SafeNet Virtual KeySecure AWS Marketplace Installation Guide

Software Version: 7.1.0
Documentation Version: 20131023
Part Number: 007-012368-001 (Rev A)

Preface

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person of organization of any such revisions or changes.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address below.

4690 Millennium Drive
Belcamp, Maryland 21017
USA

Disclaimers

The foregoing integration was performed and tested only with specific versions of equipment and software and only in the configuration indicated. If your setup matches exactly, you should expect no trouble, and Customer Support can assist with any missteps. If your setup differs, then the foregoing is merely a template and you will need to adjust the instructions to fit your situation. Customer Support will attempt to assist, but cannot guarantee success in setups that we have not tested.

This product contains software that is subject to various public licenses. The source code form of such software and all derivative forms thereof can be copied from the following website: https://serviceportal.safenet-inc.com

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

The virtual KeySecure systems use open source Linux with a customization to the dm-crypt component in the Linux kernel. For the details on this customization and the customized source code, please see:

http://c3.safenet-inc.com/Display_Results_google.asp?DocId=20353.

Technical Support

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, please contact your supplier or SafeNet support.

SafeNet 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 SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Technical Support Contact Information:

Phone: 800-545-6608, 410-931-7520
Email: support@safenet-inc.com

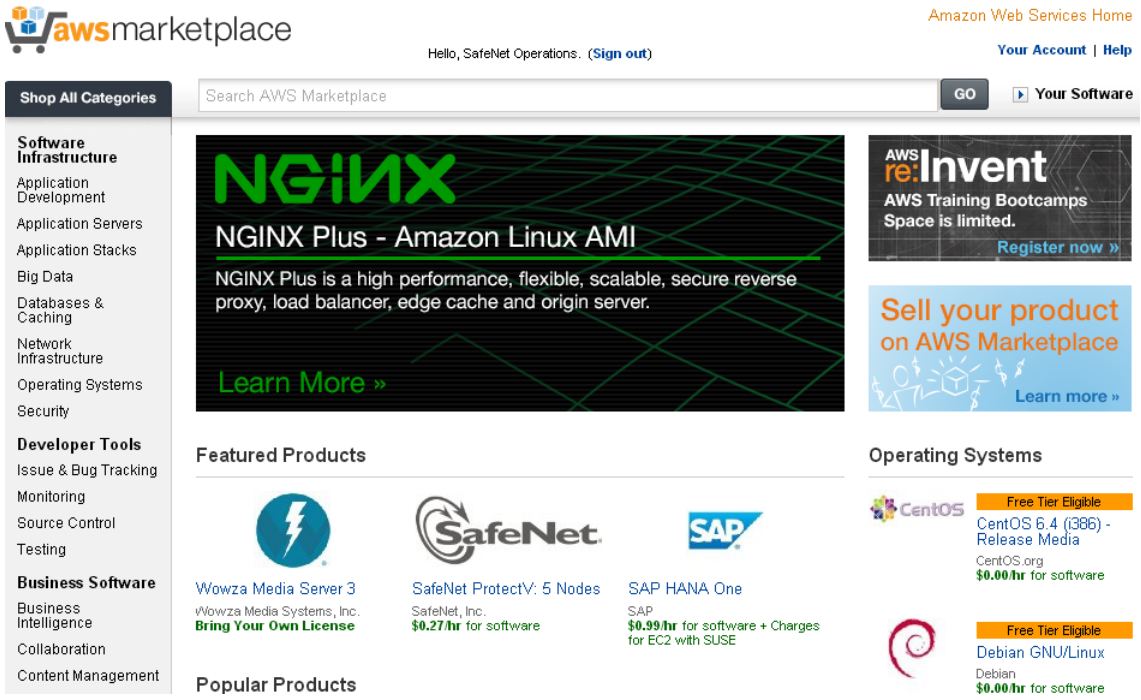
Table of Contents

Chapter 1

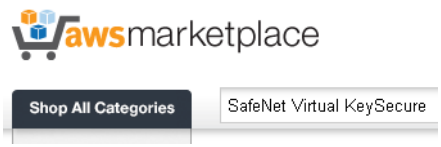
Configuring KeySecure in AWS Marketplace

In AWS Marketplace...

1 Log on to AWS Marketplace with your AWS account credentials. The following page is displayed.



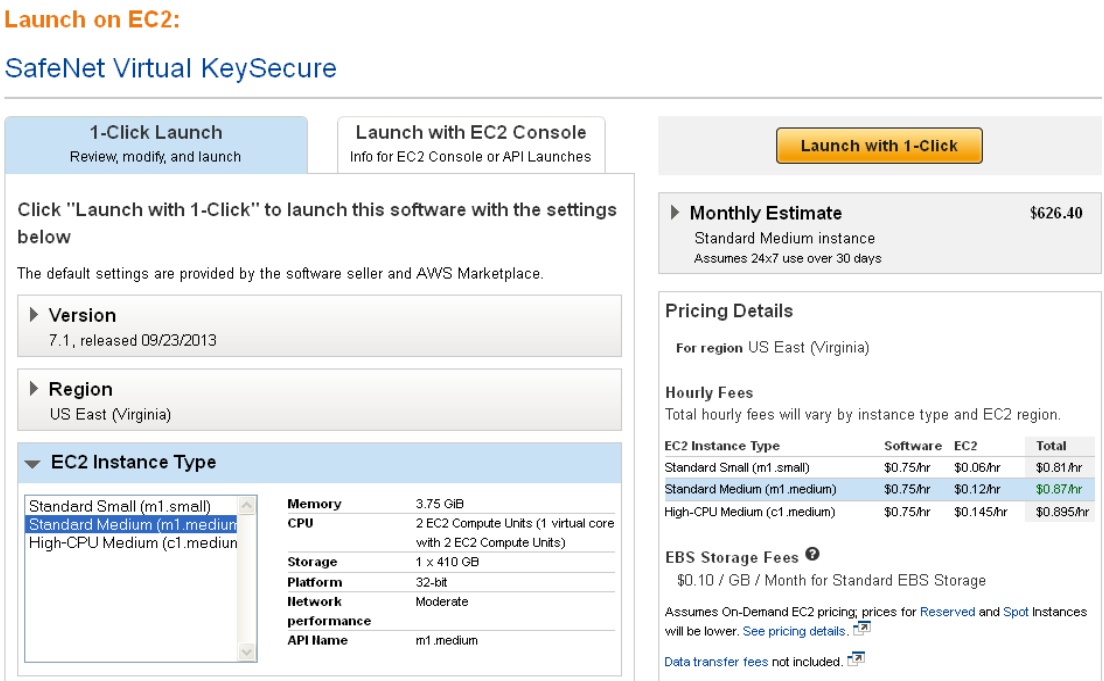
2 Type **SafeNet Virtual KeySecure** in the **Search AWS Marketplace** field.



3 Click **GO**, or press **Enter**. You will see a list of Virtual KeySecure products.

4 Click a Virtual KeySecure product that matches your needs. The following page is displayed.

5 Click **Continue**. The *Launch on EC2: SafeNet Virtual KeySecure* page is displayed.



The *Launch on EC2: SafeNet Virtual KeySecure* page contains the following two tabs, **1-Click Launch** and **Launch with EC2 Console**. These tabs provide two different ways to launch the Virtual KeySecure instance.

1-Click Launch helps you launch quickly with recommended default options such as security groups and instance types. With **1-Click Launch**, you can also see your estimated monthly bill. However, **1-Click Launch** requires an existing key pair. As a new user does not have an existing key pair, if a new instance is created using this option, then the user can't get the key pair to SSH into the instance.

Launch with EC2 Console enables you to alter the default configuration and import or generate a key pair prior to launching the instance. New users should use the **Launch with EC2 Console** tab.

To launch a Virtual KeySecure instance with the EC2 console, follow the steps mentioned in "Launching a Virtual KeySecure Instance" below.

Launching a Virtual KeySecure Instance

Virtual KeySecure instance(s) must be launched into EC2 VPC mode.

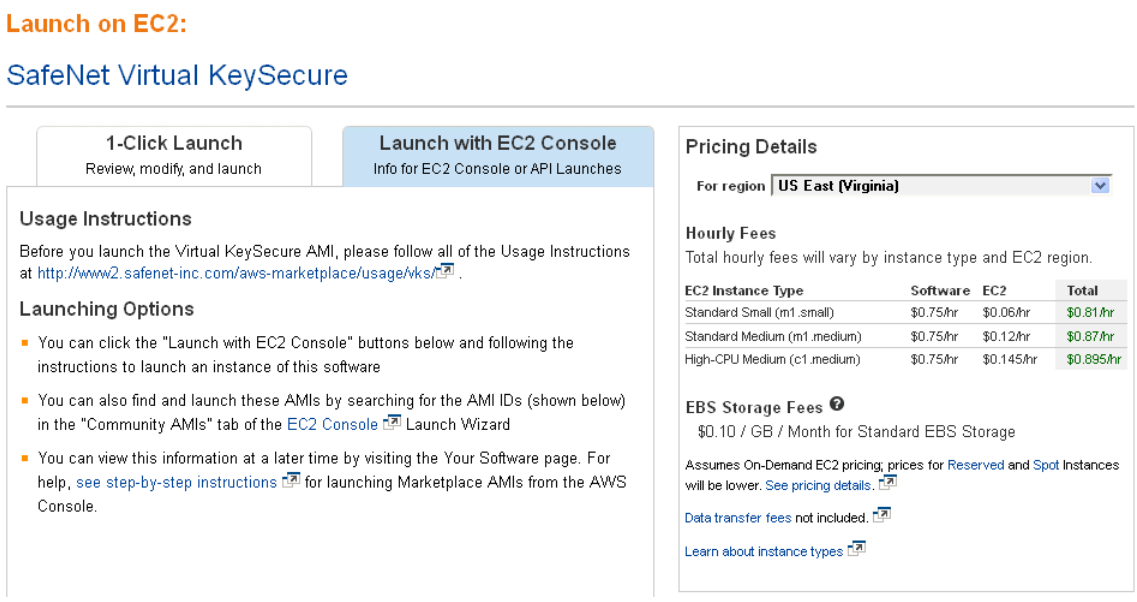
Important!

- Each Virtual KeySecure instance will have a private IP address. This IP address will be used for (create or join) cluster operations.
- The clustering feature is supported, but only between Virtual KeySecure instances deployed in the same VPC.

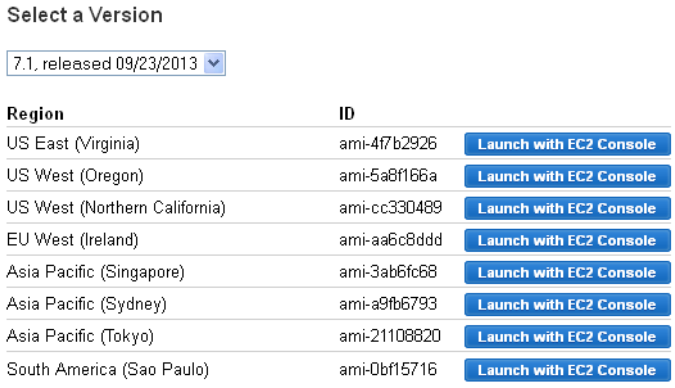
To launch the Virtual KeySecure instance with EC2 console, use the **Launch with EC2 Console** tab available on the *Launch on EC2: SafeNet Virtual KeySecure* page.

