SafeNet ProtectV

User's Guide

gemalto
security to be free

Document Information

Document Information

Product Version	4.X
Document Number	007-013689-001
Release Date	01 December 2017

Revision History

Revision	Date	Reason
E	01 December 2017	New release

Trademarks

Disclaimer

Gemalto 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, Gemalto reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon Gemalto to notify any person or organization of any such revisions or changes.

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.

Gemalto invites constructive comments on the contents of this document. Send your comments, together with your personal and/or company details to the address below.

Contact Method	Contact Information
Mail	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017 USA
Email	technical.support@gemalto.com

CONTENTS

PREFACE

This introductory section explains the importance of the Customer Release Notes (CRN), identifies the audience, provides a brief summary of the user guide's contents, explains how to best use the written material, and discusses the documentation conventions used.

Customer Release Notes

The CRN document provides important information about this release that is not included in other customer documentation. It is strongly recommended that you read the CRN to fully understand the capabilities, limitations, and known issues for this release.

Audience

All products manufactured and distributed by Gemalto are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

What's in this Guide?

The *SafeNet ProtectV User's Guide* provides an overview of SafeNet ProtectV. The document provides instructions to configure SafeNet KeySecure and generate local CA on SafeNet KeySecure.

Next the document provides instructions to launch and configure ProtectV Manager and to manage ProtectV users. The document also describes how to configure ProtectV Manager clustering. Instructions to install, configure, and enroll external ProtectV Gateway are also provided in the document.

Moreover, the document provides instructions on deploying the ProtectV Client Image on Windows and Linux client instances. Instructions for generating an encryption status report on a Windows or Linux client instance are also provided in the document.

Additionally, the document explains various tools used to configure ProtectV components. Next, it provides information on the user interface of ProtectV Manager, also known as the SafeNet ProtectV Manager Console.

Note: This document uses the terms "virtual machine (VM)," "client instance," and "instance" interchangeably. For example, for Microsoft Azure users, it is a "virtual machine;" for AWS users, it is a "client instance" or an "instance."
Also, the document may at times abbreviate "SafeNet KeySecure" or "SafeNet Virtual KeySecure" as "KeySecure", and "SafeNet ProtectV" as "ProtectV".

Organization

The *SafeNet ProtectV User's Guide* contains the following chapters:

Document Conventions

Hyperlinks

Hyperlinked text will, by default, appear in the Gemalto purple color.

For example: https://supportportal.gemalto.com

Notifications

This document uses notes, cautions, and warnings to alert you to important information that may help you to complete your task, or prevent personal injury, damage to the equipment, or data loss.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

> **Note:** Take note. Notes contain important or helpful information that you want to make stand out to the user.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

> **CAUTION:** Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

> **WARNING! Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.**

Command Syntax and Typeface Conventions

Convention	Description
Bold	The bold attribute is used to indicate the following: • Command-line commands and options (Type **dir /p**.) • Button names (Click **Save As**.) • Check box and radio button names (Select the **Print Duplex** check box.) • Window titles (On the **Protect Document** window, click **Yes**.) • Field names (**User Name**: Enter the name of the user.) • Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.) • User input (In the **Date** box, type **April 1**.)
Italic	The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
Double quote marks	Double quote marks enclose references to other sections within the document. For example: Refer to "Support Contacts" for contact details.
`<variable>`	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.

`[ optional ]`
`[ <optional> ]`
`[ a | b | c ]`
	Square brackets enclose optional keywords or `<variables>` in a command line description. Optionally enter the keyword or `<variable>` that is enclosed in square brackets, if it is necessary or desirable to complete the task.
	Square brackets enclose optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.

Convention	Description
`[<a> | <b> | <c>]`	
`{ a | b | c }` `{ <a> | <b> | <c> }`	Braces enclose required alternate keywords or `<variables>` in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.

Related Documents

The following documents contain related or additional information:

- *SafeNet ProtectV User's Guide*
- *SafeNet ProtectV Release Notes*
- *SafeNet ProtectV Clients Customer Release Notes*
- *SafeNet ProtectV API Guide*
- *SafeNet ProtectV Log Monitoring Guide*

Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	

1
SafeNet ProtectV Overview

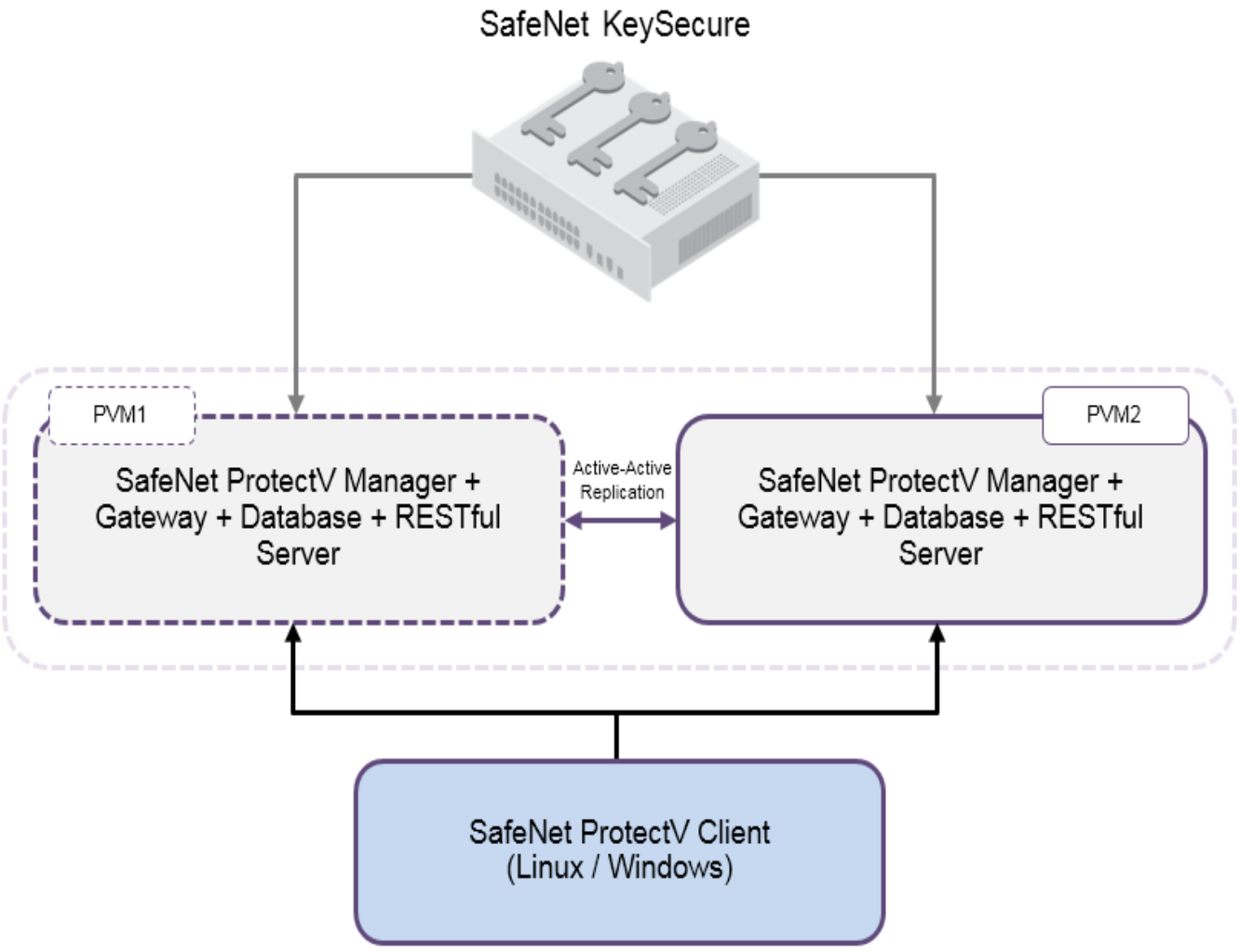
This chapter covers the following information:

