SafeNet | THE DATA PROTECTION COMPANY

ProtectV

TECHNICAL INSTRUCTIONS

Launch and Configure SafeNet ProtectV in AWS Marketplace

Contents

Overview

You've purchased the SafeNet ProtectV AMI from AWS Marketplace. What's the next step?

The workflow of this document defines the configuration prerequisites that are required before you can launch the ProtectV AMI from your AWS account. It also provides the tools you'll need to utilize your existing SSH keys to log in to encrypt and boot up the ProtectV Manager instance.

Prerequisites

Before you launch the ProtectV AMI, make sure you have completed the tasks outlined in this section.

- Make sure that you have access to and login credentials for SafeNet's Technical Support Customer Portal site at https://serviceportal.safenet-inc.com, so you can get support for the product.
- Make sure that you have access to these documents:
  - *ProtectV Installation Guide*
    http://www2.safenet-inc.com/aws-marketplace/usage/protectv/uploadedFiles/Support_and_Downloads/AWS/007-011532-001-protectv-aws-install-guide-v1.6.0.pdf
  - *KeySecure User Guide*
    http://www2.safenet-inc.com/aws-marketplace/usage/vks/uploadedFiles/Support_and_Downloads/AWS/007-012362-001-keysecure-appliance-user-guide-v7.1.0.pdf
  - *Virtual KeySecure in AWS Marketplace Installation Guide*
    http://www2.safenet-inc.com/aws-marketplace/usage/vks/uploadedFiles/Support_and_Downloads/AWS/007-012368-001-ks-aws-install-guide-v7.1.0.pdf
  - Quick start documentation included with the device
- Configure KeySecure — Use KeySecure version 6.1.2 or higher.
  - If you currently do not have a KeySecure and would like to purchase Virtual KeySecure from AWS Marketplace, please visit the following URL for pricing and more information: https://aws.amazon.com/marketplace/pp/B00FG6USBY
  - If you currently do not have a KeySecure and would like to purchase a physical KeySecure from SafeNet (it is not part of the offering on AWS Marketplace), please visit the following URL for details about the physical KeySecure and how to contact our Sales team: http://www.safenet-inc.com/data-protection/key-management/key-secure/
- Configure the Firewall Settings (for Linux clients only)
- Create Security Groups

Configure KeySecure

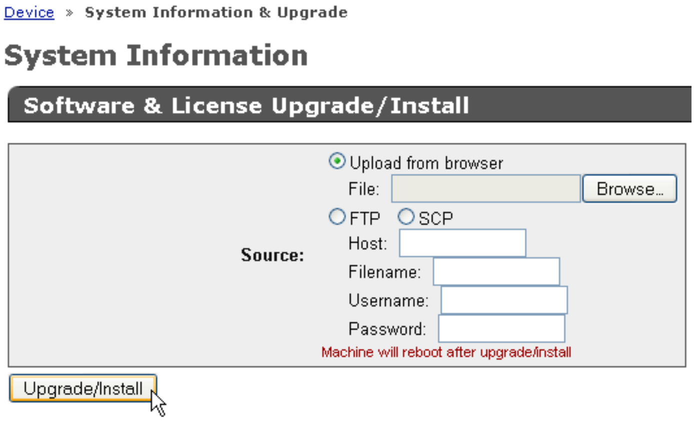
This section assumes that you have already completed the installation of your virtual or physical KeySecure.

You must complete the procedures in this section on the KeySecure device before you can launch and configure the ProtectV AMI. (You will be prompted to enter valid KeySecure settings during the ProtectV configuration.)

NOTES:

- To perform cryptographic operations, ProtectV Manager needs to export the encryption key. If the KeySecure device is configured for FIPS compliance, please be advised that key export will not be allowed over a TCP connection. This would cause the encryption/decryption operation to fail. For ProtectV to work in FIPS mode, SSL must be set up to allow key export.
- To ensure there is no SSL/TCP mismatch between the KeySecure device and ProtectV Manager, verify the protocol on the KeySecure server, go to the **Device** tab > **KeyServer**, and view the NAE-XML properties. If **Use SSL** is selected, the device is configured to use SSL.
- If the KeySecure device is already set for SSL and you decide to turn on FIPS mode later, you must edit the NAE-XML properties and enable the **Allow Key** and enable **Allow Key Export and Allow Key and Policy Configuration Operations** properties.

1. Set up the KeySecure device in the network. Please refer to the *KeySecure Quick Start Guide* for details.
2. Complete the following installation and configuration procedures. Where noted in parentheses, please refer to that section in the *KeySecure User Guide* for details.
   - **Obtain the software license from SafeNet and install it.** (see "*Install Software Licenses*")



Device » System Information & Upgrade

System Information

Software & License Upgrade/Install

Source: ● Upload from browser

File: [Browse...]

○ FTP ○ SCP

Host:

Filename:

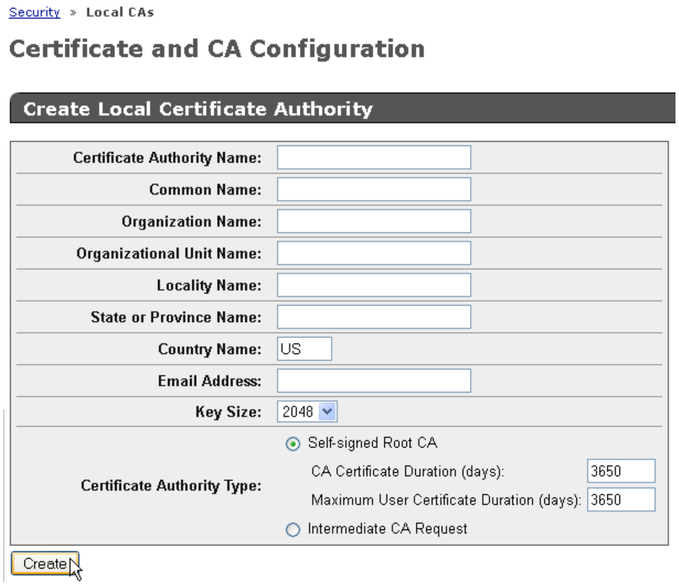
Username:

Password:

Machine will reboot after upgrade/install

[Upgrade/Install]

- **Configure SSL.** These procedures are required only if you are using an SSL connection between KeySecure and ProtectV. Before the KeySecure can respond to SSL requests from ProtectV Manager, the KeySecure must be configured with at least one server certificate.
    - **Create a Local Certificate Authority on KeySecure.** (see "*Create a Local Certificate Authority*")

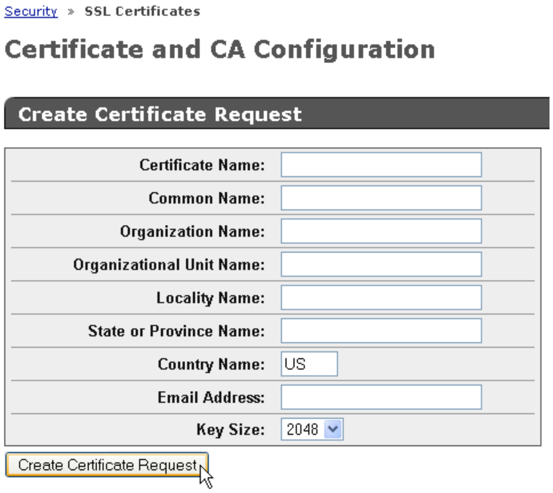


Certificate and CA Configuration

Create Local Certificate Authority

Certificate Authority Name:	
Common Name:	
Organization Name:	
Organizational Unit Name:	
Locality Name:	
State or Province Name:	
Country Name:	US
Email Address:	
Key Size:	2048
Certificate Authority Type:	● Self-signed Root CA CA Certificate Duration (days): 3650 Maximum User Certificate Duration (days): 3650 ○ Intermediate CA Request

- **Create a Server Certificate signed by the Local CA**. (see "*Creating a Server Certificate for the KeySecure*")