Perform the following steps:

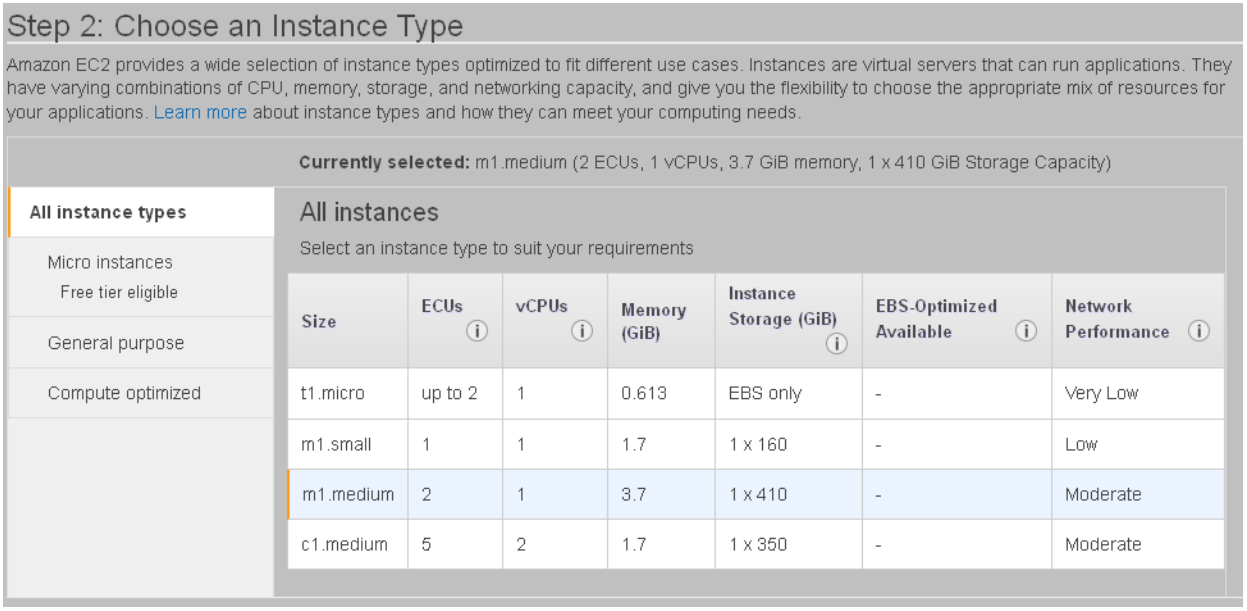
1 Click the **Launch with EC2 Console** tab. The following screen is displayed.



2 Select a Virtual KeySecure AMI version from the **Select a Version** drop-down list.

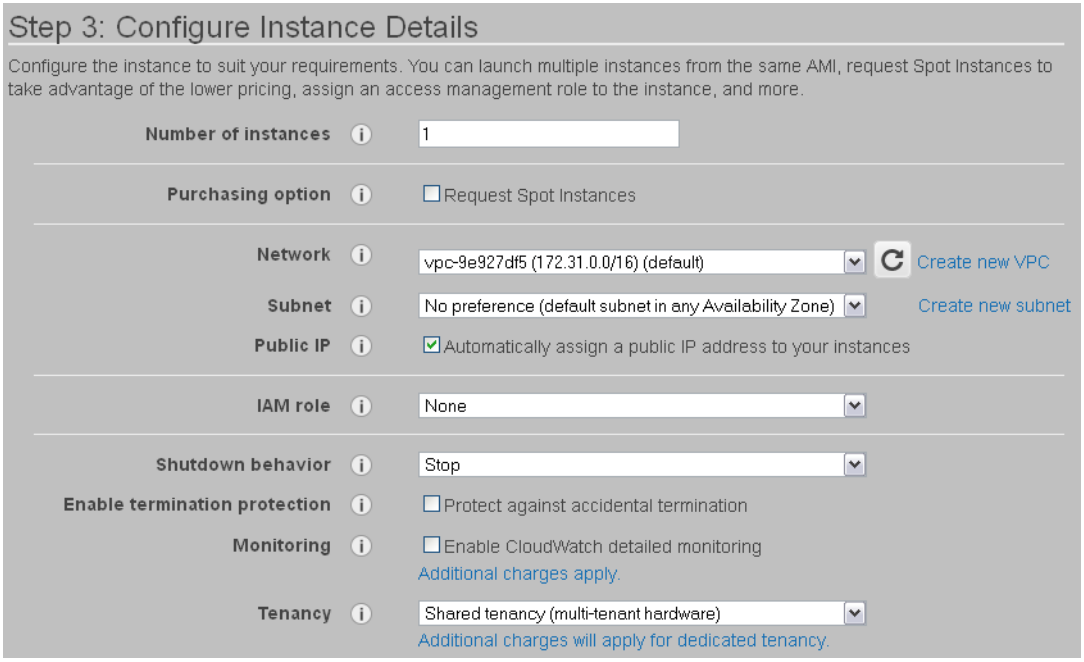


3 Click **Launch with EC2 Console** next to your region. The *Step 2: Choose an Instance Type* screen of the Request Instances Wizard is displayed.



4 Select the instance size, which determines the number of ECUs, vCPUs, memory, storage, and network performance. The Virtual KeySecure 32-bit AMI runs only on **m1.small**, **m1.medium**, or **c1.small** Instance Type. For details about Instance Type, refer to AWS documentation.

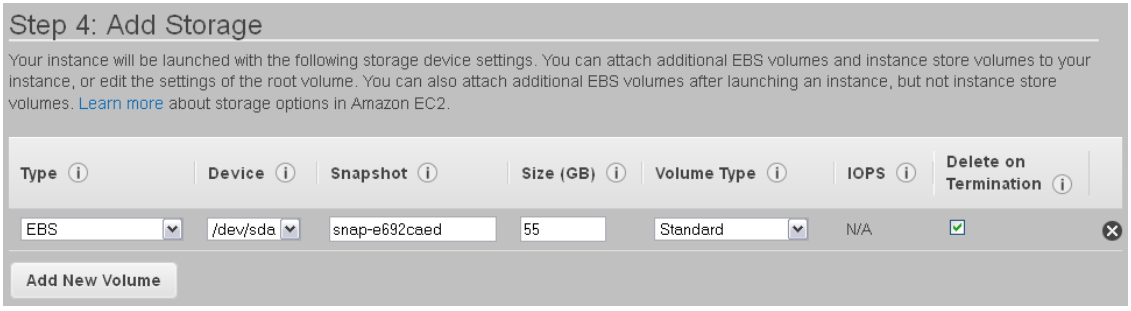
5 Click **Next: Configure Instance Details**.



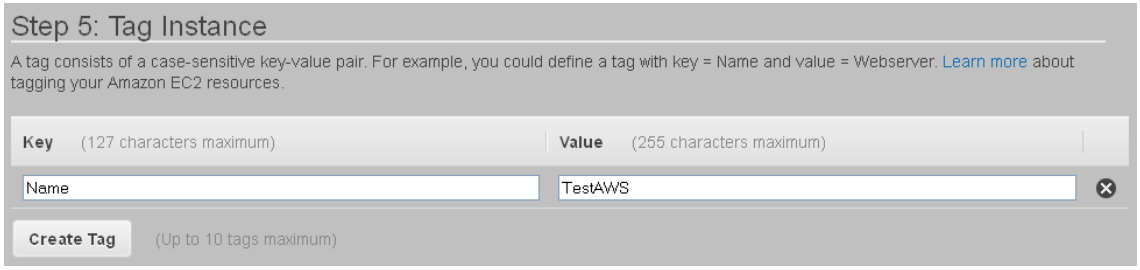
6 Configure the instance details (the number of instances, network, subnet, etc.). This document assumes the following values: Number of instances as **1**, Network as **default**, and Subnet as **No preference**.

7 Configure advanced details (Monitoring, Termination Protection, Shutdown Behavior etc.) For the **Kernel ID** and **RAM Disk ID** fields, use the default value, **Use Default**. This document assumes default values for all fields.

8 Click **Next: Add Storage**. The instance will be launched with these storage device settings. Do not alter these settings.

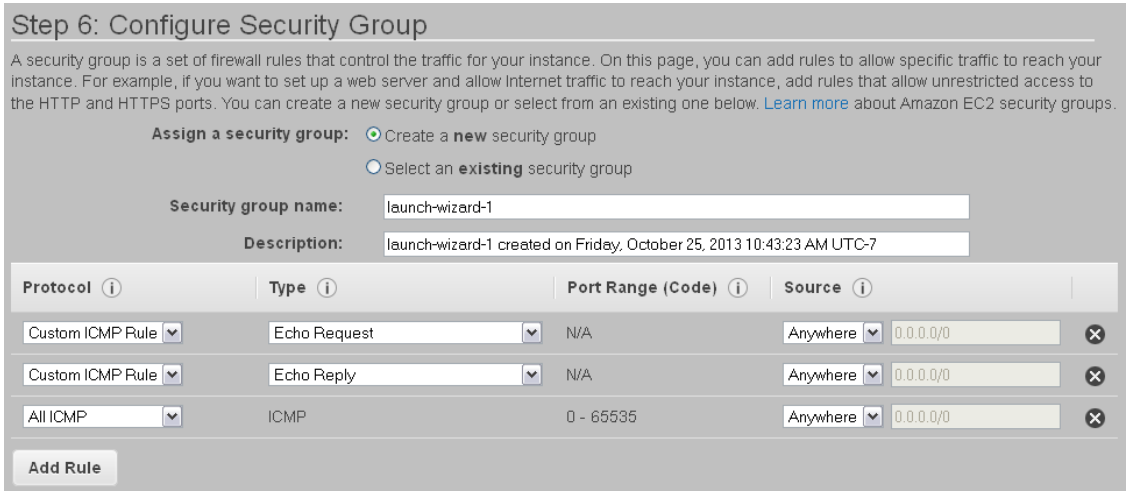


9 Click **Next: Tag Instance**.



10 Enter a name for the machine in the **Value** field. This document assumes **TestAWS**. Note down this value, as it will be required later. Adding tags such as instance name to your instance will simplify the administration of your EC2 infrastructure. Tags can be added, edited, and removed.

11 Click **Next: Configure Security Group**.



12 Select an existing security group or create a new security group. Multiple security groups can also be selected. **Don't select a default security group**.

Note: If you want to use an existing security group, select **Choose one or more of your existing Security Groups**, select the security group(s), and click **Continue**.

To create and use a new security group:

a Select **Create a new Security Group**.