Overview

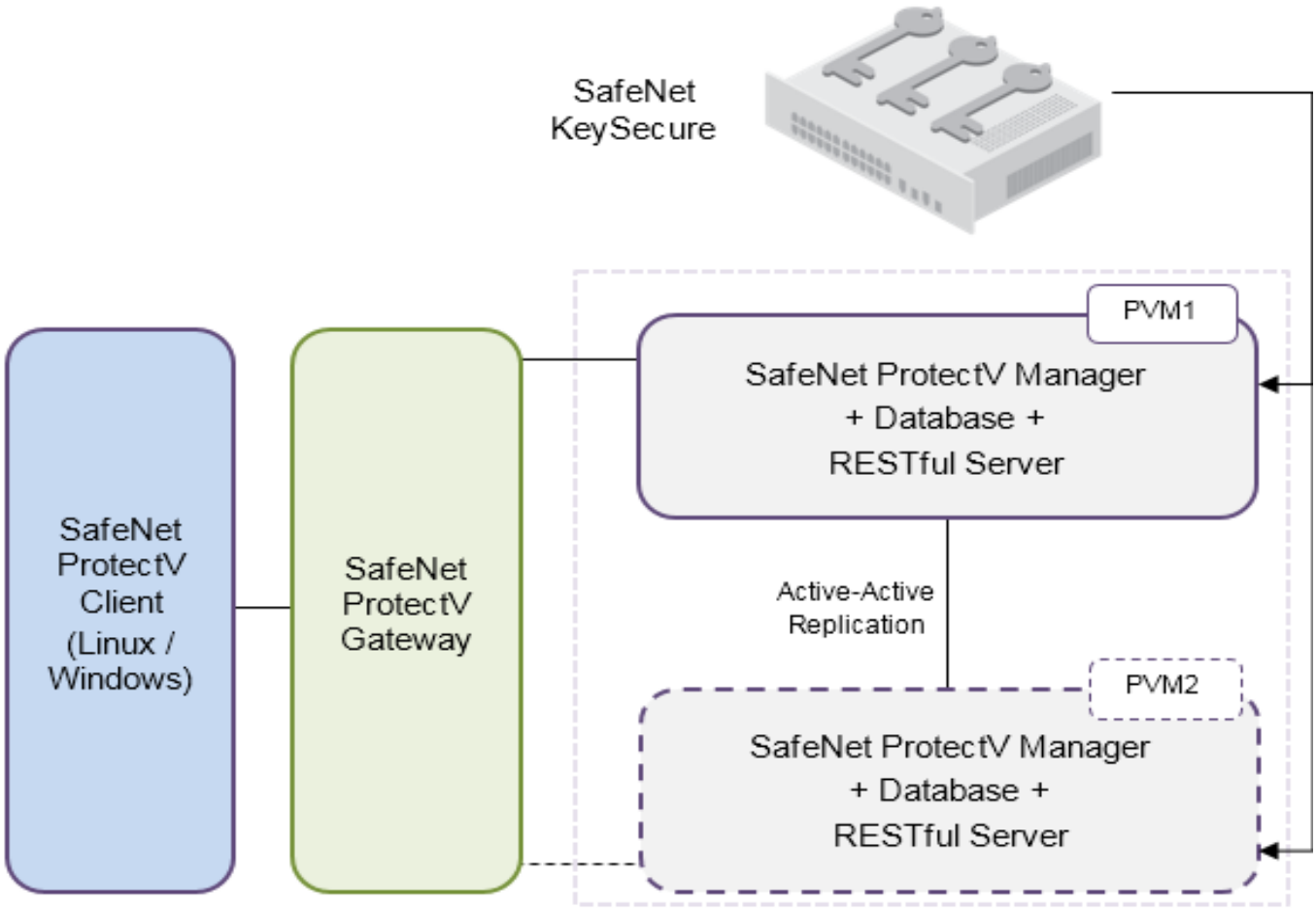
SafeNet ProtectV secures sensitive data by encrypting all data within an entire virtual machine located on all attached storage volumes. After the SafeNet ProtectV Client Image is installed and the client virtual machine is registered with ProtectV Manager, the encryption process begins. To check the encryption status, an encryption status report can be requested for up-to-date statistics on each volume and partition.

By default, SafeNet ProtectV encrypts or decrypts the entire virtual machine. However, mechanism is provided to select specific volumes/partitions for encryption or decryption.

The following diagram shows the SafeNet ProtectV architecture when using local ProtectV Gateways in a two-node ProtectV Manager cluster:



The following diagram shows the SafeNet ProtectV architecture when using an external ProtectV Gateway in a two-node ProtectV Manager cluster:



How SafeNet ProtectV Works?

The ProtectV Client image installed on a virtual machine encrypts and decrypts data. The data remains encrypted until successful authentication during preboot. If ProtectV Client receives the valid key, the data is decrypted. After successful log on, users gain access to their data in plaintext. When the virtual machine is shut down, the data is again encrypted.

The data encryption/decryption process is as follows:

1. After the ProtectV Client image is deployed successfully, the data is encrypted. Linux clients require reboot for successful encryption.
2. During the next reboot, ProtectV Client requests ProtectV Gateway for key to decrypt data.
3. ProtectV Gateway requests ProtectV Manager for the key.
4. ProtectV Manager receives the key from SafeNet KeySecure. Keys are stored on SafeNet KeySecure.
5. ProtectV Manager returns the key to ProtectV Gateway.
6. ProtectV Gateway returns the key to ProtectV Client.
7. ProtectV Client decrypts the data using the key.

Supported Platforms

Note: The ProtectV Linux installer updates only the current kernel during installation. Other versions, present at the time of installation, are not updated automatically.

Note: SafeNet ProtectV supports upgrade of minor kernel versions on client instances. Upgrade of major kernel versions is not supported.

SafeNet ProtectV supports the following virtualized platforms:

- Linux
- Microsoft Windows

Refer to the *SafeNet ProtectV Clients Customer Release Notes* for the complete list of supported platforms.

Supported SafeNet KeySecure Versions

SafeNet ProtectV supports both virtual and physical SafeNet KeySecure servers (referred to as SafeNet Virtual KeySecure, SafeNet KeySecure, or KeySecure in this document.)

SafeNet ProtectV supports SafeNet KeySecure OS v8.1.0 and higher versions.

System Requirements

This section summarizes the system requirements to launch and configure ProtectV components, and to install and run the ProtectV Client on Windows or Linux instances on supported virtual and cloud platforms.