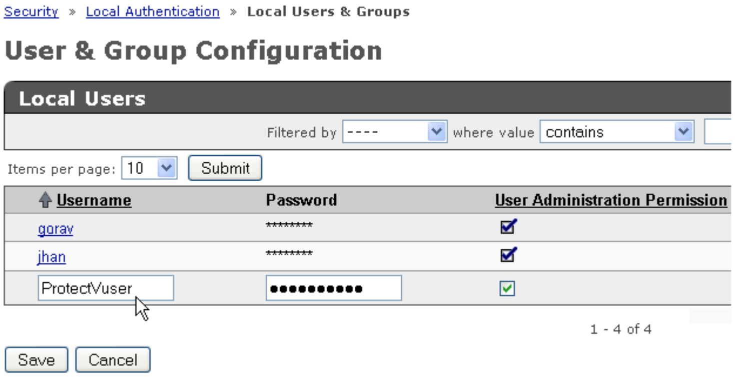


Certificate and CA Configuration

Create Certificate Request

Certificate Name:	
Common Name:	
Organization Name:	
Organizational Unit Name:	
Locality Name:	
State or Province Name:	
Country Name:	US
Email Address:	
Key Size:	2048

- **Create a Local user on the KeySecure.** *(see "Create a Local User")*



Security » Local Authentication » Local Users & Groups

User & Group Configuration

Local Users

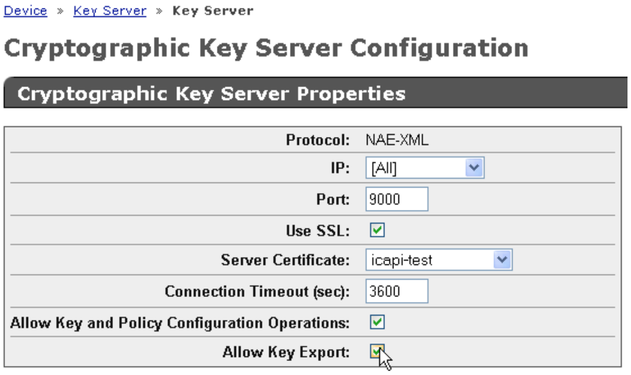
Filtered by ---- where value contains

Items per page: 10 Submit

Username	Password	User Administration Permission
gorav	********	☑
jhan	********	☑
ProtectVuser	●●●●●●●●●●●	☑

1 - 4 of 4

- **Enable Key Export on the KeySecure.** (see steps below)



Device » Key Server » Key Server

Cryptographic Key Server Configuration

Cryptographic Key Server Properties

Protocol:	NAE-XML
IP:	[All]
Port:	9000
Use SSL:	☑
Server Certificate:	icapi-test
Connection Timeout (sec):	3600
Allow Key and Policy Configuration Operations:	☑
Allow Key Export:	☑

  - Log in to the KeySecure Management Console with administrative access.
  - Go to **Device** tab > **KeyServer**.
  - Go to **NAE-XML** properties and click **Edit**.
  - Select **Allow key export**. Save the changes.

Configure the Firewall (for Linux Clients Only)

Make sure the following ports are open for ProtectV Linux clients:

- 22 - SSH
- 9090 – SC/TCP
- 9093 – SC/SSL

Use the *system-config-securitylevel-tui* tool to set basic firewall rules. For example:

1. SSH to the client.
2. Open ports 9090 and 9093 for TCP in the firewall. For example, for RHEL/CentOS 5.x distributions, use the following command: *system-config-securitylevel-tui -q -p 9090:tcp -p 9093:tcp*
3. For other distributions, consult your system firewall documentation.

Create Security Groups

We recommend that you create three AWS security groups: one for ProtectV Manager servers, one for Linux clients, and one for Windows clients.

If you need assistance adding security groups, please refer to the Amazon Web Services documentation at http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html.

ProtectV Manager Security Group

Add these ports for the ProtectV Manager security group:

- 22 - SSH
- 443 - HTTPS
- 5984 – HA/Replication/TCP
- 6984 – HA/Replication/SSL
- 7080 – HA/SOAP
- 8080 – PVM/SOAP
- 9000 – Default KeySecure NAE_XML
- 9090 – SC/TCP
- 9093 – SC/SSL

Linux Server Security Group

Add these ports for the Linux server security group. Please make sure you limit the **Source** field to the ProtectV Manager security group.

- 22 - SSH
- 9090 – SC/TCP
- 9093 – SC/SSL

Windows Server Security Group

Add these ports for the Windows server security group. Please make sure you limit the **Source** field to the ProtectV Manager security group.

- 3389 – RDP
- 9090 – SC/TCP
- 9093 – SC/SSL

NOTE: After you have installed the Windows ProtectV Client, note that ProtectV Thrift Inbound and Outbound rules are automatically created in the Windows firewall. These rules are used for ProtectV communications.

Supported Platforms

The following table presents the virtualized server platforms that currently support ProtectV in an AWS environment.

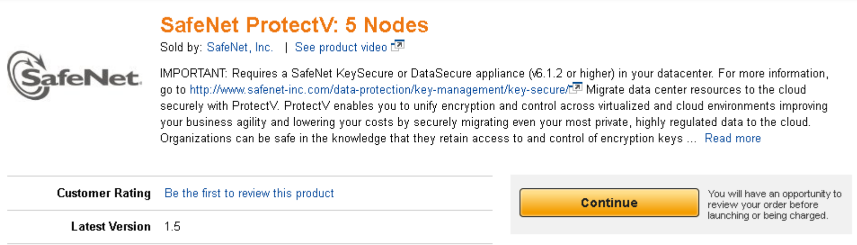
Please make sure you check this list before you perform the steps in Configure the ProtectV Client on page 21.

- Microsoft Windows Server 2003 R2 (32-bit), SP2
- Microsoft Windows Server 2003 R2 (64-bit), SP2
- Microsoft Windows Server 2008 (32-bit), SP2
- Microsoft Windows Server 2008 (64-bit), SP2
- Microsoft Windows Server 2008 R2 (64-bit), SP1
- Microsoft Windows Server 2012 (64-bit)
- CentOS Linux 6.2, 64-bit
- Red Hat Enterprise Linux (RHEL) 5.8, 64-bit
- Red Hat Enterprise Linux (RHEL) 6.2, 64-bit
- Red Hat Enterprise Linux (RHEL) 6.3, 64-bit

Launch and Configuration Procedures

In AWS Marketplace...

1. Log in to AWS Marketplace with your AWS Management Console account credentials.
2. Locate the instance by searching for the word, “ProtectV.” You will see a list of ProtectV AMI instances. Choose the one that matches your sizing needs.
3. Select the number of nodes (**SafeNet ProtectV: 5 Nodes**, **100 Nodes**, or **25 Nodes**), and then click **Continue**.



SafeNet ProtectV: 5 Nodes

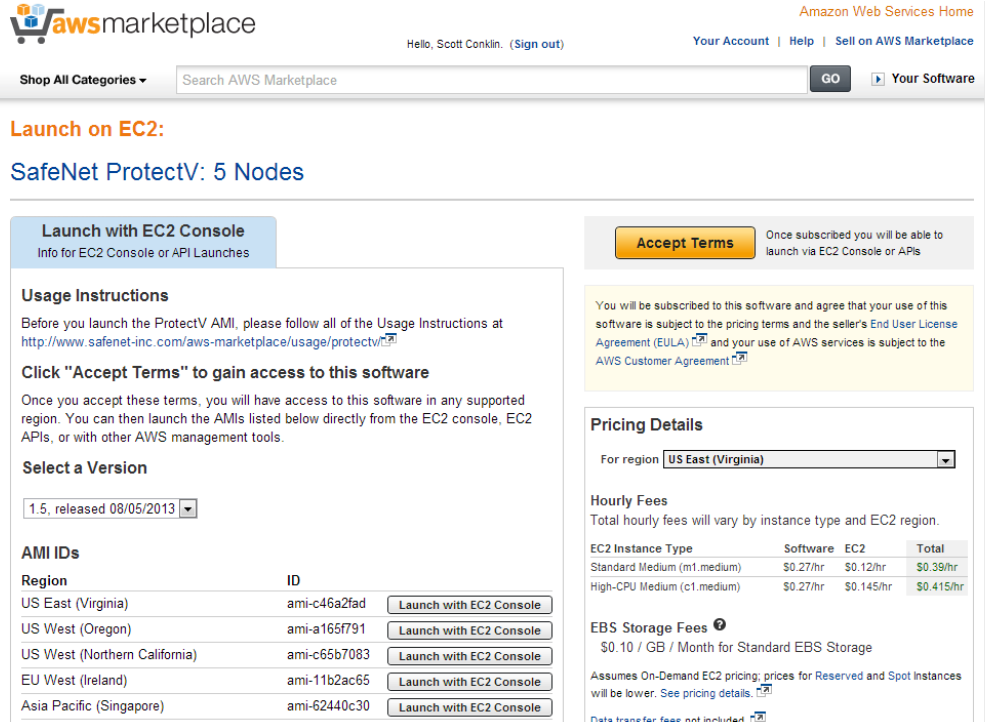
Sold by: SafeNet, Inc. | See product video

IMPORTANT: Requires a SafeNet KeySecure or DataSecure appliance (v6.1.2 or higher) in your datacenter. For more information, go to http://www.safenet-inc.com/data-protection/key-management/key-secure/ Migrate data center resources to the cloud securely with ProtectV. ProtectV enables you to unify encryption and control across virtualized and cloud environments improving your business agility and lowering your costs by securely migrating even your most private, highly regulated data to the cloud. Organizations can be safe in the knowledge that they retain access to and control of encryption keys ... Read more

Customer Rating	Be the first to review this product
Latest Version	1.5

You will have an opportunity to review your order before launching or being charged.

