabric Adapter

eni-02458eeaeaef47b07
Network
Availability Zone: eu-west-2b Subnet: subnet-0cba0dbfacfaebfff

eni-0b41494e6195a2e1f
Network-5.5.0
Availability Zone: eu-west-2b Subnet: subnet-0cba0dbfacfaebfff

eni-0a3bacb735858be81
Management-5.5.0
Availability Zone: eu-west-2b Subnet: subnet-08d0df296d6c15da7

eni-0c996a7c23b6c00b8
Web Server
Availability Zone: eu-west-2b Subnet: subnet-0fef5b5a7c0053018

eni-0cc248fb1a8c48216
Local
Availability Zone: eu-west-2b Subnet: subnet-0fef5b5a7c0053018

- Click on the **Add network interface** button to add the **Network** (encrypted) network interface next.

- Repeat the steps used to create **Network interface 2** above to create **Network interface 3** but select the **Network** (encrypted) interface instead.

7. **Configure storage**
    - No changes are required for this section.

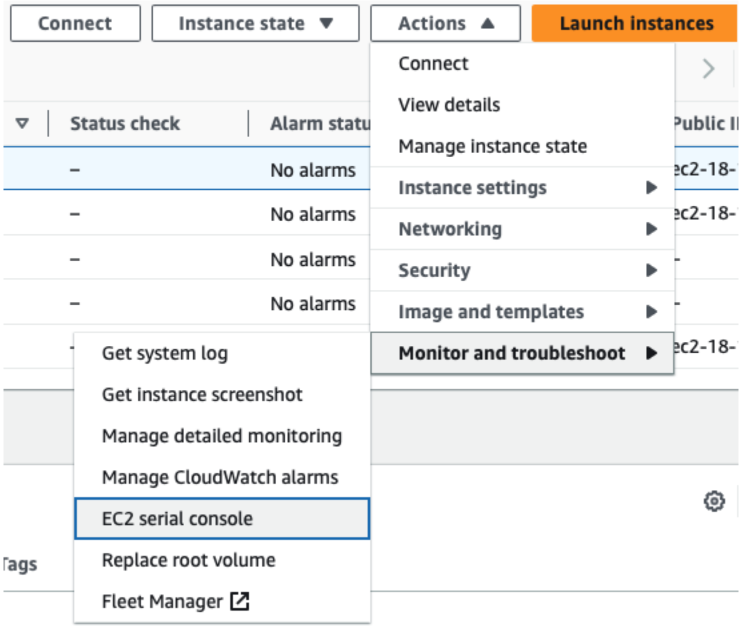
8. **Advanced details**
    - No changes are required for this section.

9. **Launch Instance**
    - Click on the **Launch instance** button to create and launch the Instance. A **Create key pair** screen will appear.

10. **Create key pair**
    - Click on the **Proceed without key pair** radio button and then click on the **Proceed without key pair** button and then the **Launch Instance** button again.

11. **Verify CLI Access**

To verify that the CLI can be used to connect to and activate the encryptor, ensure that the encryptor instance is running and then initiate a **CLI** session using the AWS **EC2 serial console** in the EC2 **Actions** drop-down menu.



A normal CLI login prompt should appear and the default username and password of an encryptor not activated should be used to logon (i.e., admin/$Password1).

7 Configure CV1000-AWS Instance

Once the CV1000 instance is up and running, configure the encryptor via the CLI and/or CM7 as per the CV1000 User Guide.

The basic steps are as follows:

1. **Activate** the encryptor and change the default credentials via the AWS **EC2 serial console** in the EC2 Actions drop-down menu.
   - `activate -l`

2. Enable SSH & SNMP over SSH and set the Remote Cli Key. (This step must be done before accessing the CV1000 via CM7)
   - snmpcfg -s on
   - sshcli -e
   - sshcli -a “ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLmndQo3+UQJUgpP00pz4HRmqbZ3yoA6PGp4ODSKYaC8tVEZ9TTIt+QR3xUMZNTwIkphDNeYVvhnk5i9pRh16nk= CM7@192.168.2.106”

     Note that the value inside the double quotes is the public key of the SSH Key created using the procedures in Appendix A. This enables both SSH access and SNMP over SSH which is a security best practice and more secure than SNMP.