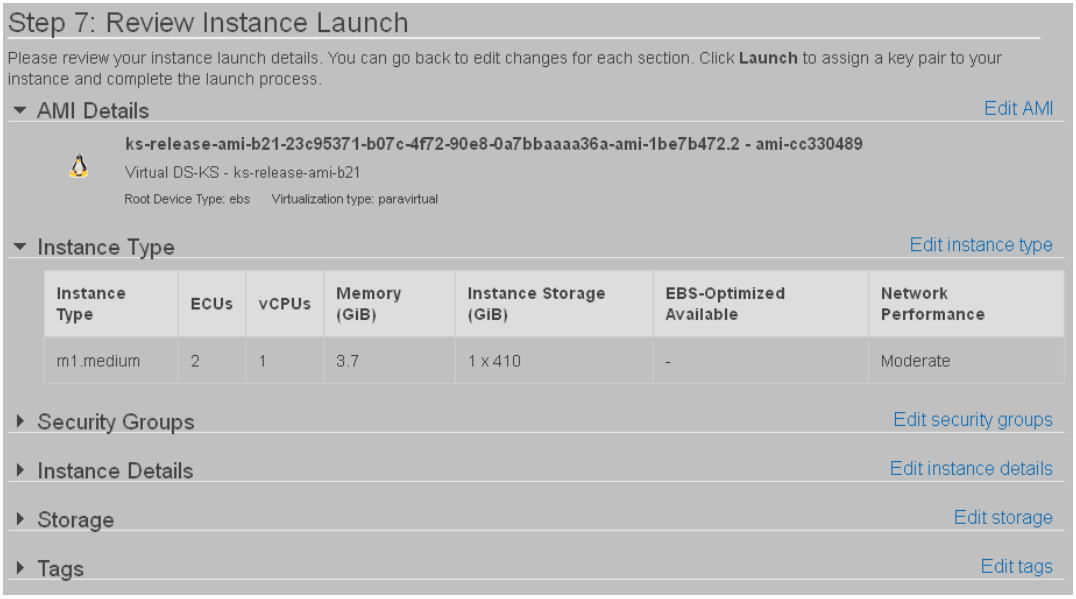
b Enter the following details:

- **Group Name:** Name for the security group.
- **Group Description:** Description for the security group.
- **Rules:** Create the inbound and outbound rules. Specify a protocol, type, port range, etc.

c Click **Add Rule.**

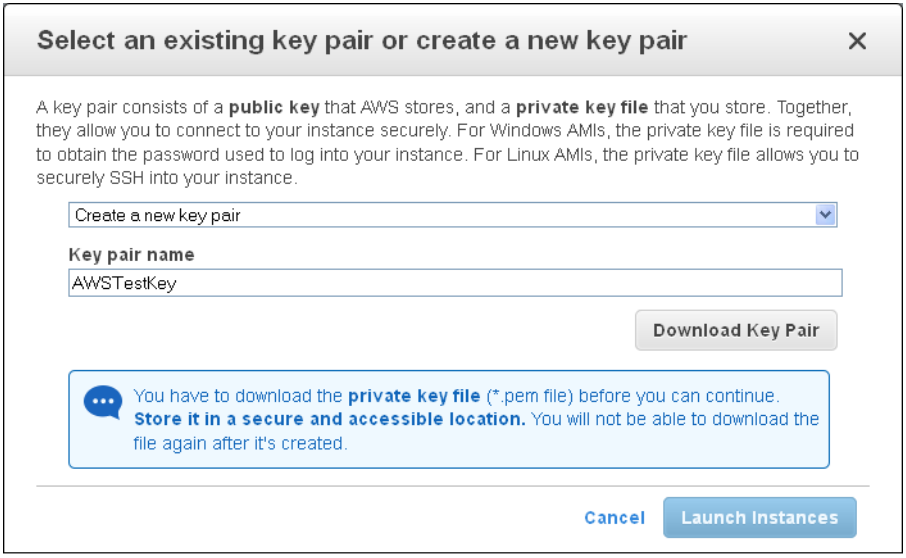
Important! Because you cannot differentiate between inbound and outbound rules at this stage, we recommend that you configure only the ICMP rules, shown above. You can update the security group after completing the Virtual KeySecure configuration. The security group updates are applied immediately. For the complete list of inbound and outbound rules, as well as instructions for updating the security group, see step 18, below.

13 Click **Review and Launch**.



14 Review the information. If changes are needed, click **Previous** to return to the appropriate screen.

15 Click **Launch**. The *Select an existing key pair or create a new key pair* window appears.



16 Select either **Create a new key pair** or **Choose an existing key pair**. Do NOT select **Proceed without a Key Pair**.

Note: If you want to use an existing key pair, select **Choose an existing Key Pair**, select the key pair from the **Your existing Key Pairs** drop-down list, and click **Continue**.

To create and use a new key pair:

a Select **Create a new Key Pair**.

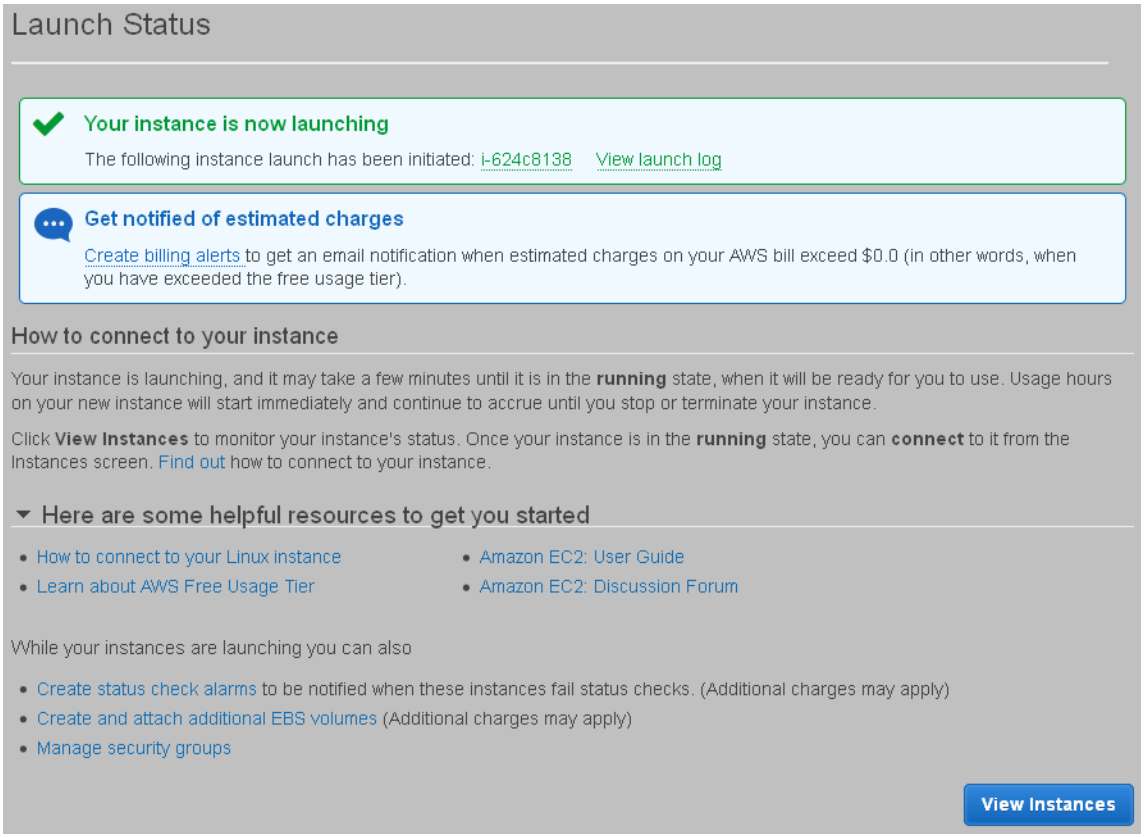
b Enter a name for your key pair. This document assumes **AWSTestKey**.

c Click **Create & Download your Key Pair**. The new key pair is created and download to your machine.

Tip: To use PuTTY for SSH connectivity on Windows, the generated PEM file must be converted into a PPK file.

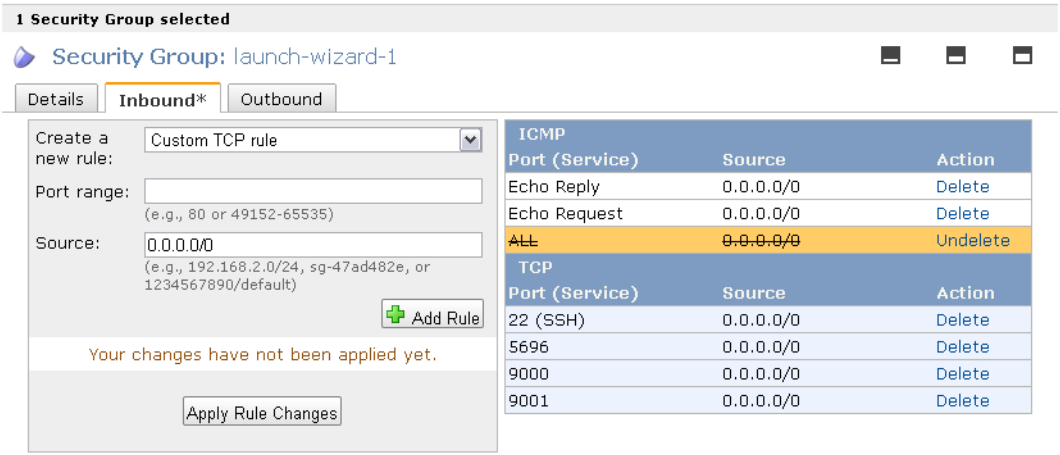
17 Click **Launch Instances**. The instance is launched and the AWS console displays the instance ID(s).

Note: Depending on the software you are running, instance(s) may take a few minutes to launch.



18 If you have not fully configured the inbound and outbound ports, click **Manage security groups**.

19 Select your security group's **Group ID** and edit the **Inbound** and **Outbound** tabs so that they reflect the table below.



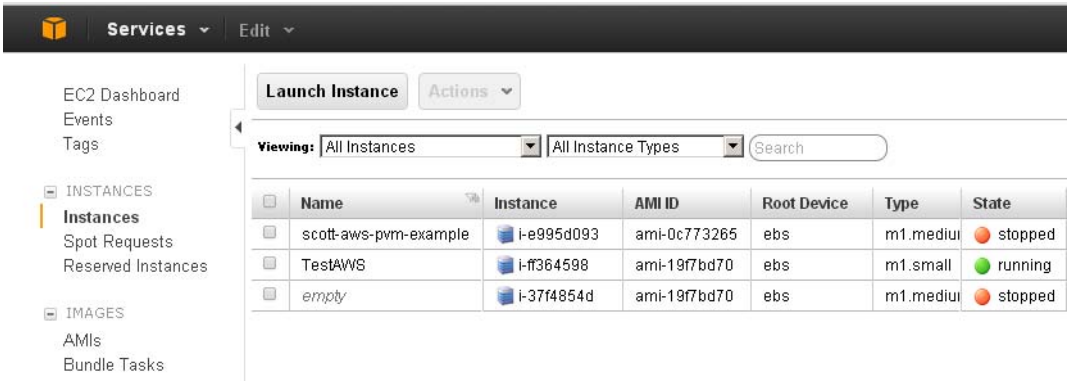
The following table shows the recommended ports/services for inbound and outbound rules for different purposes.