4. The AWS Marketplace launch page displays. Click **Accept Terms**. You cannot proceed until you do so.



Hello, Scott Conklin. (Sign out)

Launch on EC2:

SafeNet ProtectV: 5 Nodes

Launch with EC2 Console

Info for EC2 Console or API Launches

Usage Instructions

Before you launch the ProtectV AMI, please follow all of the Usage Instructions at http://www.safenet-inc.com/aws-marketplace/usage/protectv/

Click "Accept Terms" to gain access to this software

Once you accept these terms, you will have access to this software in any supported region. You can then launch the AMIs listed below directly from the EC2 console, EC2 APIs, or with other AWS management tools.

Select a Version

1.5, released 08/05/2013

AMI IDs

Region	ID	
US East (Virginia)	ami-c46a2fad	Launch with EC2 Console
US West (Oregon)	ami-a165f791	Launch with EC2 Console
US West (Northern California)	ami-c65b7083	Launch with EC2 Console
EU West (Ireland)	ami-11b2ac65	Launch with EC2 Console
Asia Pacific (Singapore)	ami-62440c30	Launch with EC2 Console

Once subscribed you will be able to launch via EC2 Console or APIs

You will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA) and your use of AWS services is subject to the AWS Customer Agreement

Pricing Details

For region: US East (Virginia)

Hourly Fees

Total hourly fees will vary by instance type and EC2 region.

EC2 Instance Type	Software	EC2	Total
Standard Medium (m1.medium)	$0.27/hr	$0.12/hr	$0.39/hr
High-CPU Medium (c1.medium)	$0.27/hr	$0.145/hr	$0.415/hr

EBS Storage Fees

$0.10 / GB / Month for Standard EBS Storage

Assumes On-Demand EC2 pricing; prices for Reserved and Spot Instances will be lower. See pricing details.

Data transfer fees not included

5. **Select a Version** of ProtectV from the drop-down menu.
6. Click **Launch with EC2 Console** adjacent to the Region/AMI ID you want to launch.

7. The **EC2 Console Wizard** launches. It will guide you through the remaining steps, including:

   - Selecting the AMI and configure the **Instance Details** pages (i.e., Instance Type - **use m1.medium or larger**, Availability Zone, Kernel ID, RAM Disk ID, Termination Protection, etc.).
   - Creating a key pair.

   > **NOTE:** On Linux, you will need to convert the PEM file to a PPK file in PuTTY for SSH connectivity.

   - Configuring the firewall by selecting the ProtectV Manager security group created earlier in the "ProtectV Manager Security Group" section. If you did not create a security group earlier, create one now by referring to page 6.
   - Launching the instance, and connecting to it with SSH, as described in the next section.

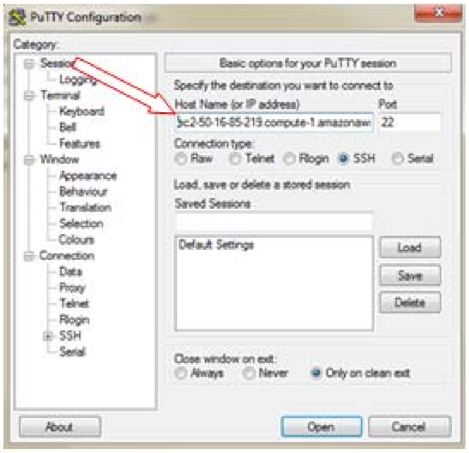
   > **NOTE:** When an instance of the ProtectV Manager AMI is launched, an additional disk is created and attached to it. This disk is attached to */dev/sdd*, and contains the client installer files. When an AWS instance is created (launched) from the ProtectV Manager AMI, **do not** remove or relocate the */dev/sdd* device that is created, and **do not** attach ephemeral storage at */dev/sdd*.

ProtectV Manager StartGuard Pre-boot Setup

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

1. Use SSH to connect to the launched and running ProtectV Manager instance on port **22**, and use your AWS private key for authentication.

   > **NOTE:** Sometimes a private key generated by AWS cannot be used directly and will need to be converted. For example, a PEM file must be converted to a PPK file in PuTTY for SSH connectivity.
   >
   > For additional details, please refer to the AWS documentation at: http://docs.aws.amazon.com/gettingstarted/latest/wah-linux/getting-started-deploy-app-connect.html.



Specify the destination you want to connect to

Host Name (or IP address): ec2-50-16-85-219.compute-1.amazonaw   Port: 22

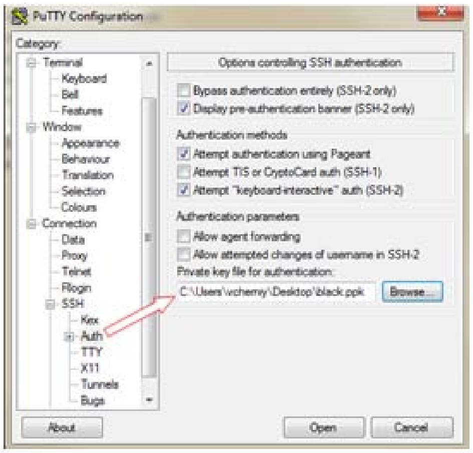
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit



□ Bypass authentication entirely (SSH-2 only)

☑ Display pre-authentication banner (SSH-2 only)

Authentication methods

☑ Attempt authentication using Pageant

□ Attempt TIS or CryptoCard auth (SSH-1)

☑ Attempt "keyboard-interactive" auth (SSH-2)

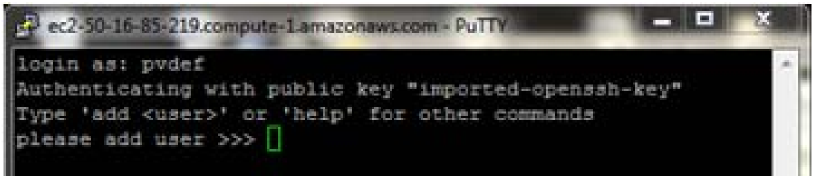
Authentication parameters

□ Allow agent forwarding

□ Allow attempted changes of username in SSH-2

Private key file for authentication: C:\Users\vcherny\Desktop\black.ppk

2. Click **Open**. This will display the ProtectV Manager's SSH Pre-boot Login Shell.
3. Log in as the default user (**pvdef**) at the prompt shown in the ProtectV Manager's SSH Pre-boot Login Shell.



```
login as: pvdef
Authenticating with public key "imported-openssh-key"
Type 'add <user>' or 'help' for other commands
please add user >>> 
```

4. A successful login as the **pvdef** user will launch the ProtectV Manager SSH Login Shell which provides access to a list of commands that will allow you to setup the StartGuard Pre-boot Security for the ProtectV Manager.

   The options that are available in the ProtectV Manager's SSH Login Shell are shown below. Some options will always display, and some will not display until after you have added at least one user, and performed an encryption.

   - **add** *<username>* — Use this option to add a registered user who can access the ProtectV Manager (PVM) instance. This option is always available.
     - You can have a maximum of eight registered users.
     - User names cannot exceed 32 characters.
     - User names can contain alphanumeric, '_', '-' symbols, but must begin with a letter or digit.
   - **boot** — Use this option to unlock drives and boot a decrypted PVM instance. This command will be available after a successful encryption. This option displays only after at least one user has been added, and encryption has been performed.
   - **encrypt** — Use this option to encrypt the PVM. This command will be available if at least one user exists. This option displays only after at least one user has been added.
   - **exit** — Use this option to close the PVM SSH Login Shell. This option is always available.
   - **help** / ? — Use this option to list all of the available commands. This option is always available.
   - **list** — Use this option to list all current users. This option is always available.
   - **password** *<user>* — Use this option to change the password for a specified user. This option is always available.
   - **port** *<port>* — Use this option to change the port connection. The default port is 22. This option displays only after at least one user has been added, and encryption has been performed,
   - **reboot** — Use this option to reboot the PVM instance. This option displays only after at least one user has been added.
   - **rm** *<user>* — Use this option to delete the specified user. This option is always available.
   - **shutdown** — Use this option to shut down the PVM instance. This option displays only after at least one user has been added.