3. Set encryption **Policy**, e.g., AES-GCM-256.

4. Assign a **Key Derivation Key**.

5. Assign an **NTP time server** if time-based key synchronisation is being used.

6. Create **IP Rules** for Layer 3, Layer 4 or Layer 4 UDP Tunnelling encryption based on the network requirements.

7. Enable **Autodiscover** for the Layers required (e.g., L3, L4, LTU).

8. Set the **Global mode** to encrypt.
   - `global -e`

[**Notes**:

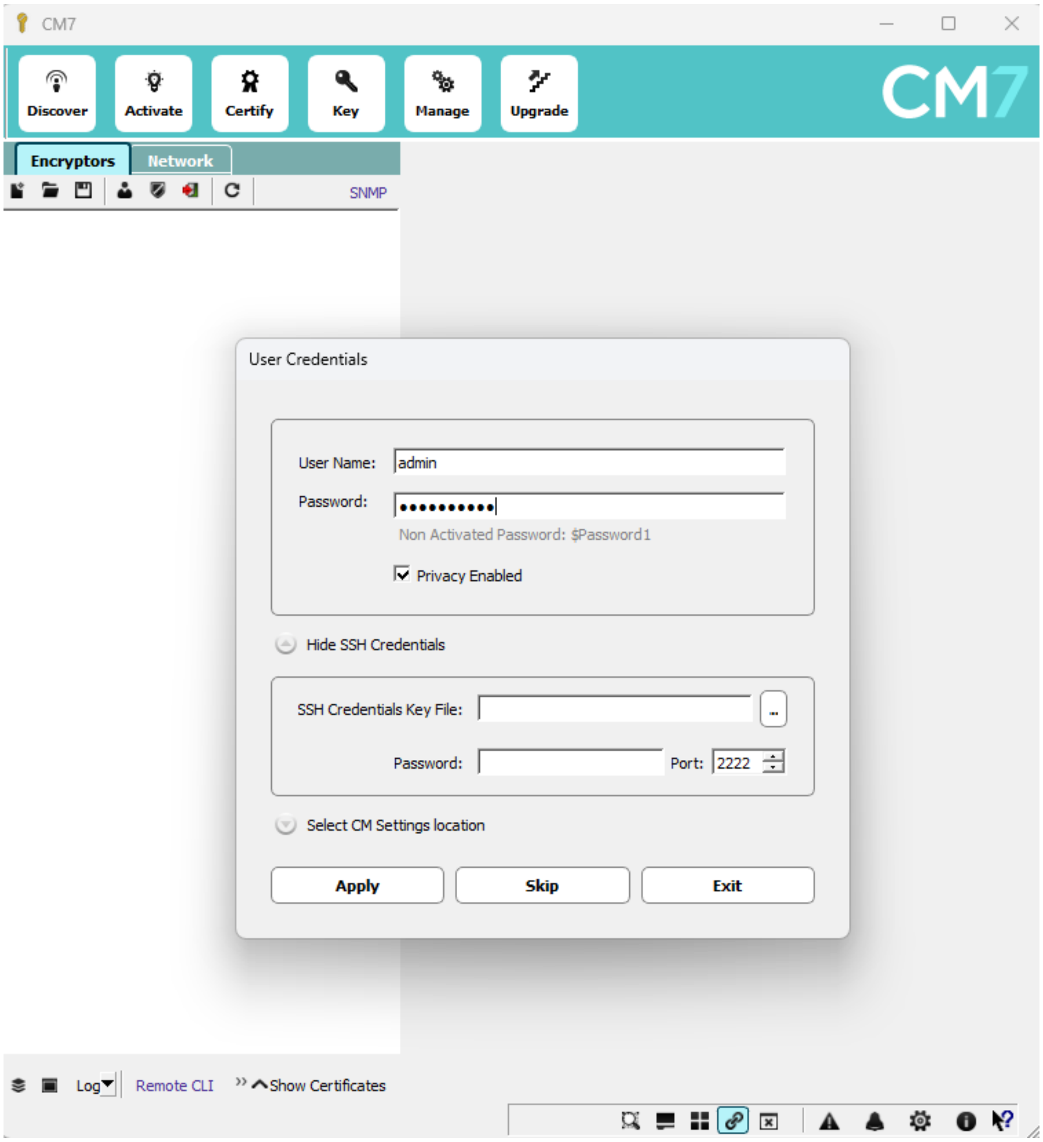
1. It should not be necessary to assign a Management IP address, as this should already have been assigned as part of the Management interface configuration above.