Inbound			
Protocol	**Port/Service**	**Source**	**Purpose**
ICMP	echo request	0.0.0.0/0	Connectivity
	echo reply	0.0.0.0/0	
TCP	22	0.0.0.0/0	SSH (CLI admin)
	5696	0.0.0.0/0	KMIP Server
	9000	0.0.0.0/0	NAE-XML
	9001	0.0.0.0/0	Cluster
	9080	0.0.0.0/0	Health Check
	9081	0.0.0.0/0	FIPS Status
	9443	0.0.0.0/0	Web Admin
	9656	0.0.0.0/0	KMIP Agent acceptor
UDP	161	0.0.0.0/0	SNMP agent

Outbound			
Protocol	**Port/Service**	**Destination**	**Purpose**
ICMP	ALL	0.0.0.0/0	Connectivity
TCP	20	0.0.0.0/0	FTP data
	21	0.0.0.0/0	FTP control
	22	0.0.0.0/0	SCP
	389	0.0.0.0/0	LDAP
	636	0.0.0.0/0	LDAP
	9001	0.0.0.0/0	Cluster
	1792	0.0.0.0/0	Cloud HSM
UDP	53	0.0.0.0/0	DNS
	123	0.0.0.0/0	NTP
	162	0.0.0.0/0	SNMP Traps
	514	0.0.0.0/0	Syslog

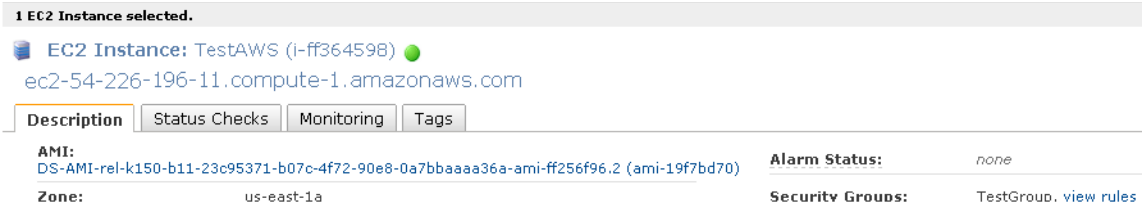
20 Click **Apply Rule Changes** on both the **Inbound** and **Outbound** tabs. Changes are propagated immediately.

21 Click **ECS Dashboard**. The EC2 Management Console is displayed showing all the available instances.



Wait until the **State** of the newly created instance changes from *pending* to **running**.

22 When the newly created instance is **running**, select the instance. The details of the selected instance appear at the bottom of the window.



23 Select and copy the IP address (or DNS name) under **EC2 Instance: <instance name>**. This document assumes the instance name as **TestAWS (i-ff364598)** and the IP address or DNS name as **ec2-54-226-196-11.compute-1.amazonaws.com**.

24 Try to connect to this IP address or DNS name using SSH, as described in “Connecting to Virtual KeySecure AWS Instance Using SSH” on page 10.

Connecting to Virtual KeySecure AWS Instance Using SSH

Connecting through SSH on Linux

Any Linux machine should be able to directly connect to this IP address or DNS name. Connect as the **dsuser**. The user **dsuser** is fixed. On Linux machine, execute: `ssh -i <key pair name.pem> dsuser@<copied IP address or DNS name>`

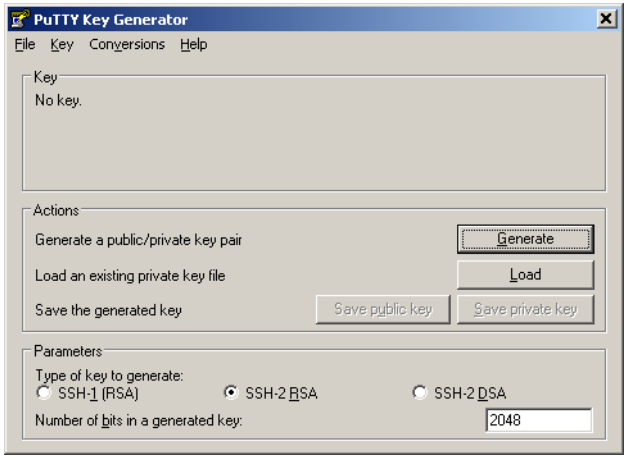
For example: `ssh -i AWSTestKey.pem dsuser@ec2-54-226-196-11.compute-1.amazonaws.com`

Connecting through SSH on Windows

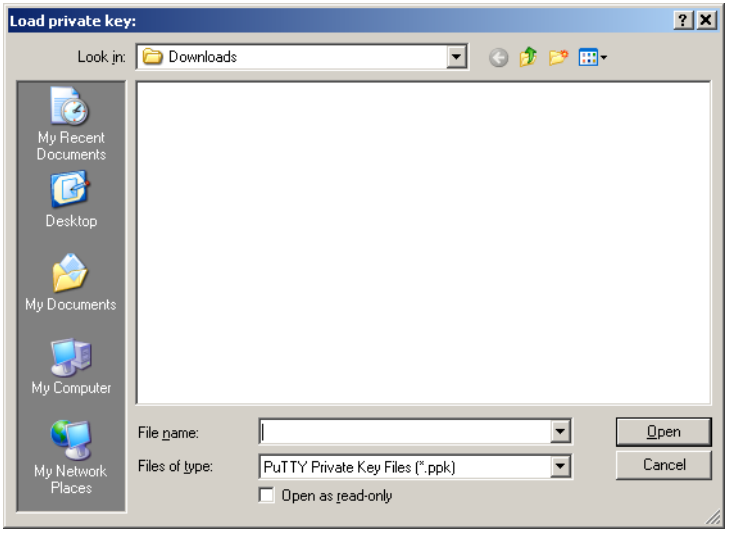
To use PuTTY for SSH connectivity on Windows, the key pair file (PEM file, in our case, `AWSTestKey.pem`) must be converted into a PPK file. This can be done by using the PuTTY Key Generator tool.

Converting PEM Key Pair File into PPK File

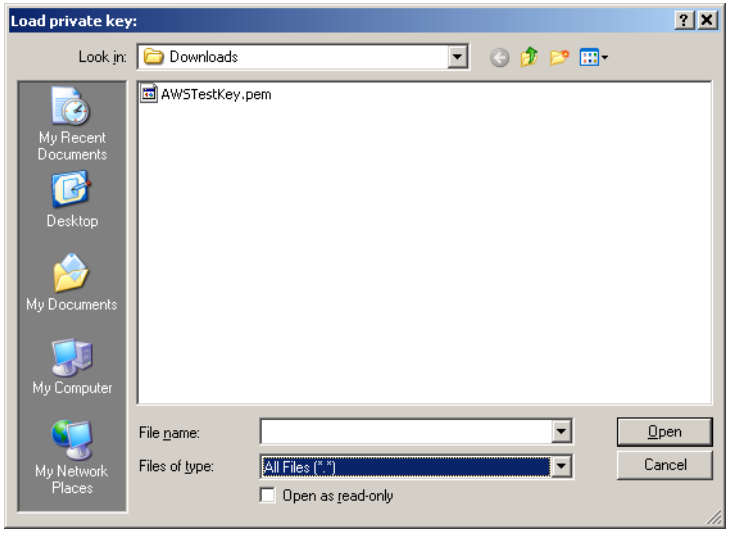
1 Run the PuTTY Key Generator tool.



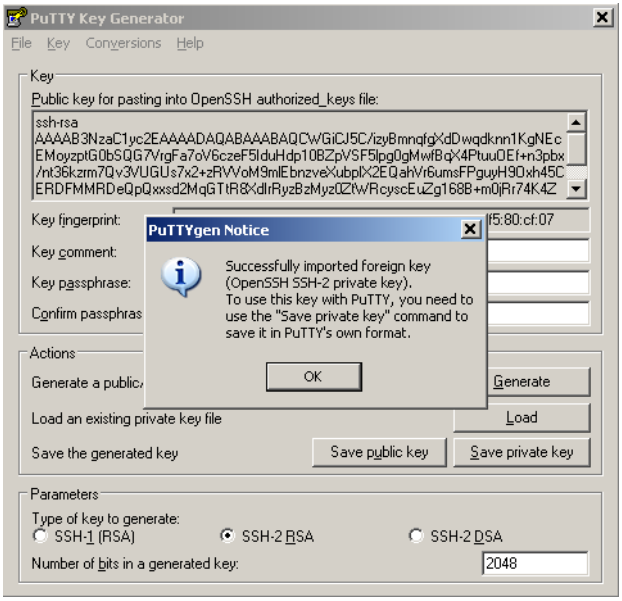
2 Click **Load**. The **Load private key** dialog box is displayed.



3 In the **Load private key:** dialog box, change **Files of type** to **All Files**.



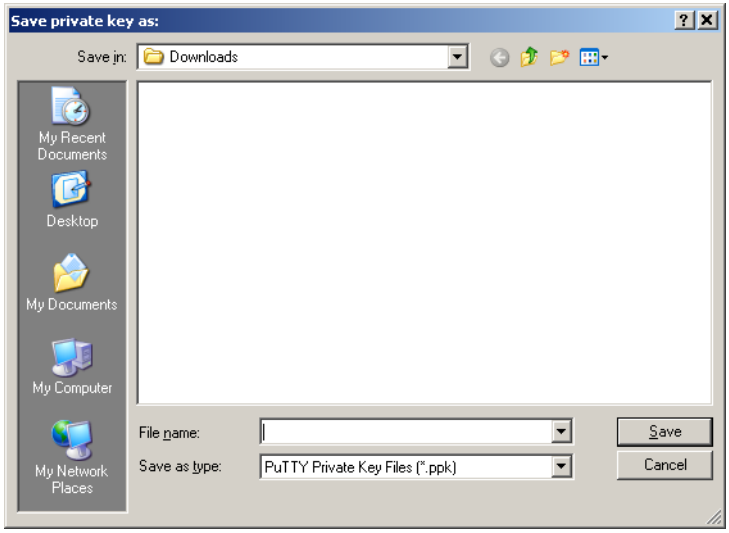
4 Open the downloaded key pair (PEM) file (in our case, **AWSTestKey.pem**).



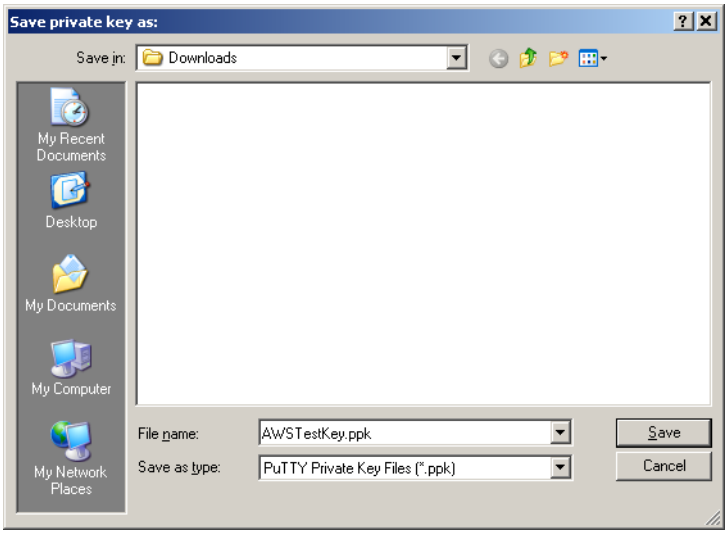
The key pair file is successfully converted to PuTTY's format (PPK).