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

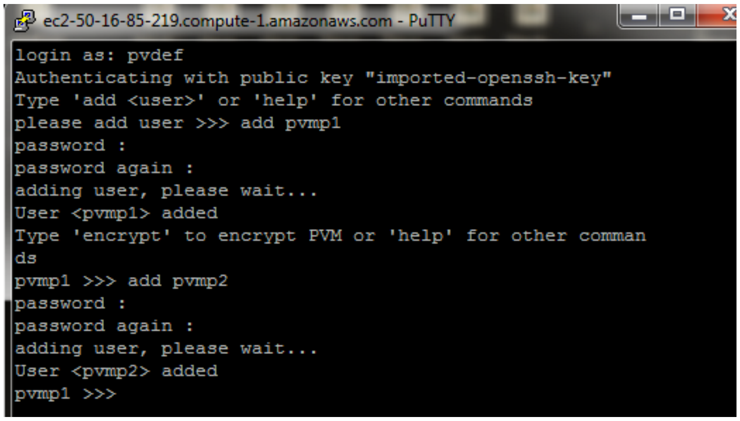
   To add a user, type `add <username>`, specify and confirm the user's password, and then press **Enter**.

NOTE: After the first user is added, the default user (**pvdef**) will automatically be removed. Therefore, you will need to use one of the users you added in this step for subsequent logons.

Here is an example of how to add two users—pvmp1 and pvmp2:

```
>>> add <pvmp1>
password : *******
password again : *******
adding user, please wait...

User <pvmp1> added

Type 'encrypt' to encrypt PVM or 'help' for other commands

>>> add <pvmp2>
password : *******
password again : *******
adding user, please wait...

User <pvmp2> added
```

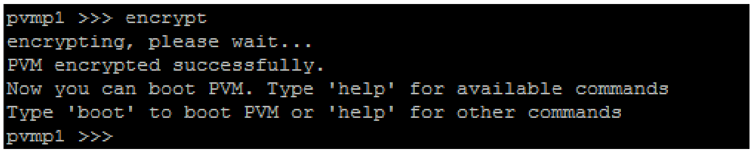
The following screen displays the two users created (pvmp1 and pvmp2).



```
login as: pvdef
Authenticating with public key "imported-openssh-key"
Type 'add <user>' or 'help' for other commands
please add user >>> add pvmp1
password :
password again :
adding user, please wait...
User <pvmp1> added
Type 'encrypt' to encrypt PVM or 'help' for other comman
ds
pvmp1 >>> add pvmp2
password :
password again :
adding user, please wait...
User <pvmp2> added
pvmp1 >>>
```

NOTE: After users are created, if the provisioning process is stopped for any reason, rebooting the instance will allow you to resume at the point that provisioning was interrupted. Log in as one of the newly created users (follow steps 1 -3 at the beginning of the "ProtectV Manager StartGuard Pre-boot Setup" section) to continue.

6. **Do not skip this step!** Type `encrypt` and press **Enter** to encrypt the ProtectV Manager instance. This mandatory step will protect the data stored in the ProtectV Manager.

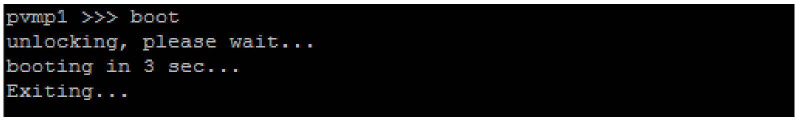


```
pvmp1 >>> encrypt
encrypting, please wait...
PVM encrypted successfully.
Now you can boot PVM. Type 'help' for available commands
Type 'boot' to boot PVM or 'help' for other commands
pvmp1 >>>
```

- The encrypt operation takes approximately two to four minutes, depending on the environment's performance.
- The StartGuard **boot** command will be available upon successful encryption.
- After successful encryption, the ProtectV instance will always be ready to 'boot' if rebooted/disconnected—just connect as one of the newly created users (follow steps 1 -3 at the beginning of this "ProtectV Manager StartGuard Pre-boot Setup" section) to continue.

⚠ **IMPORTANT:** The **add *<username>*** and **encrypt** operations are not recoverable if interrupted. Please do not disconnect or shutdown the instance during the encryption!

7. Type `boot` and press **Enter** to boot the ProtectV Manager instance.



```
pvmp1 >>> boot
unlocking, please wait...
booting in 3 sec...
Exiting...
```

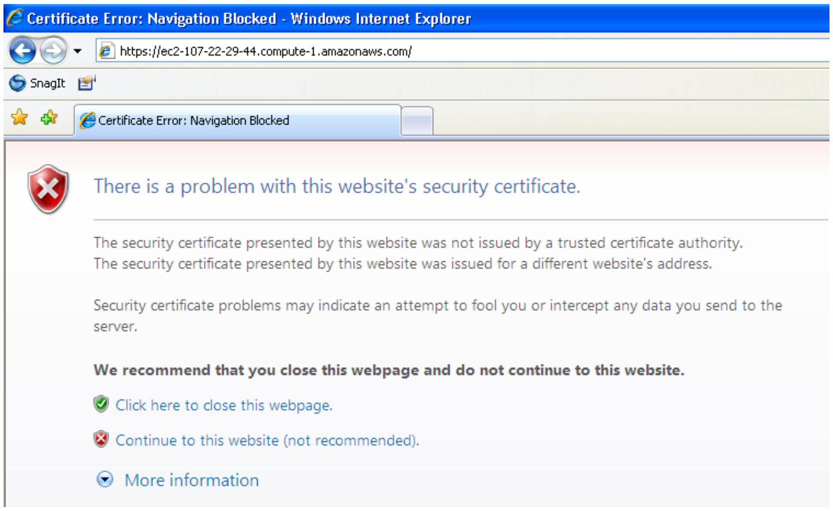
The StartGuard **boot** operation from ProtectV Manager's Pre-boot to Runtime takes approximately one to two minutes, depending on the environment's performance.

Once the ProtectV Manager is booted up, then the ProtectV Manager's runtime services are started, allowing access to ProtectV Manager's API, CLI, and GUI.

ProtectV Manager's Runtime Initial Setup

The first time you access the ProtectV Manager's runtime environment via GUI, API, or CLI, you are required to perform additional setup (i.e., accepting the EULA, changing the default password, etc.). This process is described below.

1. For GUI access, open a new browser window, and connect to ProtectV Manager using its instance DNS address. For example, *https://ec2-50-16-85-219.compute-1.amazonaws.com*
2. ProtectV defaults with a self-signed HTTPS certificate. When the certificate security warning displays, proceed through the screens to accept the certificate. For example, if you're using Internet Explorer, you'd see:


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://ec2-107-22-29-44.compute-1.amazonaws.com/
SnagIt
Certificate Error: Navigation Blocked

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

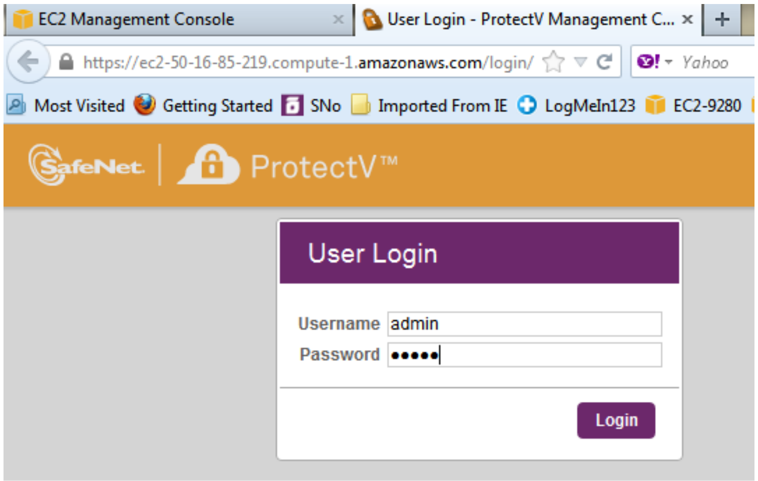
Click here to close this webpage.