Appendix A: Set up remote cli (ssh) key in CM7

A remote cli (ssh) key needs to be created in CM7 and the public key needs to be set in the CV1000 – see step 2 in section 7.

Below are the steps needed to create the key in CM7:

First login to CM7. Notice there is no SSH Credentials Key File on a fresh install of CM7, there will not be any key files present.



User Credentials

User Name: admin

Password: ••••••••••

Non Activated Password: $Password1

☑ Privacy Enabled

Hide SSH Credentials

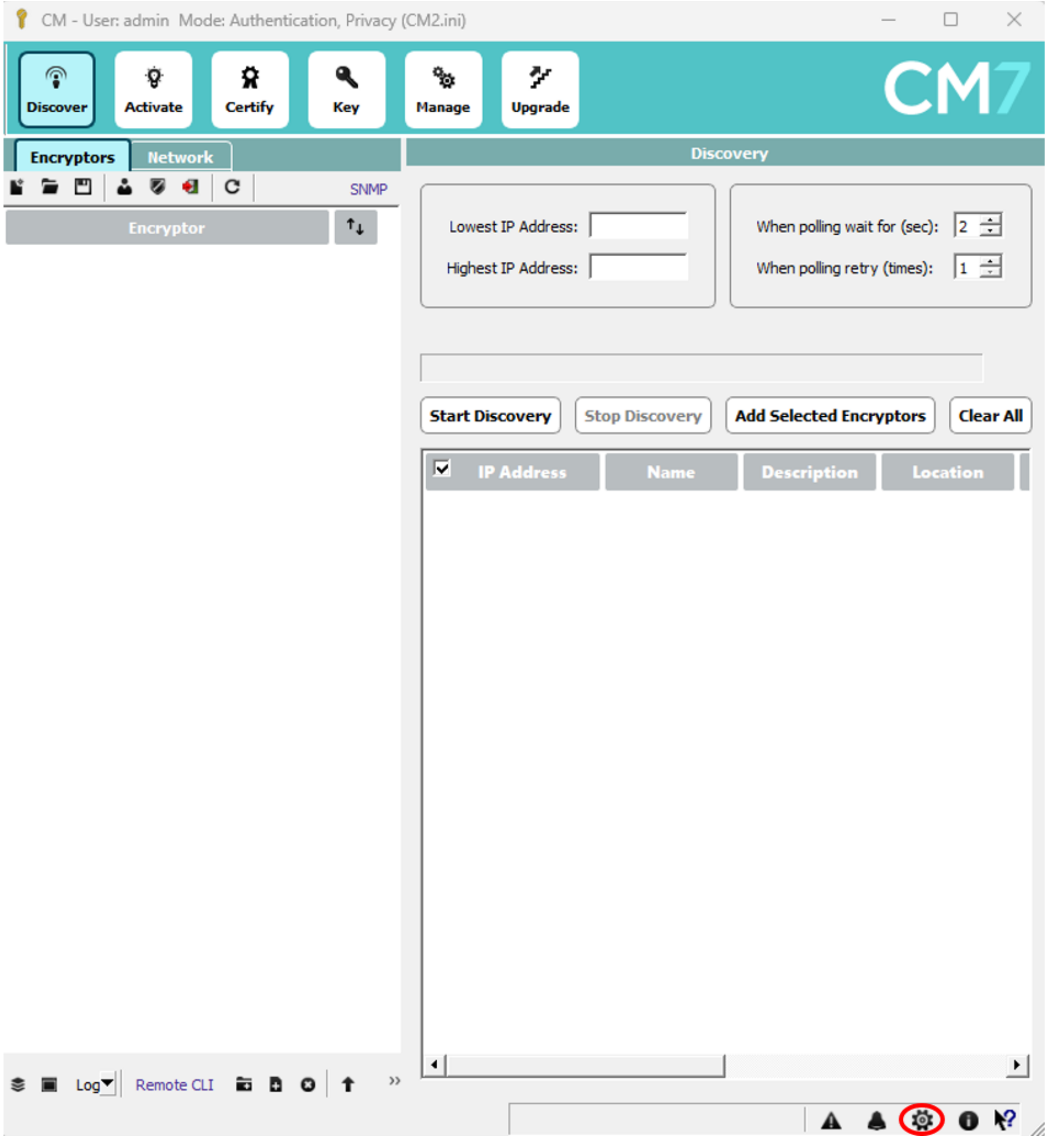
SSH Credentials Key File:

Password:

Port: 2222

Select CM Settings location

Click on Apply and you will be logged in.



CM - User: admin Mode: Authentication, Privacy (CM2.ini)

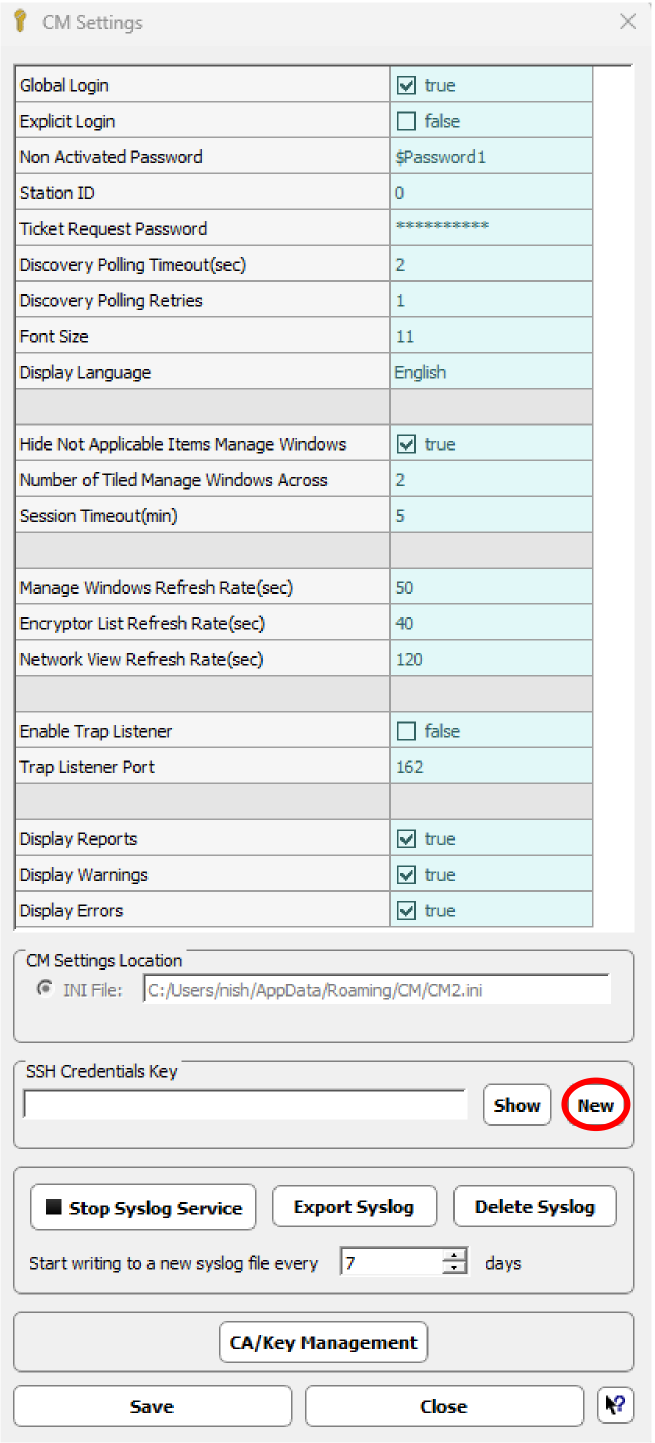
Lowest IP Address:

Highest IP Address:

When polling wait for (sec): 2

When polling retry (times): 1

Click on the gear icon to open the CM Settings window.