5 Click **OK**.

6 Click **Save private key**. The **Save private key as:** dialog box is displayed.



7 Enter the original key pair file, but with **.ppk** extension. For example, **AWSTestKey.ppk**, in our case.



8 Click **Save**. The key pair file is saved as a **.ppk** file (**AWSTestKey.ppk**, in our case).

9 Close the PuTTY Key Generator tool.

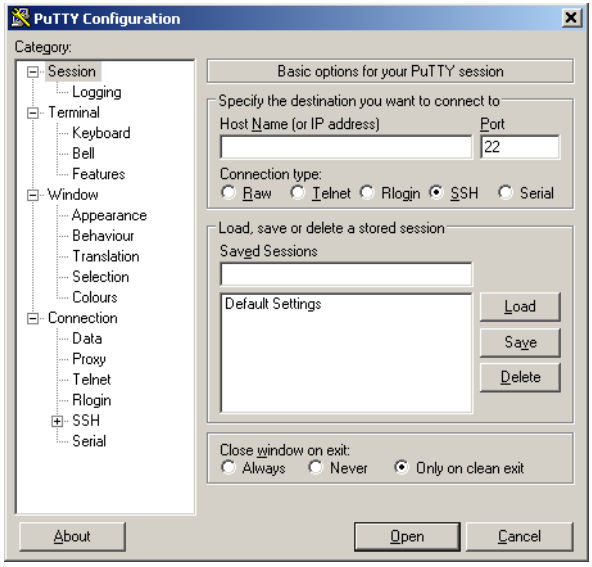
Adding First User from KeySecure Pre-boot Shell

When powered-up, a KeySecure instance will stop at the SSH Pre-boot Login Shell and wait for a pre-boot authentication to allow the user to launch KeySecure.

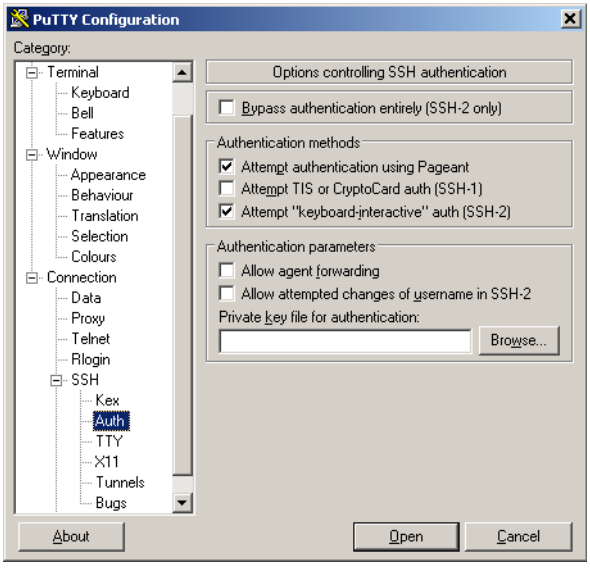
Prior to the boot, you will need to perform a set of setup steps (which includes adding users) described in this section, which will allow you to ultimately launch KeySecure.

1 Run the PuTTY Configuration tool.

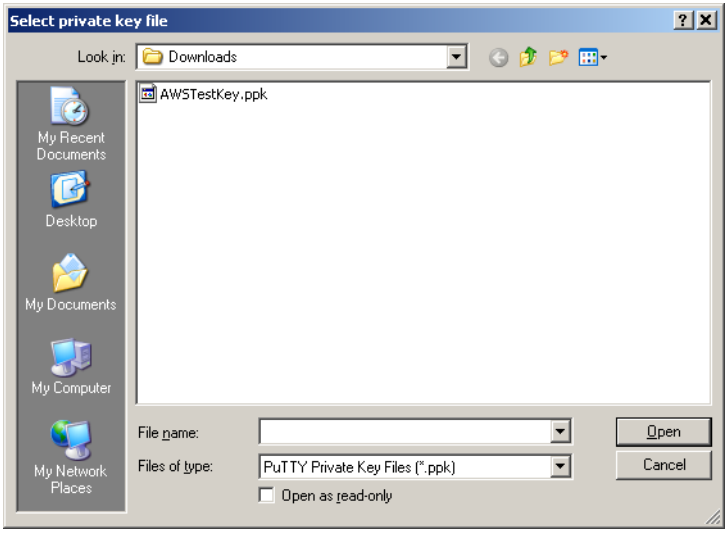
2 In the left pane, expand **SSH** under Connection.



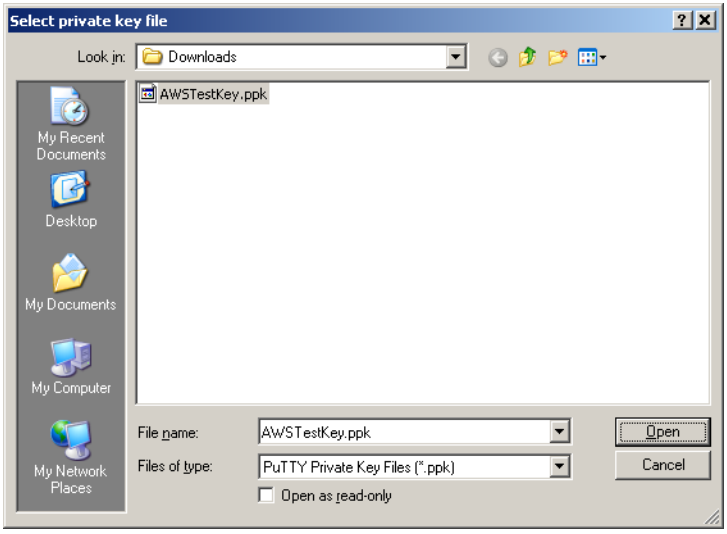
3 Click **Auth**.



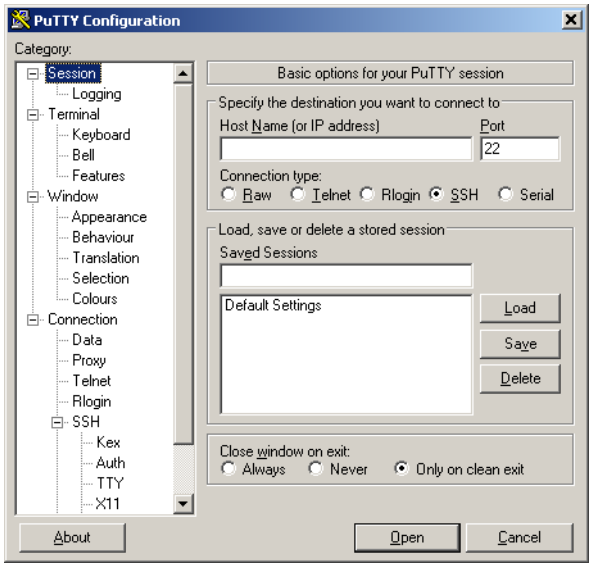
4 Click **Browse**.



5 Open the newly converted key pair (**.ppk**) file. In our case, the file name is **AWSTestKey.ppk**.

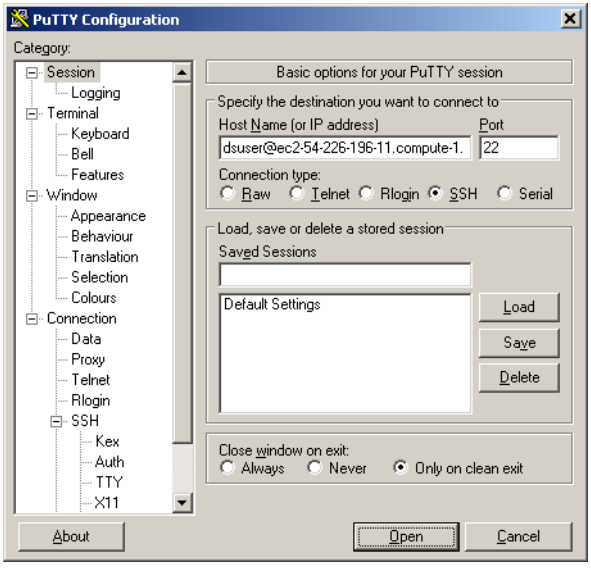


6 In the left pane, click **Session**.



7 Use SSH to connect to the launched and running KeySecure instance on port **22**, and use your AWS private key for authentication. Perform the following steps:

a Enter **dsuser@<copied IP address or DNS name>** in the **Host Name (or IP address)** field. For example, **dsuser@ec2-54-226-196-11.compute-1.amazonaws.com**. You must log on as **dsuser**. The user **dsuser** is fixed.



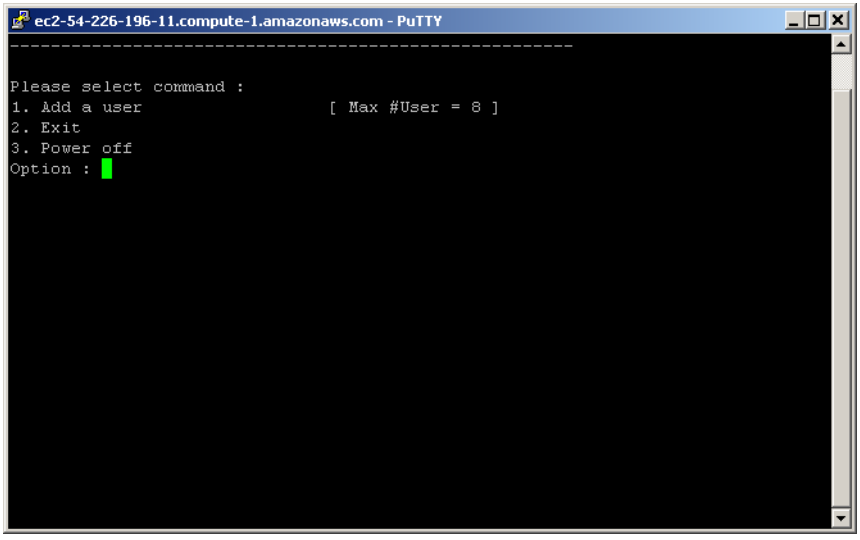
b Enter **22** in the **Port** field.

c Make sure **SSH** is selected as **Connection type**.

d Click **Open**.

Note: As the authentication is done using the downloaded PEM or PPK file, the user password is not required.

KeySecure's SSH Pre-boot Login Shell is displayed, as shown below.