Continue to this website (not recommended).

More information

Click **Continue to this website**.

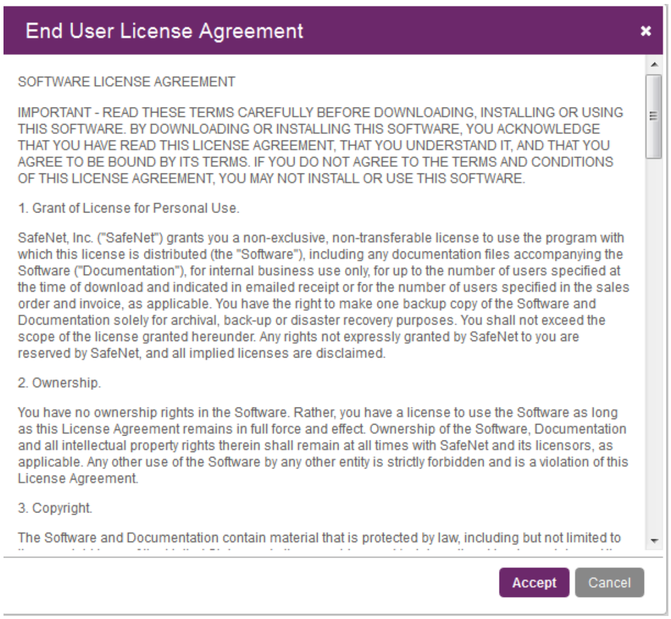
3. Log into ProtectV Manager as **admin/admin**.



Username admin

Password •••••

4. The **End User License Agreement** displays. Scroll to the end of the agreement and click **Accept** to continue.



SOFTWARE LICENSE AGREEMENT

IMPORTANT - READ THESE TERMS CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING THIS SOFTWARE. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT, YOU MAY NOT INSTALL OR USE THIS SOFTWARE.

1. Grant of License for Personal Use.

SafeNet, Inc. ("SafeNet") grants you a non-exclusive, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified at the time of download and indicated in emailed receipt or for the number of users specified in the sales order and invoice, as applicable. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by SafeNet to you are reserved by SafeNet, and all implied licenses are disclaimed.

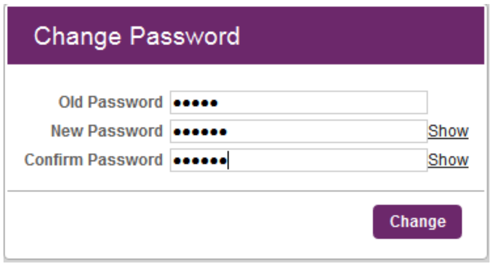
2. Ownership.

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with SafeNet and its licensors, as applicable. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3. Copyright.

The Software and Documentation contain material that is protected by law, including but not limited to

5. Change the default admin password that you used to log into ProtectV Manager in step 3. Enter the old password, enter and confirm the new one, and then click **Change**.



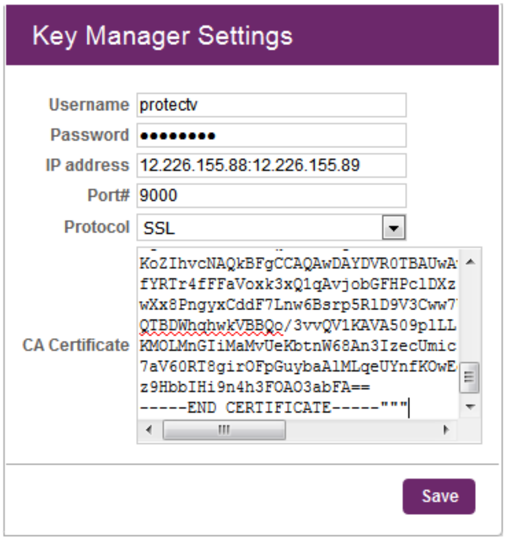
Old Password •••••

New Password ••••••

Confirm Password ••••••

6. Configure settings for your KeyManager. Select **Administration > System Settings > Key Manager Settings**. You must already have a Virtual KeySecure or a physical KeySecure device (K150 or higher) configured to complete this page. (Refer to the tasks outlined in the "Configure KeySecure" section starting on page 3.)

   Complete this page and then click **Save**:

   Key Manager Settings

   Username: protectv

   Password: ••••••••

   IP address: 12.226.155.88:12.226.155.89

   Port#: 9000

   Protocol: SSL

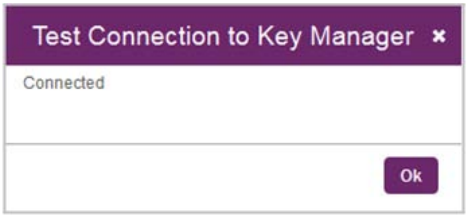
   CA Certificate:

   ```
   KoZIhvcNAQkBFgCCAQAwDAYDVR0TBAUwA
   fYRTr4fFFaVoxk3xQ1qAvjobGFHPclDXz
   wXx8PngyxCddF7Lnw6Bsrp5R1D9V3Cww7
   QTBDWhqhwkVBBQo/3vvQV1KAVA509plLL
   KMOLMnGIiMaMvUeKbtnW68An3IzecUmic
   7aV60RT8girOFpGuybaAlMLqeUYnfKOwE
   z9HbbIHi9n4h3FOAO3abFA==
   -----END CERTIFICATE-----"""
   ```

   - **Username**: Enter the user created on the KeyManager device.
   - **Password**: Enter the password of the user created on the KeyManager device.
   - **IP address**: Enter the KeyManager IP address. (For KeySecure clustering, enter the multiple IP addresses delineated by ':'. For example, 123.12.12.123:123.12.12.124)
   - **Port #**: Enter the KeyManager port.
   - **Protocol**: Select SSL.
   - **CA Certificate**: Copy the Local CA Certificate from the KeyManager device and paste it here.

NOTE: You must enter valid KeySecure settings to ensure that connection to the KeySecure server with the current configuration is correct. If you do not have the KeySecure configured properly, ProtectV Manager cannot make a connection. If the configuration is correct, the *System Status* section on ProtectV Manager Dashboard will display the Key Manager connection status as *Connected*.

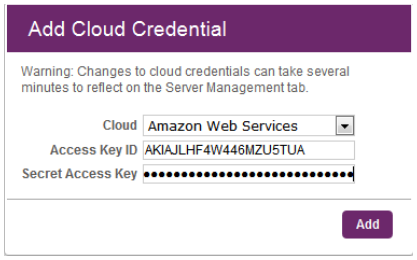
7. Test the connection to Key Manager. From the **Key Manager Settings** page, click **Test Connection**. A successful connection will display this message:

   Test Connection to Key Manager

   Connected

8. Add cloud credentials according to your account credentials. Enter the **Access Key ID** and **Secret Access Key** used to access your Amazon Web Services account, and then click **Add**.



Add Cloud Credential

Warning: Changes to cloud credentials can take several minutes to reflect on the Server Management tab.

Cloud: Amazon Web Services
Access Key ID: AKIAJLHF4W446MZU5TUA
Secret Access Key: ••••••••••••••••••••••••••••

Configure ProtectV Manager in High Availability Mode (optional)

AWS Marketplace provisioned PVMs can be configured in High Availability (HA) mode if desired. One will act as the primary PVM and the other as the secondary PVM.

Please refer to the previous section for configuration details (i.e., logging into ProtectV and changing the default password, configuring the Key Manager settings and checking the connection, etc.)

General HA Setup in AWS EC2/VPC Cloud Types

High Availability setup is similar to previous versions of ProtectV (prior to 1.5), but it does have some Marketplace-specific features that have to be taken into considiration during HA Failover scenarios.

Get Started

CAUTION: In an HA setup, if two PVMs are launched without a keypair, then HA will fail to perform the SSL Handshake, and an error will be reported.

For HA setup to get established successfully, the PVMs must be launched with a keypair.

1. Launch two identical ProtectV Manager instances (we will refer to them as “PVM1” and “PVM2”).
2. Use SSH to connect to the launched and running ProtectV Manager instances on port **22.**

Configure the Pre-boot SSH Shell on Both Nodes

3. For each PVM, follow steps 3-7 in the “Launch and Configuration Procedures > In AWS...” section, and steps 3-7 in the “Launch and Configuration Procedures > ProtectV Manager StartGuard Pre-boot Setup” section described earlier in this document.