SafeNet ProtectV Manager

Minimum system requirements to launch SafeNet ProtectV Manager for a setup with 2000 client instances:

- **AWS:** m3.medium and larger (for production environments), 4 GB memory (minimum,) 250 GB disk
- **IBM Bluemix:** minimum Private 1 x 2.0 GHz Core, 4 GB memory (minimum,) 250 GB disk
- **Microsoft Azure:** minimum Standard A2 size, 4 GB memory (minimum,) 250 GB disk
- **VMware:** Ubuntu [Linux 64-bit,] 2vCPUs, 4 GB memory (minimum,) 1 NIC (VMXNET3,) 250 GB disk
- **Hyper-V:** Ubuntu [Linux 64-bit,] 2vCPUs, 4 GB memory (minimum,) 1 NIC (VMXNET3,) 250 GB disk

Note: Select the ProtectV Manager configuration depending on the number of client instances to protect. If the number exceeds 2000, select a higher configuration appropriately. For example, increase RAM to 8 GB or 16 GB depending on the number of VMs. Similarly, increase the disk space appropriately to support large number of VMs. For example, to support 10000 client instances, select disk space 500 GB or more.

Note: At minimum, a two-node ProtectV Manager cluster is recommended. In case of large number of client instances, appropriately increase the number of member nodes of the ProtectV Manager cluster. Moreover, it is recommended to register client instances with different ProtectV Manager instances in the cluster. Doing this keeps the numbers of client instances per ProtectV Manager manageable and ensures efficient use of resources.

SafeNet ProtectV Client on Windows Instances

The minimum system requirements to install and run the ProtectV Client on Windows operating system instances are:

- AWS only: Instances should be larger than micro, for example, m3.medium. (t1.micro instances are not supported.)
- 100 MB system free space.
- Additionally, note the following limitations and considerations:
  - Data partitions on GPT (GUID Partition Table) based disks are supported. System partitions, however, must reside on MBR-based disks.
  - Only FAT32 and NTFS file systems are supported. Any other file systems (if not mentioned here) are not supported.
  - Basic disks are supported — dynamic disks are not.

SafeNet ProtectV Client on Linux Instances

The minimum system requirements to install and run the ProtectV Client on Linux operating system instances are:

- AWS only: Instances should be larger than micro, for example, m3.medium. (t1.micro instances are not supported.)
- 100 MB system free space.
- The recommended instance configuration is a pv-grub instance with a separate `/boot` volume or partition at `/dev/sda1` in `XFS`, `ext3`, or `ext4` format (on distributions that support `ext4` by default, such as Ubuntu 14.04. If the instance does not have a separate `/boot` partition, ProtectV will reconfigure the instance to `pv-grub` with a separate boot partition upon first encryption.
- For instances whose root volume is `/dev/sda` (not an unpartitioned `/dev/sda1`), a separate boot partition is required.
- The root partition must be in `XFS`, `ext3`, or `ext4` format (on distributions that support `ext4` by default, such as Ubuntu 14.04).
- Any partition to be encrypted must be in swap, `XFS`, `ext3`, or `ext4` format (on distributions that support `ext4` by default).
- SafeNet ProtectV can encrypt swap, `XFS`, `ext3`, and `ext4` partitions that are larger than 10 MB. On client reboot, encryption keys are generated on KeySecure. These keys are used to encrypt partitions.
- If the swap partition is smaller than 10 MB, then ProtectV does not encrypt it during reboot, but the encryption key is generated. To disable encryption of the swap partition, disable the swap partition using the `swapoff -a` command.
- ProtectV does not support non-PVGRUB instances.

Prerequisites

Access to Gemalto Technical Support

Ensure that you have access to login credentials for Gemalto Technical Support Customer Portal at https://supportportal.gemalto.com to open support tickets, if necessary. If you do not have access to this portal, contact Gemalto Customer Support. Refer to "Support Contacts" for details.

These credentials are also required when provisioning a new version of ProtectV Manager.

An AWS Account

Ensure that you have an AWS account. If needed, create it here: https://console.aws.amazon.com/. In addition, go through the following information carefully:

- You should already be familiar with virtual cloud and Amazon Web Services terminology, know how to navigate and use the AWS Management Console, and launch an instance. Refer to the Amazon Web Services EC2 and VPC documentation for help. The AWS EC2 documentation is available at: http://aws.amazon.com/documentation/ec2/.
- ProtectV Manager supports both AWS EC2 and Amazon VPC.
- Linux AMIs using AWS Marketplace product codes are not supported unless the instance has /boot in a partition separate from the root filesystem (system disk). Such AMIs are rare, but ProtectV does not provide guidance or instruction on how to modify an existing AMI to meet this requirement.

A Microsoft Live Account (for Azure)

Ensure that you have a Microsoft Live account. It is needed to deploy SafeNet ProtectV on virtual machines in Microsoft Azure. If you do not have a Microsoft Live account, you can create one here: https://signup.live.com. Refer to the Microsoft Azure documentation for help.