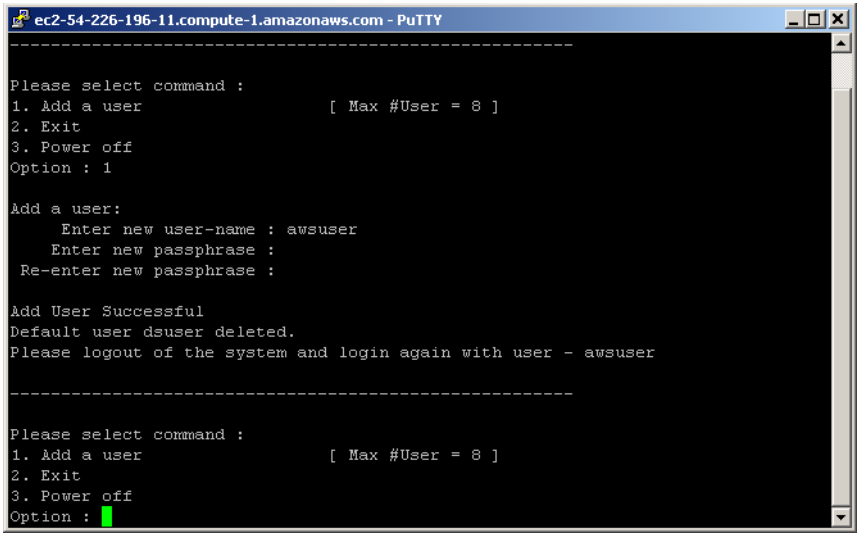


Note: Since this is the first time logging in, you are required to add at least one user to the system (up to 8 users can be added). Adding the first user takes approximately one minute.

8 Enter **1** to add a user.

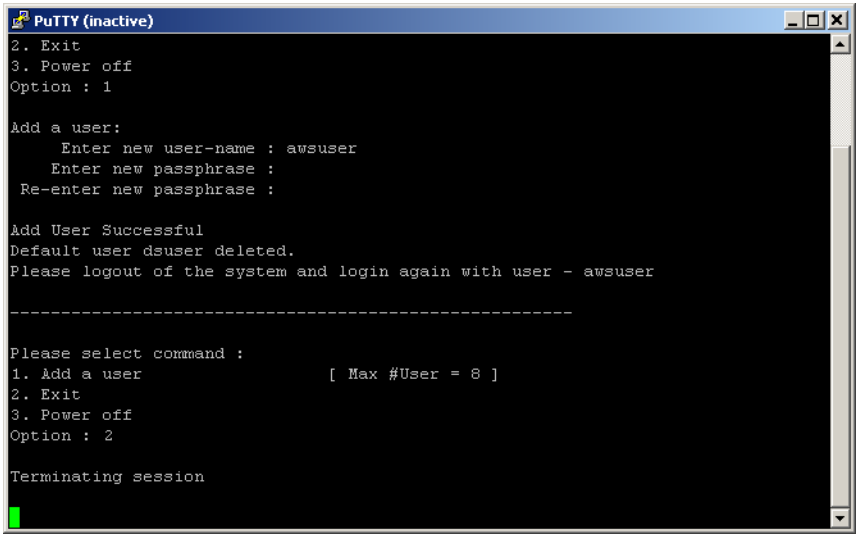
9 Specify name for the new user.

10 Enter and confirm the passphrase for the new user.



Note: The default user, **dsuser**, is used only to create new users. Due to security reasons, as soon as a new user is created, the default user, **dsuser,** gets deleted.

11 Enter **2** to terminate the session.

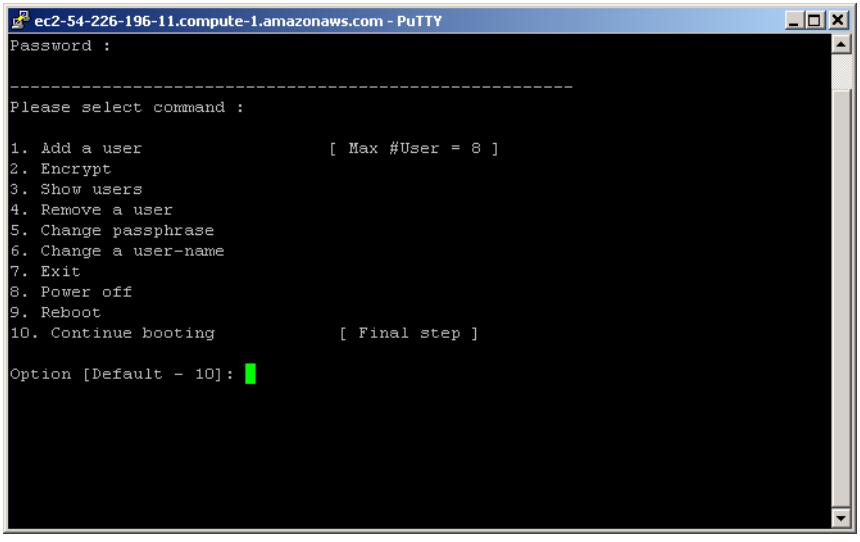


Terminating the session may take some time. Please wait.

Connecting as New User

1 As the new user (**awsuser**, in our case), connect to the IP address or DNS name. Follow steps 1 through 7 described above. See "Adding First User from KeySecure Pre-boot Shell".

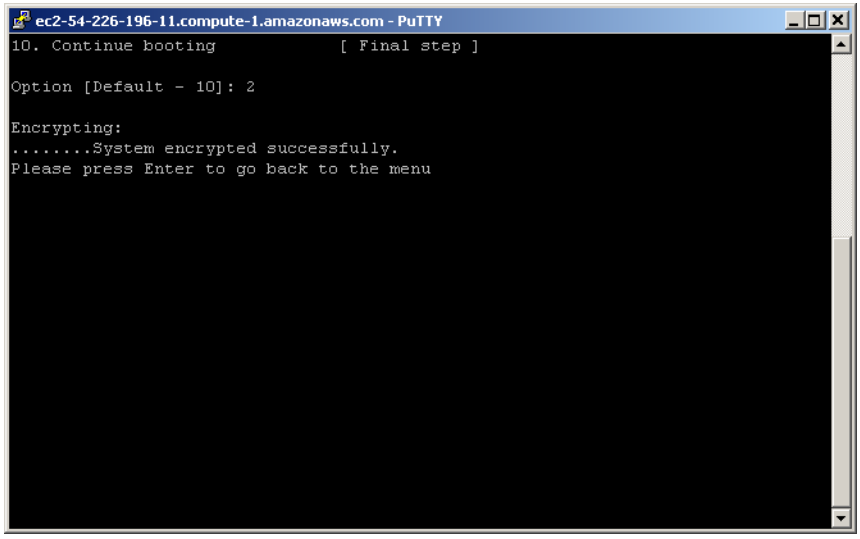
2 Enter password of the new user. The following menu is displayed:



Note: During the pre-boot setup, as the system is not yet encrypted, the system can't be booted. Therefore, the system must be encrypted before it can be booted for the first run.

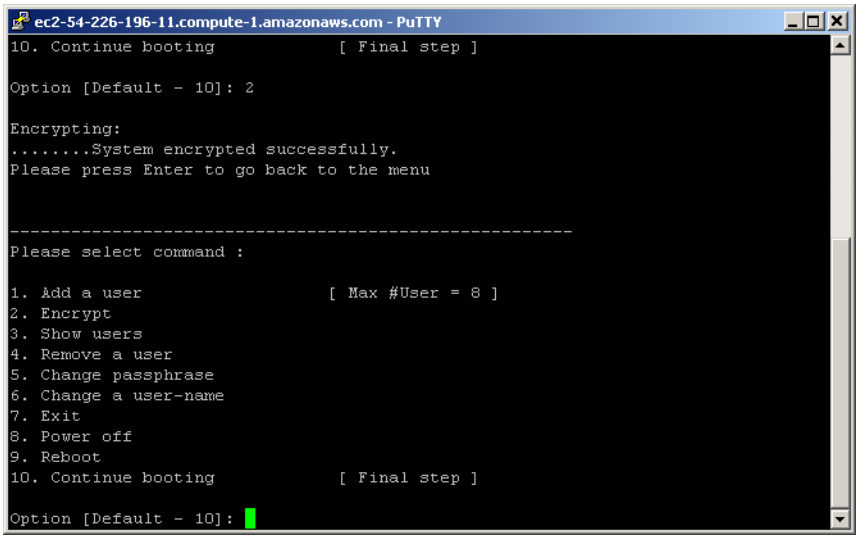
3 **Do not skip this step!** Enter **2** to encrypt the KeySecure instance. This mandatory step will protect the data stored in KeySecure. All the available partitions will be encrypted. The encrypt operation takes approximately 2 to 4 minutes, depending on the environment's performance. The progress is indicated by dots (. . .):

Important! The **add users** and **encryption** operations are not recoverable, if interrupted. Please do not disconnect or shutdown the instance during the encryption!

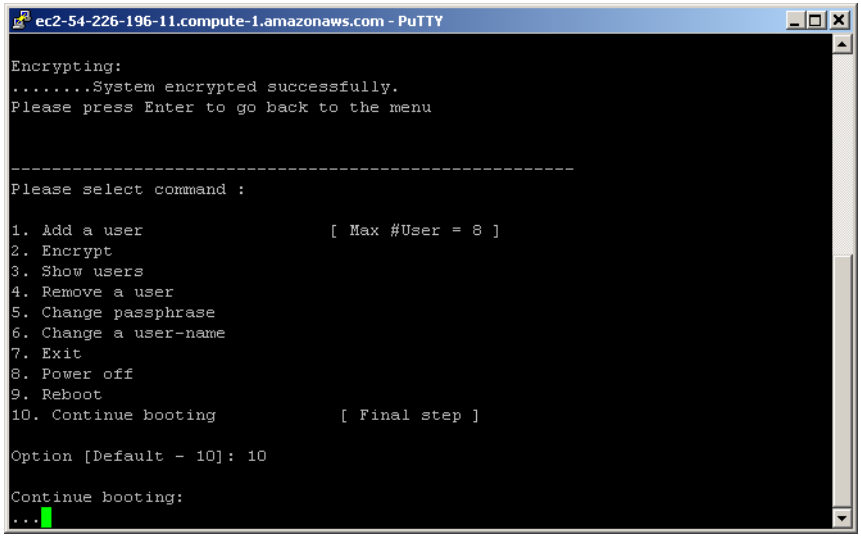


After successful encryption, if the KeySecure instance is rebooted/disconnected, the KeySecure instance will be ready to "boot" for the first run. You'll just need to connect as one of the newly created users to continue.

4 Press **Enter** to return to the menu.



5 Enter **10** to continue booting.



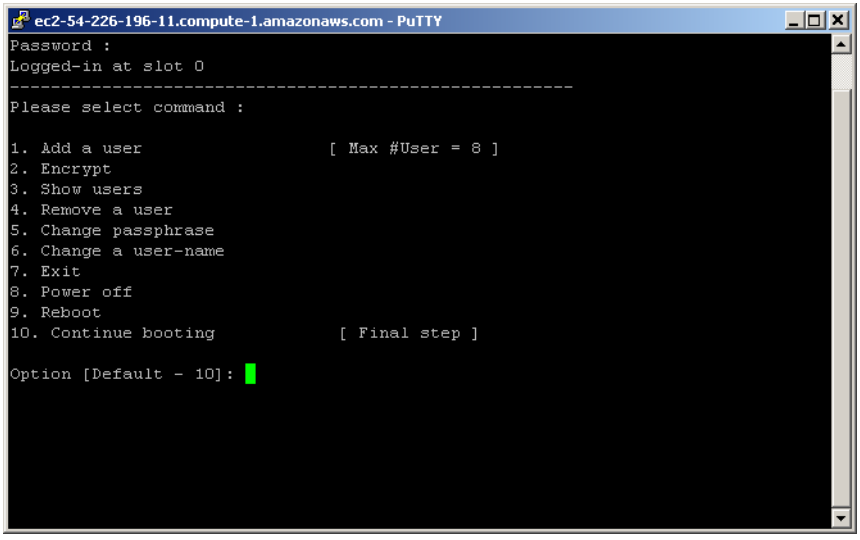
Booting may take some time. Please wait.