Global Login	☑ true
Explicit Login	□ false
Non Activated Password	$Password1
Station ID	0
Ticket Request Password	***********
Discovery Polling Timeout(sec)	2
Discovery Polling Retries	1
Font Size	11
Display Language	English
Hide Not Applicable Items Manage Windows	☑ true
Number of Tiled Manage Windows Across	2
Session Timeout(min)	5
Manage Windows Refresh Rate(sec)	50
Encryptor List Refresh Rate(sec)	40
Network View Refresh Rate(sec)	120
Enable Trap Listener	□ false
Trap Listener Port	162
Display Reports	☑ true
Display Warnings	☑ true
Display Errors	☑ true

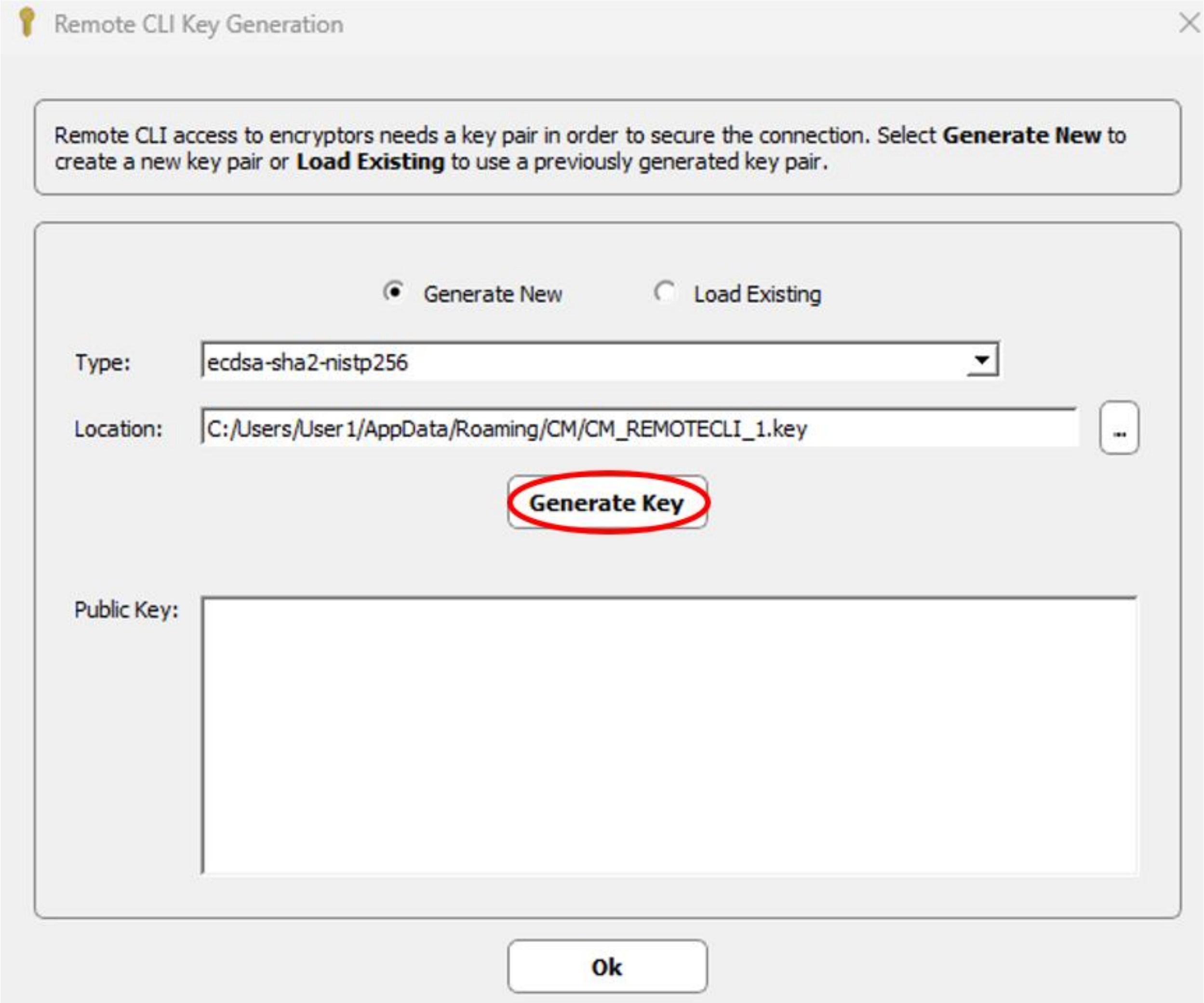
CM Settings Location