VMware vCenter Server and vSphere Client

Ensure that you have VMware vCenter Server and vSphere Client installed and configured in your environment. It is needed to deploy SafeNet ProtectV on virtual machines on VMware vSphere. Refer to the VMware documentation for help.

Microsoft Hyper-V Manager

Ensure that you have Hyper-V Manager installed and configured in your environment. It is needed to deploy SafeNet ProtectV on virtual machines on Hyper-V. Refer to the Hyper-V documentation for help.

An IBM Bluemix Account

Ensure that you have an IBM Bluemix (formerly SoftLayer) account. It is needed to deploy SafeNet ProtectV on IBM Bluemix machines. Refer to the IBM Bluemix documentation for help.

Note: IBM Bluemix Bare Metal Servers are equivalent to Bluemix physical servers.

A Linux Instance

Ensure that you have a Linux instance launched and running in a supported cloud platform. You will install, configure, and deploy SafeNet ProtectV Client Image on this instance.

A Windows Instance

Ensure that you have a Windows instance launched and running in a supported cloud platform. You will install, configure, and deploy SafeNet ProtectV Client Image on this instance.

A Web Proxy Server

A Web proxy is needed only when ProtectV Manager/external ProtectV Gateway is running in AWS to manage client instances in AWS. It is needed if “client authentication from cloud” is enabled on the ProtectV Manager/external ProtectV Gateway instance and Amazon EC2 endpoints are inaccessible from ProtectV Manager/external ProtectV Gateway.

A Syslog Server

A Syslog server must be up and running if you want to configure ProtectV Manager to redirect audit and services logs to a dedicated Syslog server. SafeNet ProtectV supports the `syslog-ng` implementation of the Syslog protocol for Linux platforms. It is recommended to use `syslog-ng 3.5.3` with SafeNet ProtectV.

> **Note:** SafeNet ProtectV supports the `tcp`, `udp`, and `tls` protocols. The `tcp` and `tls` protocols are supported by the `syslog-ng` implementation only.

Refer to "Redirecting Logs to Syslog Server" on page 115 for details.

Administrator Access to Instances

Ensure that you have the administrator (or “root”) access to your client instances. Administrator access is needed to install and configure SafeNet ProtectV Client Image on client instances.

IAM Roles

> **Note:** IAM roles are needed for Amazon cloud if client authentication from cloud is enabled.

Ensure that you have appropriate IAM permissions. The SafeNet ProtectV setup needs ProtectV Manager/Gateway instances with an AWS IAM role. Your AWS account must be configured properly; otherwise, the SafeNet ProtectV setup may not work properly.

For details about AWS IAM permissions, refer to the AWS documentation at:
http://docs.aws.amazon.com/IAM/latest/UserGuide/PermissionsOverview.html

Creating a Policy for IAM Role

Creating an IAM role requires a policy. This policy specifies the operations an IAM role can perform without requiring credentials.

To create a policy on Amazon AWS:

1. Sign in to https://console.aws.amazon.com/iam/.
2. In the left pane, click **Policies**.
3. Click **Create Policy**. The **Create Policy** screen is displayed.
4. Click **Select**. The **Review Policy** screen is displayed.
5. Enter the following details:
   a. Specify a **Policy Name**. For example, **AWSPolicy**, in this document.
   b. Add **Description** of the policy.
   c. In the **Policy Document** field, specify the policy details. For example, content of a sample policy is given below:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PVMLogos",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
            ],
            "Resource": [
                "*"
             ]
        }
    ]
}
```

6. Click **Validate Policy**. If an error is returned, rectify it.

> **Note:** When creating an AWS IAM policy, `Sid` must be unique. For example, `PVMLogos` in the sample policy above.

7. After the policy is validated, click **Create Policy**. A message appears stating that the policy has been created.

You can now create an IAM role and attach the newly created policy to the role. Refer to "Creating an IAM Role" for details.

Creating an IAM Role

An IAM role can be used by multiple instances; however, specific policies according to their requirements must be attached to the role. You can attach up to 10 policies to an IAM role.

To create an IAM Role:

1. Sign in to https://console.aws.amazon.com/iam/.
2. In the left pane, click **Roles**.
3. Click **Create New Role**. The **Set Role Name** screen is displayed.
4. Specify the **Role Name**.
5. Click **Next Step**. The **Select Role Type** screen is displayed.
6. Under **AWS Service Roles**, select **Amazon EC2**. Click **Select** on the right. The **Attach Policy** screen is displayed.
7. Search for your policy.
8. Select your policy under **Policy Name**.
9. Click **Next Step**. The **Review** screen is displayed.
10. Review the information.
11. Click **Create Role**. The IAM role is now created. You will need an IAM role when "Setting up SafeNet ProtectV Gateway" on page 85.

Migration from SafeNet ProtectV 2.x

SafeNet ProtectV 4.X is based on a new architecture. It does not support direct upgrade of ProtectV Manager from ProtectV Manager 2.x. However, SafeNet ProtectV 2.0.5 clients may be upgraded to use the latest SafeNet ProtectV version.

To migrate from SafeNet ProtectV 2.x to use the latest version:

1. Set up SafeNet ProtectV components, as described in this document.
2. Upgrade SafeNet ProtectV Clients on client instances. Refer to "Upgrading SafeNet ProtectV Clients" on page 109 for details.
3. Reboot the client instances.

SafeNet ProtectV Components

The following table lists the SafeNet ProtectV components:

Component	Description
SafeNet KeySecure	Virtual instances or physical appliances used to store and manage encryption keys. Local CA certificate is generated on SafeNet KeySecure to establish secure communication between the client instances and ProtectV Manager.
SafeNet ProtectV Manager	Instance(s) to manage ProtectV Gateway, ProtectV Manager Database (PVMDB,) and ProtectV Client images.

Component	Description
ProtectV Manager Database (PVMDB)	PostgreSQL database to store ProtectV configurations. The database resides inside ProtectV Manager.
Active Directory (AD)	Authenticates AD users with SafeNet ProtectV.
SafeNet ProtectV Gateway	Provides keys to ProtectV clients. ProtectV Gateway can be local or external to ProtectV Manager.
Client Instances	Instances where you install, configure, and deploy the ProtectV Client software. Partitions on these instances will be encrypted.