KeySecure Initial Setup and First Run

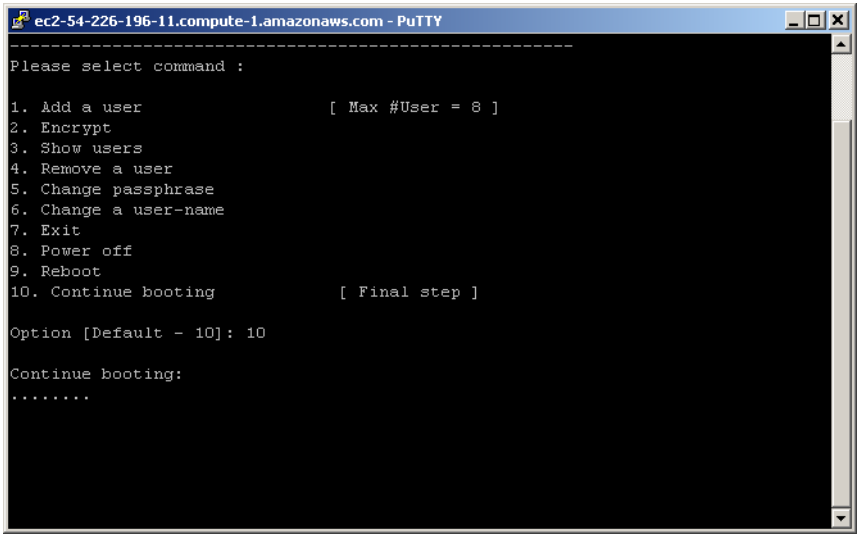
After the "**Continue booting**" step above, the PuTTY session will be automatically closed. The system is not yet fully setup. The KeySecure is being initialized in the background. This may take up to 10 - 15 minutes. Please be patient. The progress can be seen in the instance's System Log, by right-clicking the selected instance and selecting **Get System Log**. However, the logs appear very delayed. Keep trying to connect as the new user. As soon as the KeySecure is initialized, the users can log on to it.

1 As a new user (**awsuser**, in our case), connect to the IP address or DNS name. Follow steps 1 through 7 described above. See "Adding First User from KeySecure Pre-boot Shell".

2 Enter password of the new user. The following menu is displayed:

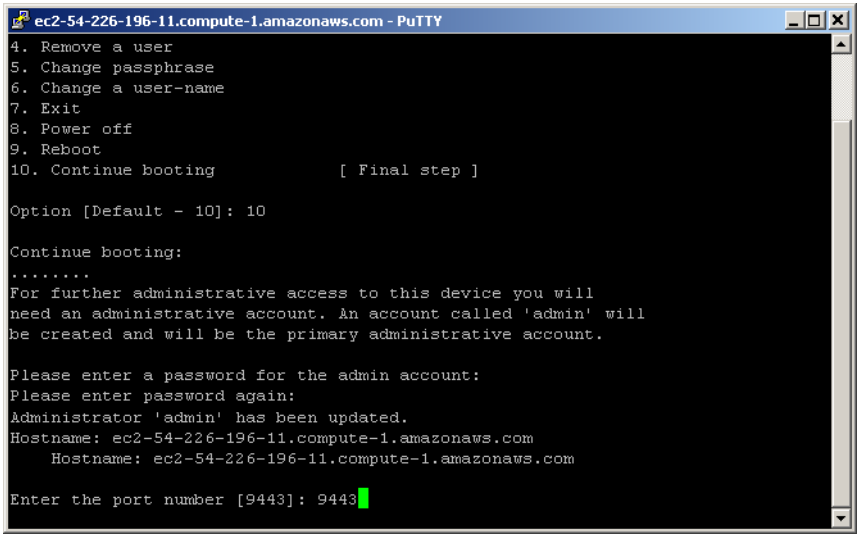


3 Enter **10** to continue booting.



Booting may take some time. Please wait.

4 Enter password for the KeySecure's "**admin**" user, hostname, and port, when prompted.



The KeySecure is now configured and ready to use. Once the KeySecure is booted up, then the KeySecure's runtime services are started, allowing access to KeySecure's API, CLI, and GUI.

Connecting to KeySecure

After KeySecure booting, you can login through SSH using the "**admin**" user name and password. Also, you can access KeySecure UI through Web.

Connecting to KeySecure Using CLI

To access virtual KeySecure through CLI, connect to the KeySecure's IP address or DNS name as KeySecure's "**admin**" user (not as pre-boot user) using SSH.

Connecting to KeySecure Using Management Console

To connect to KeySecure through Management Console:

1. Browse `https://<IP address or DNS name>:<port>`. For example, `https://ec2-54-226-196-11.compute-1.amazonaws.com:9443`
2. Log on to KeySecure using KeySecure's "**admin**" credentials.

Chapter 2

Storing Master Key on AWS CloudHSM

This chapter describes instructions to set up and configure the AWS CloudHSM (referred to as CloudHSM in this document).

After receiving an instance of the CloudHSM, you need to set it up. Once the CloudHSM is set up, you can configure it to use with Virtual KeySecure.

Note:

- The CloudHSM is an enhanced security option. This is not mandatory.
- AWS network parameters are configured dynamically through DHCP. Executing commands to edit these parameters result in the following message: `Error: Network setup commands are not supported for this platform`
- Management Console (GUI) also does not allow editing of AWS network parameters.

To set up and configure the CloudHSM, perform the following steps:

1. Setting Up CloudHSM
2. Registering CloudHSM with Virtual KeySecure
3. Registering Virtual KeySecure with CloudHSM
4. Verifying Virtual KeySecure Registration with CloudHSM
5. Logging On to CloudHSM Partition as Crypto User from Virtual KeySecure
6. Viewing CloudHSM Objects from Virtual KeySecure
7. Logging Out from CloudHSM Partition as Crypto User from Virtual KeySecure
8. Unregistering CloudHSM from Virtual KeySecure

Setting Up CloudHSM

The CloudHSM needs to be set up before any Virtual KeySecure instance can use it. When you receive an instance of the CloudHSM, the following are provided:

- Subnet ID in which the CloudHSM is hosted.
- IP address of the CloudHSM (CloudHSM is accessible only from a VPC).
- Appliance “`admin`” name.
- Appliance “`admin`” password.

For example:

```
Subnet ID: subnet-318ba85a
IP (Private): 172.31.16.18
Appliance admin: manager
Appliance admin password: <**********>
```

Setting Up CloudHSM

Upon receiving an instance of the CloudHSM, the first step is to set it up.

To setup a CloudHSM:

1. Log on to the CloudHSM as Appliance "admin" through ssh. For example:

```
ssh manager@172.31.16.18
manager@172.31.16.18's password:
Last login: Wed Oct  2 22:42:15 2013 from 10.0.0.67
Luna SA 5.1.0-25 Command Line Shell - Copyright (c) 2001-2011 SafeNet, Inc.
All rights reserved.
[hsmaas-hsm2103.dub2] lunash:>
```

2. Initialize the CloudHSM.

   Perform the following steps:

   a. Execute the following command at the lunash prompt: `hsm -init -label myLuna`

   b. Enter and confirm password for the Security Officer's login.

   c. Press **Enter** when prompted for cloning domain.

   d. Type **proceed** to initialize the HSM.

   Sample output:

```
lunash:> hsm -init -label myLuna
> Please enter a password for the security officer
> ********
Please re-enter password to confirm:
> ********
Please enter the cloning domain to use for initializing this
HSM (press <enter> to use the default domain):
> <Press enter here>

CAUTION:  Are you sure you wish to re-initialize this HSM?
```

```
All partitions and data will be erased.
Type 'proceed' to initialize the HSM, or 'quit'
to quit now.
>proceed
‘hsm - init’ successful.
```

Registering CloudHSM with Virtual KeySecure

Before a CloudHSM can be configured, it must be registered with the Virtual KeySecure. In addition, the Virtual KeySecure must also be registered with the CloudHSM.

First of all, connect to Virtual KeySecure through CLI in the configuration mode. To do so, execute the `configure` command.

For example:

```
DemoBox# configure
DemoBox (config)#
```

Checking Whether CloudHSM is Registered

To check whether the CloudHSM is already registered, execute the `show remote hsm settings` command from the KeySecure CLI. This command displays the CloudHSM configuration settings on a Virtual KeySecure.

Syntax: **`show remote hsm settings`**

For example:

```
DemoBox (config)# show remote hsm settings
Error: No remote HSM is registered
```

The output above shows that no CloudHSM is currently registered.

Registering CloudHSM

WARNING! Registering will DELETE ALL existing keys, certificates, and local CAs. Please take full system backup before proceeding with the command.

Important! It is recommended to follow the steps given below while registering/unregistering the CloudHSM with Virtual KeySecure; otherwise, you may lose your data.

1. Remove the device from the cluster (if part of a cluster).
2. Take full system backup.
3. Register/unregister the device.
4. Restore backup. This step is needed only if the device was not in a cluster before.

Note: If the device was in the cluster earlier, no need to restore backup, as cluster synchronization will synchronize it with other members.

5 Join the cluster again (if it was in the cluster before).

6 Synchronize with the cluster.

To register the CloudHSM with Virtual KeySecure, execute the `remote hsm register` command.

Syntax: **`remote hsm register`**

When prompted, please enter the CloudHSM's IP address or hostname and administrator password. Client certificate can be generated either IP address bound or hostname bound. Please ensure that the IP address used to generate certificate remains persistent across reboots.

For example:

```
DemoBox (config)# remote hsm register

                    WARNING
ALL EXISTING KEYS, CERTIFICATES, LOCAL CA AND KNOWN CA WILL BE LOST
PLEASE PROCEED ONLY IF YOU HAVE ALREADY TAKEN FULL BACKUP

Please enter "proceed" or anything else to cancel : proceed
Clearing old objects ..

Please enter:
HSM IP address/Hostname : 172.17.5.131
HSM admin login name : admin
HSM admin password :
Generate client certificate bound to IP address (y) or to hostname(n) ? ([y]/
n) :y
IP address(es) assigned to this host:
        [1] 172.17.3.249/255.255.255.0
IP address (172.17.3.249) will be set as Common Name(CN) in client certifi-
cate
Please make sure this machine always get the same IP address
Remote HSM registered successfully
Please also register this client with the remote HSM
```

Note: Once the CloudHSM has been registered, the Home page of Virtual KeySecure shows the CloudHSM status. The Home page also shows the crypto user login status.