   After completing the above steps, it is assumed that:

   a. Both PVMs have been SSH-ed into ProtectV Manager Preboot SSH Shell as the **pvdef** user, using the DNS address with Key Pair authentication.
   b. Both PVMs have at least one user with credentials created in the ProtectV Manager Preboot SSH Shell.
   c. Both PVMs have encrypted ProtectV Manager.
   d. Both PVMs have been ‘boot'ed from the ProtectV Manager Pre-boot SSH Shell into ProtectV Manager Runtime.

NOTE: The steps mentioned above (i.e., steps1, 2, 3a to d) MUST be performed **on both HA nodes** (referred to as “PVM1” and “PVM2” in this document).

Configure the Runtime on the HA “Primary” Node

4. Connect to the **PVM1 instance** using its instance DNS address. This PVM will be the primary PVM in HA mode. Complete the following initialization steps needed in the ProtectV Manager Run Time (described in the “ProtectV Manager’s Runtime Initial Setup” section of this document):

   a. Login as **admin / admin**.
   b. Accept the EULA.
   c. Change the **admin** user password used in step a) above.
   d. Set the Key Manager Settings.
   e. Check the connection to the Key Manager Server.
   f. Add the AWS Cloud Credentials.

5. Create an elastic IP from the AWS Management Console.

No Runtime Configuration is Needed for the HA “Secondary” Node

6. **Do not do anything to the Secondary Node (PVM2)**, which will be the secondary PVM in HA (**do not** log in; **do not** accept the EULA, etc.).

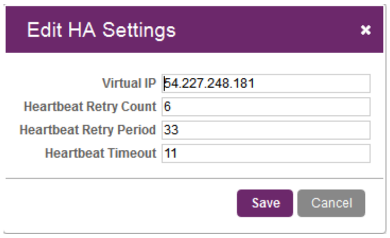
Configure HA Mode for Both PVMs from PVM1

The PVM on which the HA configuration is completed will be submitted as the Primary PVM. The primary’s settings will be replicated to the secondary PVM.

1. In PVM1, click the **Administration** tab.
2. Click the **System Settings** tab.
3. Click **High Availability**.
4. Click **Modify** and define the following:

   - **Virtual IP**—This is an available AWS elastic IP address to use for ProtectV Manager High Availability. The same IP address is used regardless of which instance is backing it (the primary or the secondary). If the primary fails, the secondary will assume the “master” role, and it will associate the elastic IP address while it resuscitates the primary.
   - **Heartbeat Retry Count**—This is the number of retries until an action is taken on the PVM. The interval between retry attempts is the number of seconds defined in the **Heartbeat Interval** field. (The default is 5.)
   - **Heartbeat Interval**—This is the time (in seconds) between checking the PVM’s health. (Must be a minimum of 5 seconds. The default is 30.)
   - **Heartbeat Timeout**—This is the allowed timeout (in seconds) for non-responsive PVM calls. (The default is 10.)

   Example of modified HA settings:



Virtual IP 54.227.248.181
Heartbeat Retry Count 6
Heartbeat Retry Period 33
Heartbeat Timeout 11

5. Click **Save**. Now you can add the secondary PVM to the HA configuration.

Add a Peer

Complete this procedure **on the primary PVM**. Remember that the secondary PVM must remain untouched, which means the default admin password has not been changed, the EULA has not been accepted, etc. These will be replicated from the primary.

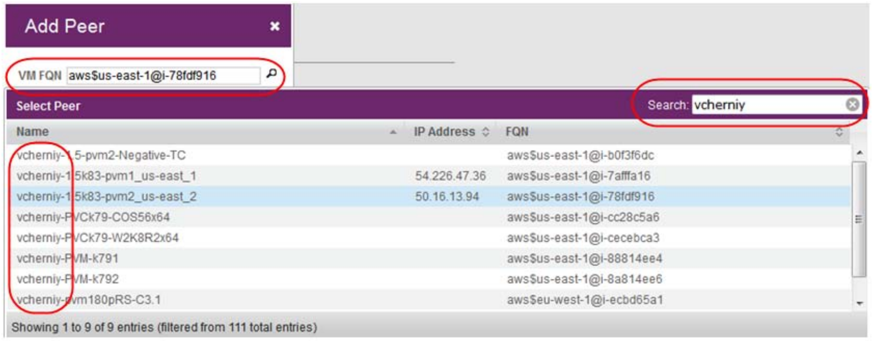
1. Click the **Administration** tab.
2. Click the **System Settings** tab.
3. Click **High Availability**.
4. Click **Add Peer** and define the following:

    - **VM FQN**—This is the secondary PVM's instance FQN identifier. You also enter the FQN manually or search for a specific one.

      For manual entry, the format is <cloud>$<region>@<VMID>, so the VM FQN may look like this: *aws$us-east-1@i-123abcd*

      To use the search mechanism, click the search icon 🔍 and choose a PVM from the list of instances.You can narrow the the list of machines you may want to use as the Secondary PVM by entering a key word in the **Search** field. The filtered list will display only those instances that include the search criteria. Choose the desired instance from this list. Your selection will display in the **VM FQN** field in the **Add Peer** dialog.

      The example below shows the relationship between the VM FQN search mechanism in the **Add Peer** dialog, and using the **Search** field to further narrow the list to locate a specific machine name.



VM FQN aws$us-east-1@i-78fdf916

Select Peer

Search: vcherniy

Name	IP Address	FQN
vcherniy-1.5-pvm2-Negative-TC		aws$us-east-1@i-b0f3f6dc
vcherniy-1.5k83-pvm1_us-east_1	54.226.47.36	aws$us-east-1@i-7afffa16
vcherniy-1.5k83-pvm2_us-east_2	50.16.13.94	aws$us-east-1@i-78fdf916
vcherniy-PVCk79-COS56x64		aws$us-east-1@i-cc28c5a6
vcherniy-PVCk79-W2K8R2x64		aws$us-east-1@i-cecebca3
vcherniy-PVM-k791		aws$us-east-1@i-88814ee4
vcherniy-PVM-k792		aws$us-east-1@i-8a814ee6
vcherniy-pvm180pRS-C3.1		aws$eu-west-1@i-ecbd65a1

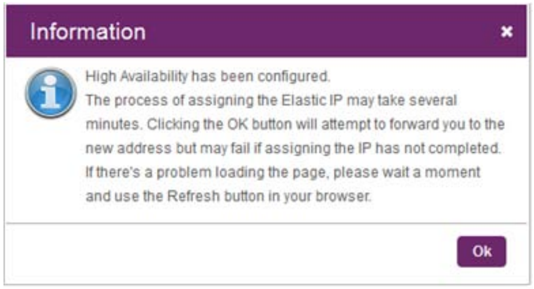
Showing 1 to 9 of 9 entries (filtered from 111 total entries)

    - **Port**—This is the port that the PVM HA service is running on. The default for the ProtectV Manager HA service is port **7080**.

NOTES: If you entered the FQN manually and are unsure where to obtain the secondary PVM's FQN:

- From the **Server Management** tab, in the *Clouds* pane, select the cloud where the secondary PVM is running.
- In the center pane, select the check box adjacent to the instance name of the secondary PVM.
- Copy the **Server ID** value located in the right information pane. This the <*VMID*> portion of the VM FQN.
- Return to the High Availability **Add Peer** dialog, and enter the VM FQN, and make sure to paste the copied Server ID as the <*VMID*> portion of the VM FQN.