The AMI ID, AMI Name, and images in the *SafeNet ProtectV User Guide* are representational only. They may differ in your setup.

Configuring SafeNet ProtectV Components

The ProtectV Manager AMI includes ProtectV Manager with PVMDB and REST server, and a local ProtectV Gateway. Based on your requirements, you may configure ProtectV for Active Directory and external ProtectV Gateway instances. Steps to launch the ProtectV Manager and external ProtectV Gateway instances are standard. You may alter launch settings to suit your requirements. To launch a SafeNet Virtual KeySecure instance, customized settings are needed.

Note: Instructions to configure different ProtectV components are provided in separate chapters in this document. We strongly recommend that you walk through the chapters, sections, and subsections in the order they are presented. Additionally, it is recommended to carefully read and understand the notes provided in the document.

Supported Configurations

SafeNet ProtectV provides flexibility to:

- Configure and manage ProtectV Manager and ProtectV Gateway on *same* instance. ProtectV Gateway is called *local* to the Manager instance. You only need to launch single instance of the ProtectV Manager AMI.

  Refer to "Setting up SafeNet ProtectV Manager" on page 41 for details.

- Configure and manage ProtectV Manager and ProtectV Gateway on *different* instances. ProtectV Gateway is called *external* to the ProtectV Manager instance. You need to launch two instances of the ProtectV Manager AMI – one for ProtectV Manager, one for ProtectV Gateway.

  Refer to the following chapters for details:

  - "Setting up SafeNet ProtectV Manager" on page 41
  - "Setting up SafeNet ProtectV Gateway" on page 85

The following table lists supported configurations based on ProtectV Gateway location:

Local	External
ProtectV Manager *and* ProtectV Gateway	None

Local	External
ProtectV Manager	ProtectV Gateway

Multi-instance Support

A basic SafeNet ProtectV setup includes ProtectV Manager and ProtectV Gateway running locally on same instance. You can also configure multiple instances of ProtectV Gateway to communicate with single ProtectV Manager instance.

An external ProtectV Gateway instance can also communicate with any of the multiple nodes in a ProtectV Manager cluster. When a new cluster node is added, ProtectV Gateway automatically establishes connection with it. If a ProtectV Manager goes down, ProtectV Gateway starts communicating with another node in the cluster. However, for this configuration, replication among ProtectV Manager nodes in the cluster *must be synchronous*.

The following table lists supported instances of ProtectV Manager and ProtectV Gateway:

ProtectV Manager	ProtectV Gateway
Single	Single
Single	Multiple
*Multiple (n)**	*Single**

** Configuration is supported for ProtectV Manager clustering only. Refer to "Setting up SafeNet ProtectV Manager Clustering" on page 78 for details.*

2
Setting up SafeNet KeySecure

A SafeNet KeySecure manages the keys SafeNet ProtectV uses to encrypt partitions on your client instances. SafeNet ProtectV supports both physical SafeNet KeySecure and SafeNet Virtual KeySecure.

> **Note:** SafeNet KeySecure must be purchased separately from AWS Marketplace or Gemalto. Refer to https://safenet.gemalto.com/data-encryption/enterprise-key-management/key-secure/ for details about SafeNet KeySecure and how to contact our Sales team.

This chapter covers the following information:

Prerequisites