Registering Virtual KeySecure with CloudHSM

At this stage, executing the `show remote hsm settings` command results the following output:

```
DemoBox (config)# show remote hsm settings
HSM IP/hostname          :       172.17.5.131
Error: This device is not registered with the remote HSM. Please register and
assign partition on the HSM
```

After the CloudHSM is registered, the Virtual KeySecure must also be registered with the CloudHSM. In addition, an empty partition must be created on the CloudHSM and assigned to the Virtual KeySecure.

Important! Create a new partition for every Virtual KeySecure instance or recycle the old partition, but only one Virtual KeySecure instance should be using it. Sharing a partition among Virtual KeySecure instances will lead to undefined results. Please make sure that each Virtual KeySecure instance gets its own partition.

To view the registered clients, the registered client details, and the partitions on the CloudHSM, execute the `client list`, `client show`, and `partition list` commands respectively. These commands are described in details below.

Viewing Registered Clients

To view clients (Virtual KeySecure instances) registered on the CloudHSM, execute `client list`. For example:

```
lunash:> client list

registered client 1: sk3_250
registered client 2: sk3_249

Command Result : 0 (Success)
```

The output shows that two clients "`sk3_250`" and "`sk3_249`" are currently registered.

Viewing Registered Client Details

To view the details of a registered client, execute `client show -c <Virtual_KeySecure_Name>`. For example:

```
lunash:> client show -c sk3_250

ClientID:     sk3_250
IPAddress:    172.17.3.250
Partitions:   "sk3_250"

Command Result : 0 (Success)
```

The output shows that the IP address "`172.17.3.250`" and a partition named "`sk3_250`" are assigned to the client "`sk3_250`". Make sure that the same partition (for example, "`sk3_250`") is not assigned to any other Virtual KeySecure instance.

Viewing Partitions

To view the list of partitions on the CloudHSM, execute the `partition list` command. For example:

```
lunash:> partition list

                                                        Storage (bytes)
                                                  ---------------------------
Partition    Name                        Objects     Total      Used       Free
==========================================================================================
156115009    sk3_250                           4      1024       508        516
156115012    sk3_249                           3      1024       380        644

Command Result : 0 (Success)
```

The output shows that two partitions named "`sk3_250`" and "`sk3_249`" are available on the CloudHSM.

Registering Virtual KeySecure

To register the Virtual KeySecure with the CloudHSM:

1. Log on as Security Officer using the password created in **Step 2b** of "Setting Up CloudHSM" on page 24.
2. Create an empty partition on the CloudHSM. A partition of 1 KB (1024 bytes) is recommended. The partition must be empty, that is, the partition must not contain any objects.

   For example, execute:

   ```
   lunash:> partition create -par partition_name -s 1024
   ```
3. Register the client (Virtual KeySecure) with the CloudHSM.

   For example, execute:

   ```
   lunash:> client register -c <Your_Virtual_KeySecure_Name> -ip 172.17.3.249
   ```
4. Assign the created partition to Virtual KeySecure.

   For example, execute:

   ```
   lunash:> client assignPartition -c 172.17.3.249 -par partition_name
   ```

Verifying Virtual KeySecure Registration with CloudHSM

After registering Virtual KeySecure with the CloudHSM, executing the `show remote hsm settings` command results the following output:

```
DemoBox (config)# show remote hsm settings
HSM IP/hostname          :       172.17.5.131
Client IP/hostname       :       172.17.3.249
Partition Label          :       partition_name
Partition Serial Number  :       156114020
Trust-link Status        :       Active
Login Status             :       Logged out
Certificate Fingerprint :
20:64:1F:B6:9D:A8:B9:88:B4:2B:73:CF:60:B5:10:53
Certificate :
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CA, ST=Ontario, L=Ottawa, O=My company, CN=172.17.3.249
        Validity
            Not Before: Sep  1 07:15:03 2013 GMT
            Not After : Aug 31 07:15:03 2023 GMT
        Subject: C=CA, ST=Ontario, L=Ottawa, O=My company, CN=172.17.3.249
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:a7:19:9f:a1:a1:5e:8e:26:a6:82:94:24:b1:76:
                    26:fe:16:cb:57:72:6f:48:b3:80:af:4c:48:c4:92:
                    cd:ac:8d:8a:20:be:70:b5:84:5b:52:64:29:6c:ec:
                    33:49:59:0f:df:d3:cb:de:02:cc:73:10:9e:d6:99:
                    90:36:56:13:0f:1a:9b:d7:9c:2f:79:ab:08:28:ca:
                    8f:ae:62:aa:31:7b:bd:1e:b2:0a:28:72:84:04:21:
                    40:c6:ec:c7:98:2d:e0:00:95:12:6e:40:1d:47:a1:
                    c7:ab:b0:54:ad:91:1c:76:24:28:43:94:48:a6:7e:
```

```
                    00:a6:84:8d:8b:06:2b:1b:fc:91:75:20:2c:15:b2:
                    22:1e:55:7d:1e:0f:17:51:fb:33:17:c7:7f:20:c5:
                    4f:c4:dd:62:74:9d:fe:70:a0:85:d2:4f:37:66:fb:
                    e1:36:1b:57:c7:1b:4d:6e:92:86:89:98:c1:99:b7:
                    e5:23:98:cc:6f:6c:b0:56:f5:7d:48:d1:98:49:70:
                    ef:d2:83:2e:cc:25:8d:bc:8c:ab:2f:04:f7:89:0d:
                    84:bd:d2:ba:6d:00:fa:91:33:fe:64:1e:38:a9:a8:
                    58:a5:64:53:4f:99:57:d7:28:bb:f4:d0:d2:bf:71:
                    b0:13:ad:53:d7:25:48:7d:e1:37:3d:32:97:a1:35:
                    2c:53
                Exponent: 65537 (0x10001)
        Signature Algorithm: sha256WithRSAEncryption
            4b:72:bd:ea:95:33:3d:a5:45:fc:a8:00:d9:5a:39:5c:8b:44:
            ca:ec:91:09:f1:90:48:13:19:18:db:81:22:2a:7f:05:50:79:
            f2:47:71:96:9a:fe:0e:d1:22:6e:1e:67:6d:1c:f8:fd:68:ac:
            e9:28:88:6d:d1:89:87:77:ca:75:7e:9d:e5:f6:c1:2f:d8:a7:
            f6:9d:9c:94:04:11:c8:c5:a5:e4:b5:28:14:15:e6:92:a5:c4:
            21:78:ff:28:27:be:27:7b:69:47:97:af:99:f2:be:f5:f6:c5:
            ad:24:45:44:a4:a8:c0:bf:a2:07:c9:ef:da:c4:bd:cc:93:b9:
            b5:64:7c:6e:a3:44:bb:85:9e:80:e3:d4:9a:f7:b8:16:43:15:
            a2:1b:bc:6d:95:83:ef:05:b6:ff:b8:11:d3:f9:71:c2:fb:eb:
            a1:35:e3:18:3c:f2:8a:58:a6:5f:09:51:89:07:d2:99:cd:bd:
            07:6a:44:dd:e3:c1:df:09:91:e9:ed:aa:ab:aa:8e:21:d6:41:
            40:70:8c:b2:3f:b3:0f:68:31:43:98:e3:86:94:29:bb:00:6a:
            54:f8:9b:55:0b:85:8e:d6:0c:bb:0b:02:42:db:82:7a:7a:8c:
            24:85:5c:5d:29:1d:c4:a4:7f:fe:48:79:1c:dd:e0:87:1d:d7:
            5c:a6:44:66
```

In the above output:

- **HSM IP/hostname:** IP address or hostname for the CloudHSM.
- **Client IP/hostname:** IP address or hostname for the Virtual KeySecure. KeySecure is a client to the CloudHSM.
- **Partition Label:** Label assigned to the partition.
- **Partition Serial Number:** Serial number for the partition.

- **Trust-link Status:** Status of the connection between the Virtual KeySecure and the CloudHSM. **Active** trust-link signifies that KeySecure and the CloudHSM can communicate securely. **Inactive** status indicates the loss of network connectivity or certificate expiry between KeySecure and the CloudHSM.
- **Login Status:** Crypto user login status for the CloudHSM.
- **Certificate Fingerprint:** Fingerprint of the certificate.

Logging On to CloudHSM Partition as Crypto User from Virtual KeySecure

After configuration, the crypto user needs to log on to the CloudHSM from Virtual KeySecure to perform operations. All operations involving keys, certificates and local CA, such as creation, backup, restore, and clustering, are possible only if the crypto user is logged on to the CloudHSM and the Virtual KeySecure is functioning properly.

To log on to the CloudHSM as crypto user, execute the `remote hsm login crypto user` command from Virtual KeySecure.

Syntax: **`remote hsm login crypto user`**

For example:

```
DemoBox (config)# remote hsm login crypto user
Enter passphrase :
Logged in successfully to remote HSM partition
```

Viewing CloudHSM Objects from Virtual KeySecure

To list the CloudHSM objects, execute the `show remote hsm objects` command from Virtual KeySecure.

Syntax: **`show remote hsm objects`**

For example:

```
DemoBox (config)# show remote hsm objects
Number of objects in HSM partition/token = 4
        Object Labels:
                cert
                naesymm
                localca
                naeasymm
```

Logging Out from CloudHSM Partition as Crypto User from Virtual KeySecure

After performing operations, the crypto user can log out from the CloudHSM. When the user is logged out, the Virtual KeySecure is locked out, and operations such as key creation, certificates and local CA creation, backup, and replication are not possible.

To log out as the crypto user from the CloudHSM, execute the `remote hsm logout crypto user` command from Virtual KeySecure.

Syntax: **`remote hsm logout crypto user`**

For example:

```
DemoBox (config)# remote hsm logout crypto user
Warning: All key operations will not function if Crypto User is logged-out
Proceed ? (y/[n]) : y
Logged out successfully from remote HSM partition
```

Unregistering CloudHSM from Virtual KeySecure

Before unregistering the CloudHSM, remove it from the cluster. For recommended steps to unregister the CloudHSM, refer to the `remote hsm register` command **here** under “Registering CloudHSM” on page 25.

WARNING!

- Do not unregister a CloudHSM unless you have decided not to use the CloudHSM.
- Unregistering will DELETE ALL existing keys, certificates, and local CAs. Please take full system backup before proceeding with the command.

To unregister a CloudHSM from the Virtual KeySecure, execute the `remote hsm unregister` command.

Syntax: **`remote hsm unregister`**

For example:

```
DemoBox (config)# remote hsm unregister
                    WARNING
ALL EXISTING KEYS, CERTIFICATES AND LOCAL CAs, WILL BE LOST
PLEASE PROCEED ONLY IF YOU HAVE ALREADY TAKEN FULL BACKUP
(Crypto User must be logged-in for taking backup)

Type "proceed" or anything else to cancel : proceed
```

```
Restarting services ..
Clearing old objects ..
HSM unregistered successfully
Please also unregister this client from the HSM
DemoBox (config)# show remote hsm settings
Error: No remote HSM is registered
```

Note: After unregistering the CloudHSM from Virtual KeySecure, delete the client from the CloudHSM by executing: `client delete -c <client>`.