● INI File: C:/Users/nish/AppData/Roaming/CM/CM2.ini

SSH Credentials Key

Start writing to a new syslog file every 7 days

Click on New to create a new SSH Key file.



Remote CLI Key Generation

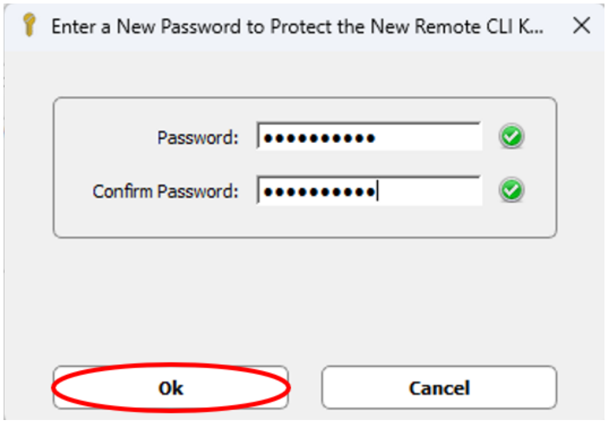
Remote CLI access to encryptors needs a key pair in order to secure the connection. Select **Generate New** to create a new key pair or **Load Existing** to use a previously generated key pair.

● Generate New ○ Load Existing

Type: ecdsa-sha2-nistp256

Location: C:/Users/User 1/AppData/Roaming/CM/CM_REMOTECLI_1.key

Click on “Generate Key” and you will be prompted to set the password for the SSH Key file.