5. Click **Save**, and then click **OK**. The following message displays:



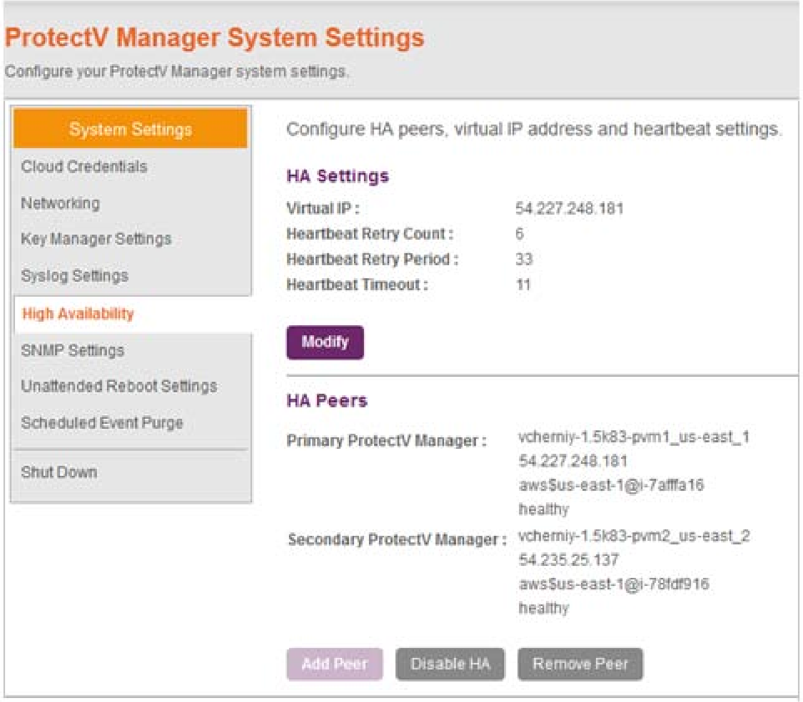
Information ×

High Availability has been configured.
The process of assigning the Elastic IP may take several minutes. Clicking the OK button will attempt to forward you to the new address but may fail if assigning the IP has not completed. If there's a problem loading the page, please wait a moment and use the Refresh button in your browser.

6. As the message above indicates, you may have to wait a few seconds and click the **Refresh** icon ⟳ before the secondary PVM settings refresh on the page, and redirection to the elastic IP will occur (you can also execute the *getHaStatus* API to verify the status).

   After some time, you will need to log in again, and then a *healthy* status will display for both the primary and secondary.

   The example below shows the completed HA settings.



ProtectV Manager System Settings

Configure your ProtectV Manager system settings.

Configure HA peers, virtual IP address and heartbeat settings.

HA Settings

Virtual IP :	54.227.248.181
Heartbeat Retry Count :	6
Heartbeat Retry Period :	33
Heartbeat Timeout :	11

HA Peers

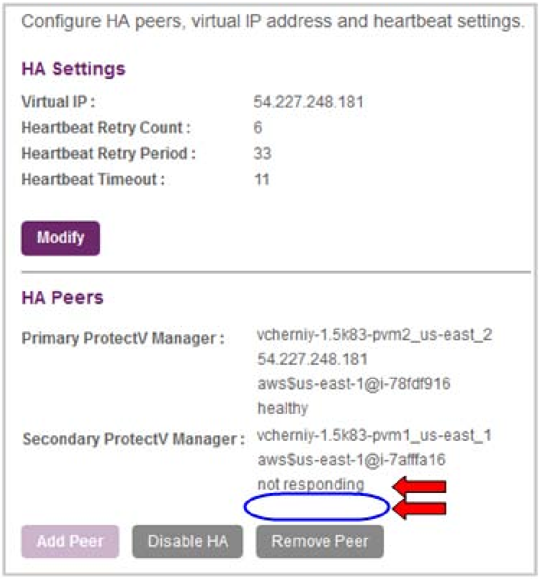
Primary ProtectV Manager :	vcherniy-1.5k83-pvm1_us-east_1 54.227.248.181 aws$us-east-1@i-7afffa16 healthy
Secondary ProtectV Manager :	vcherniy-1.5k83-pvm2_us-east_2 54.235.25.137 aws$us-east-1@i-78fdf916 healthy

Test HA Failover/Resuscitation

You can simulate the failover scenario by stopping the current Primary PVM instance. In real life, this scenario could be triggered by many different reasons. After the failover, follow this workflow on the stopped PVM:

- Until the stopped PVM is restarted and its Status in the AWS EC2 Management Console is back to "*Running*," you will not be able to get the new submitted instance DNS.

  The example below shows an HA setup that is not fully recovered—the secondary PVM has taken over the primary role, but the original primary (now the secondary PVM) still displays a "*not responding*" status, and it is missing the public IP address.



Configure HA peers, virtual IP address and heartbeat settings.

HA Settings

Virtual IP : 54.227.248.181
Heartbeat Retry Count : 6
Heartbeat Retry Period : 33
Heartbeat Timeout : 11

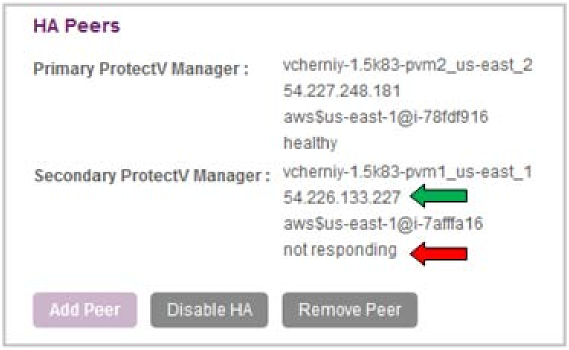
HA Peers

Primary ProtectV Manager : vcherniy-1.5k83-pvm2_us-east_2
54.227.248.181
aws$us-east-1@i-78fdf916
healthy

Secondary ProtectV Manager : vcherniy-1.5k83-pvm1_us-east_1
aws$us-east-1@i-7afffa16
not responding

- When the new primary PVM restarts the stopped PVM, the stopped PVM will pick up a new DNS.

  The example below shows the HA setup is still not fully recovered—the original primary (now the secondary PVM) still displays a "*not responding*" status, but it has picked up the new DNS.



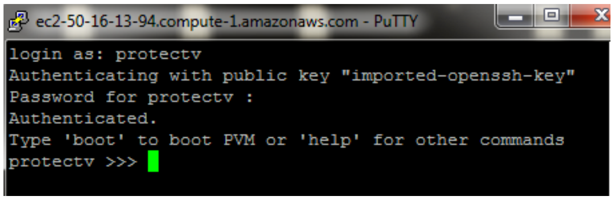
HA Peers

Primary ProtectV Manager : vcherniy-1.5k83-pvm2_us-east_2
54.227.248.181
aws$us-east-1@i-78fdf916
healthy

Secondary ProtectV Manager : vcherniy-1.5k83-pvm1_us-east_1
54.226.133.227
aws$us-east-1@i-7afffa16
not responding

The DNS will appear after the PVM is restarted and its Status in the AWS EC2 Management Console is back to "*Running*."

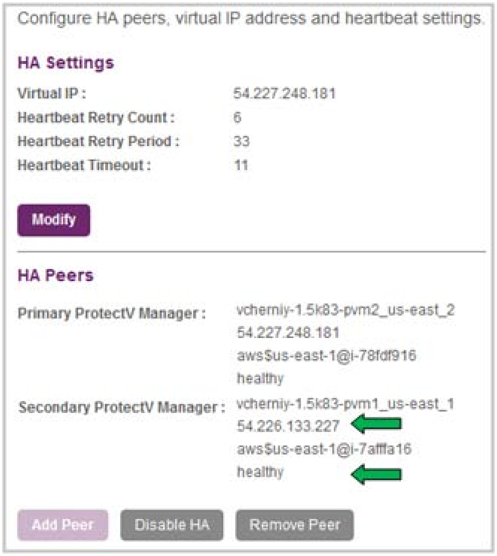
- Use SSH to connect to the recovered ProtectV Manager Pre-boot SSH Shell with the new submitted DNS, and log in as described in step 1 in the "ProtectV Manager StartGuard Pre-boot Setup" section.
  - Log in to the ProtectV Manger Pre-boot SSH Shell using the credentials of one of the previously created users (in the example below, the user credentials used are: protectv / protectv1).



```
login as: protectv
Authenticating with public key "imported-openssh-key"
Password for protectv :
Authenticated.
Type 'boot' to boot PVM or 'help' for other commands
protectv >>>
```

  - Execute the 'boot' command to boot into the ProtectV Manager Runtime.
- Failover and resuscitation recovery will take approximately 12- 15 minutes, depending on the environment's performance.

  The example below shows the HA setup is fully recovered. The final status displays not only the new public IP address, but also a "*healthy*" status for both PVMs.



Configure HA peers, virtual IP address and heartbeat settings.

HA Settings

Virtual IP :	54.227.248.181
Heartbeat Retry Count :	6
Heartbeat Retry Period :	33
Heartbeat Timeout :	11

HA Peers

Primary ProtectV Manager :	vcherniy-1.5k83-pvm2_us-east_2 54.227.248.181 aws$us-east-1@i-78fdf916 healthy
Secondary ProtectV Manager :	vcherniy-1.5k83-pvm1_us-east_1 54.226.133.227 aws$us-east-1@i-7afffa16 healthy

NOTES:

- Any time a PVM is stopped (in HA or single server mode), you should use SSH to connect to the stopped and restarted PVM, and log in using Key Pair authentication and credentials of one of the created users, and then execute the StartGuard boot command.
- PVM configuration in HA mode is supported only for PVMs allocated in the same Region (but they can be in the different zones).
- For Amazon VPC clouds, the Virtual (Elastic) IP is not used (recommended to keep it <blank>).
- HA Failover in VPC private sub-nets should be manually re-browsed to the current Primary PVM because elastic IP in VPC is not configurable.

- Provisioning PVMs in HA and in single Server modes can be configured using API, CLI, and GUI methods.
- PVM in HA mode provisioned on AWS Marketplace can have the same created users, or the users on both PVMs can be different. However, to simplify the HA recovery process on AWS Marketplace, it is recommended that you use the same users on both PVMs configured in HA mode.
- Created pre-boot users and their credentials are not replicated during HA configuration, replication, and sync.
- During an HA failover's complete recovery, manually perform provisioning:
  - SSH using the Instance DNS and one of the previously created users with their credentials.
  - You need to remember the created users and their credentials that are associated with the PVMs configured into HA mode.
- Users with created credentials should be copied and saved in safe and secure location, because they will need to use them after each instance reboot.

Configure the ProtectV Client

Before you begin, please check the list of Supported Platforms on page 7.

This section describes how to:

- Download and install the appropriate ProtectV Linux Client installer package. Each Linux distribution that ProtectV supports has a corresponding installer package (in .tar.gz format) that you can download from the ProtectV Manager Console, which can be installed either manually or via *yum*.

  Before you begin, make sure you are using a supported Linux distribution.

  NOTE: Make sure you have already configured the firewall to open ports 9090 and 9093 to allow TCP and SSL connections. For more details, refer to page 5.

- Download and install the appropriate ProtectV Windows Client installer self-extracting archive. Each Windows platform that ProtectV supports has a corresponding executable file (in .exe format) that you can download from the ProtectV Manager Console.

  Before you begin, make sure you are using a supported Windows platform.

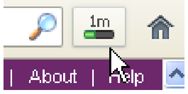
Download and Install the ProtectV Linux Client

You can choose to manually install the RPM, or automate the install using yum. The advantage of using yum is that it will automatically download and install/update dependencies for you.

Manual Install

When installing the ProtectV Linux Client RPM package, you implicitly agree to accept the SafeNet license terms.

1. Download the ProtectV Linux Client installer package from the ProtectV Manager Console:
   - Click the **Administration** tab.
   - Click the **Installers** tab.
   - Click the client installer that you want to download.
   - Click the **Take Action** menu, and then select **Download Installer**.
   - Click **Save File**. The tar.gz archive file will be saved locally to the default download directory. A progress icon in the upper-right corner of the browser will display the progress of the download, and then you will see a message that indicates the download is complete.

2. Locate the tar.gz archive file and unpack it. The file name should look something like this:

   red_hat_enterprise_linux_(rhel)_6.3_(64-bit).aws.1.6.0.208.20130926_215603460.tar.gz

   Run:

   tar -xzvf <filename>.tar.gz

3. Deploy the instance of the supported Linux platform.
4. Transfer the ProtectV Client to the instance (SCP is one method).

   Install the ProtectV Client. Run:

   rpm -i pvlinux-<filename>.rpm

5. In the unlikely event that your system does not already have the necessary dependencies, the install will fail and indicate what dependencies are missing. (Examples would be: *libcrypto.so.6() (64bit)* or *libz.so.1() (64bit)*.) Locate and install these dependencies, and then rerun the install command shown in the previous step.
   - *After the installation is complete*, the machine continues to operate its operating system and services. You can immediately start to encrypt partitions (as described in Chapter 6 in the *ProtectV Installation Guide)*. SafeNet StartGuard will be activated after the first crypto operation of a partition.
   - *For all subsequent reboots*, you will need to start the ProtectV Client instance from the ProtectV Manager Console (as described in Chapter 5 in the *ProtectV Installation Guide)*.

Automated Install with YUM

When installing the ProtectV Linux Client RPM package, you implicitly agree to accept the SafeNet license terms.

1. Download the ProtectV Linux Client installer package from the ProtectV Manager Console, as described in the previous "Manual Install" section.
2. Unpack the installer package. Run:

   tar -xzvf <filename>.tar.gz
3. Install the ProtectV Client.

   Run:

   yum install --nogpgcheck pvlinux-<filename>.rpm
4. You will be presented with a list of the updates that yum has determined it needs to make. If you tell it to proceed, it will download and install the dependencies, and then install the ProtectV Linux client.
   - *After the installation is complete*, the machine continues to operate its operating system and services. You can immediately start to encrypt partitions (as described in Chapter 6 in the *ProtectV Installation Guide)*. SafeNet StartGuard will be activated after the first crypto operation of a partition.
   - *For all subsequent reboots*, you will need to start the ProtectV Client instance from the ProtectV Manager Console.

Download and Install the ProtectV Windows Client

NOTE: During a ProtectV Windows Client fresh installation or upgrade (to version 1.4 or higher), ProtectV FIPS mode is also aligned by default with the Windows security setting, **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**.

By default, ProtectV Windows Client will install or upgrade in ProtectV FIPS mode on operating systems that support FIPS. To enforce a ProtectV installation **not** in FIPS mode, append the ProtectV.msi invocation with the **ERA_ENCRYPT_USE_FIPS=0** property. For example: *msiexec /i ProtectV.msi ERA_ENCRYPT_USE_FIPS=0*.

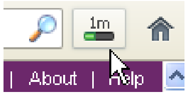
For *non-interactive installations*, if the system is not configured for FIPS operations and ERA_ENCRYPT_USE_FIPS=1 is on the command line, the ProtectV installation will fail and an error message will be written to the log.

For *interactive installations*, if the system is not configured for FIPS operations and ERA_ENCRYPT_USE_FIPS=0 is not on the command line the user will be prompted to continue or not.

NOTE: The **ERA_ENCRYPT_USE_FIPS=1** property has no affect on non-FIPS capable Windows systems.

Upgrade Note: Due to the introduction of FIPS support, a version 1.4 (or higher) ProtectV Manager will be unable to boot up a ProtectV Windows or Linux client that is installed with version 1.2 or older. You must upgrade your ProtectV Clients incrementally, first from version 1.3 to 1.5, and then from 1.5 to 1.6.

1. Download the ProtectV Windows Client installer from the ProtectV Manager Console:
   - Click the **Administration** tab.
   - Click the **Installers** tab.
   - Click the client installer that you want to download.
   - Click the **Take Action** menu, and then select **Download Installer**.
   - Click **Save File**. The self-extracting archive file will be saved locally to the default download directory. A progress icon in the upper-right corner of the browser will display the progress of the download, and then you will see a message that indicates the download is complete.

2. Locate the installer file. The file name should look something like this:

   microsoft_windows_server_2008_r2_(64-bit).aws.1.6.0.208.20130926_200156263.exe
3. Launch the **.exe** to extract the contents.
4. Launch **setup.exe** for an interactive installation. For a non-interactive installation, the **ProtectV.msi** can be used directly.
5. The ProtectV installation wizard opens. When the **Welcome** screen displays, click **Next**.
6. Accept the **License Agreement**, and then click **Next**.
7. Select **Typical Client Installation**, and then click **Next**.
8. Select the language to be used for interface labels and text messages, and then click **Next**.
9. Click **Install** to continue.
10. When the installation is complete, click **Finish**.
11. When prompted, click **Yes** to restart the machine.

> **NOTE:** If the Windows server is rebooted after the ProtectV Windows client is installed, the Windows server will be stuck at SafeNet StartGuard. To get the partition in OS mode, go to the **Take Action** menu in the ProtectV Manager Console and select **Boot to OS**.

12. This post-installation reboot will not activate SafeNet StartGuard, but StartGuard will be active for subsequent reboots.
    - *For this first reboot,* you will be prompted to log into Windows, and then you can immediately start to encrypt partitions (as described in Chapter 6 in the *ProtectV Installation Guide)*.
    - *For all subsequent reboots*, you will first need to boot the ProtectV Client virtual server from the ProtectV Manager Console.