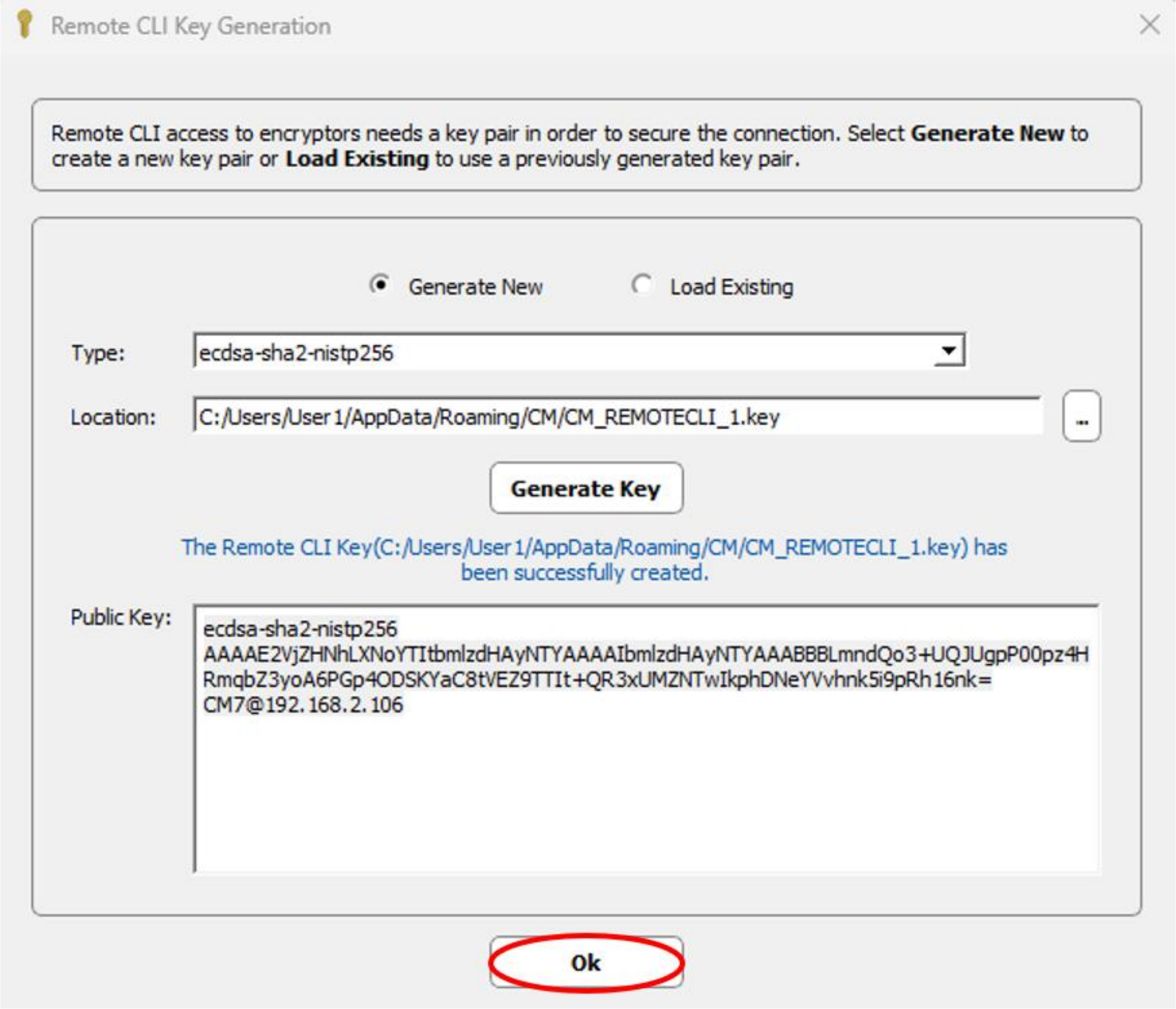


Enter a New Password to Protect the New Remote CLI K...

Password: ••••••••••

Confirm Password: ••••••••••

Set the Password for the SSH Key file and click on Ok. The SSH Key file will be created and a public key will appear in the “Public Key” box.



Remote CLI access to encryptors needs a key pair in order to secure the connection. Select **Generate New** to create a new key pair or **Load Existing** to use a previously generated key pair.

● Generate New ○ Load Existing

Type: ecdsa-sha2-nistp256

Location: C:/Users/User 1/AppData/Roaming/CM/CM_REMOTECLI_1.key

The Remote CLI Key(C:/Users/User 1/AppData/Roaming/CM/CM_REMOTECLI_1.key) has been successfully created.

Public Key:

```
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLmndQo3+UQJUgpP00pz4H
RmqbZ3yoA6PGp4ODSKYaC8tVEZ9TTIt+QR3xUMZNTwIkphDNeYVvhnk5i9pRh16nk=
CM7@192.168.2.106
```

Select the text in the Public Key box and copy it. (This public key needs to be set in the CV1000 – see step 2 in section 7.) Click on Ok and then close the CM7 Settings.

Note: This key is required for security best practices in having CM7 access the CV1000 in AWS using SNMP over SSH as it is more secure than just using SNMP.

Next time you launch CM7, input the User Name and password. In the SSH Credentials, you will now see the SSH Key file you created. Enter the SSH Key password & ensure the Port is 22 and click on Apply.

Now you are logged into CM7 and will be able to Discover and manage the CV1000 in AWS via SNMP over SSH.