Before you can launch and configure the ProtectV Manager AMI, you must perform the procedures described in this chapter on your SafeNet KeySecure. You will be prompted to enter valid SafeNet KeySecure settings during ProtectV configuration. Install, configure, and initialize your SafeNet KeySecure, as described in the following documents:

- *SafeNet KeySecure Appliance Administration Guide* for details on installing and configuring a physical SafeNet KeySecure.
- *SafeNet Virtual KeySecure AWS Marketplace Installation Guide* for details on installing and configuring a SafeNet Virtual KeySecure.

After configuring and initializing SafeNet KeySecure:

- Ensure that SSL protocol is used for communication with SafeNet KeySecure. Navigate to the **Device** tab > **Key Server**, and view the **NAE-XML** properties. Ensure that **Use SSL** is selected.
- If the SafeNet 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 Export** and **Allow Key and Policy Configuration Operations** properties.
- Ensure to set Password Authentication. Navigate to the **Device** tab > **Key Server**, and view the NAE-XML properties. Under **Authentication Settings**, set **Password Authentication** as **Required (most secure)**.
- When using the client certificate authentication, set Client Certificate Authentication. Navigate to the **Device** tab > **Key Server**, and view the NAE-XML properties. Under **Authentication Settings**, set **Client Certificate Authentication** as **Used for SSL sessions and username (most secure)**.

Generating the Local CA Certificate

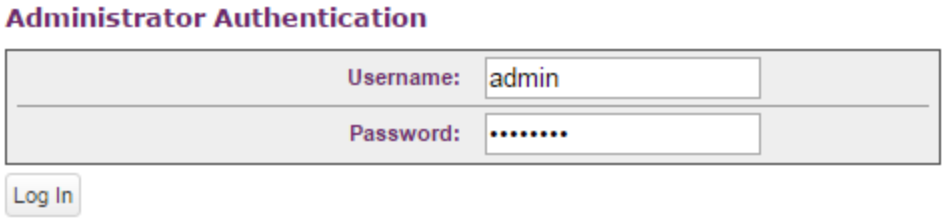
This section describes procedures to create and download a local CA certificate. It involves:

1. "Creating a Local CA" below
2. "Creating a Server Certificate Request on Management Console" on the next page
3. "Signing a Server Certificate Request with the Local CA" on page 27
4. "Downloading the Local CA Certificate" on page 36

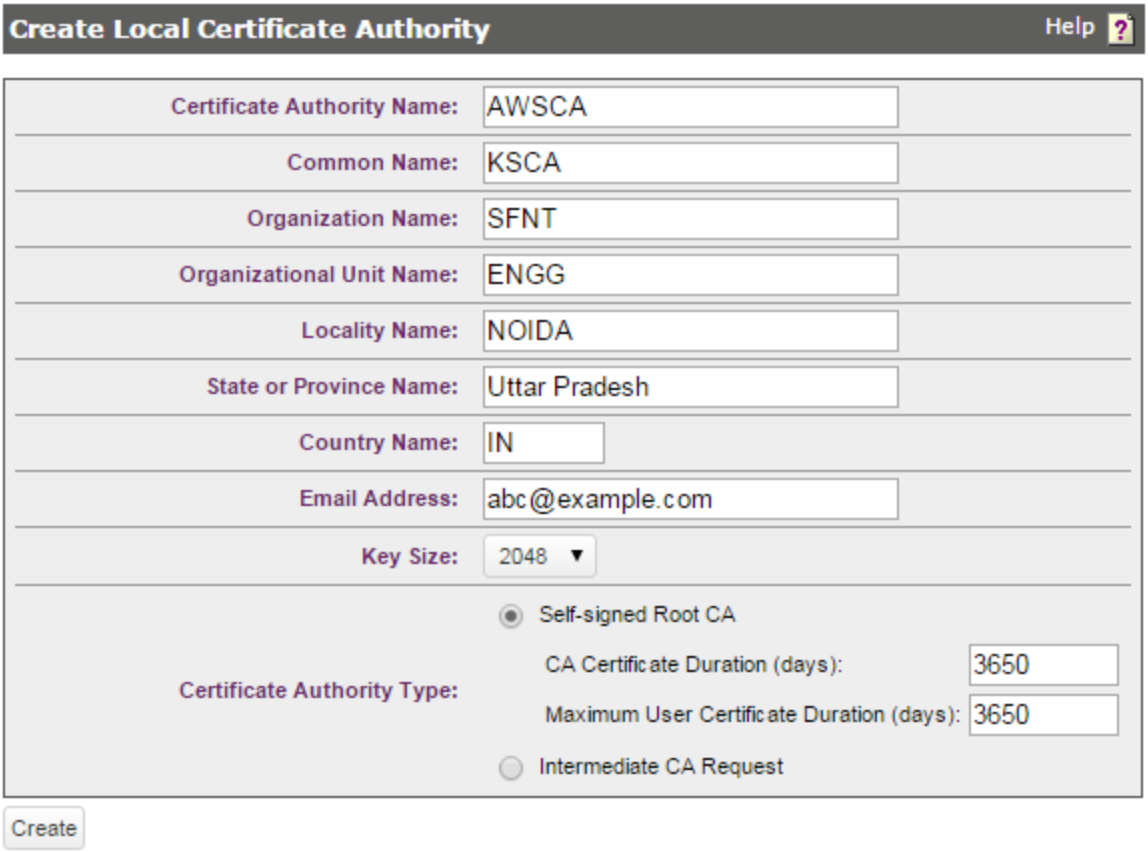
Creating a Local CA

To create a Local CA:

1. Log on to the **Management Console** as an administrator with Certificate Authorities access control.



2. Navigate to the **Create Local Certificate Authority** section on the **Certificate and CA Configuration** page (**Security**, **Device CAs & SSL Certificates**, **Local CAs**.)
3. Enter the required details.
4. Select either **Self-signed Root CA** or **Intermediate CA Request** as the **Certificate Authority Type**.



5. Click **Create**. The created CA appears in the **Local Certificate Authority List**.

> **Note:** ProtectV Manager and KeySecure can be configured to communicate with each other using Local CA certificates or certificates from an external/customer Enterprise CA. This document describes steps for using Local CA only.

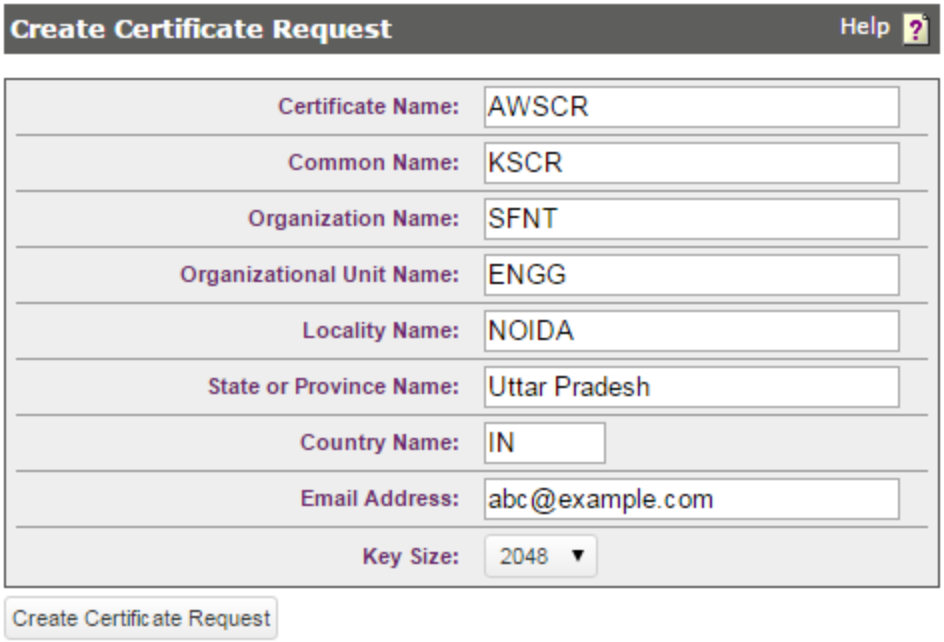
> **Note:** Local CA certificates must be added to a trusted CA list to be recognized by the NAE Server. Local CA certificates should be backed up for protection.

After a local CA is created, you need to create a server request on the Management Console, as described in the next section.

Creating a Server Certificate Request on Management Console

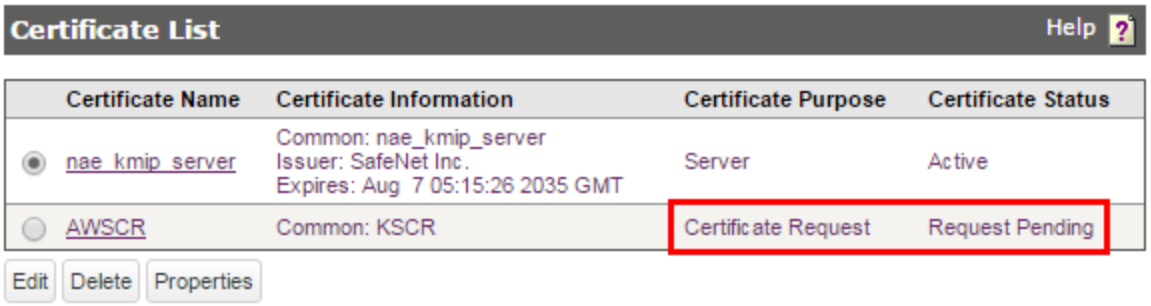
To create a server certificate request:

1. Log on to the **Management Console** as an administrator with Certificates access control.
2. Navigate to the **Create Certificate Request** section of the **Certificate Configuration** page (**Security**, **Device CAs & SSL Certificates**, **SSL Certificates**.)
3. Enter the required details.



4. Click **Create Certificate Request**.

This creates the certificate request and places it in the **Certificate List** section of the **Certificate and CA Configuration** page.

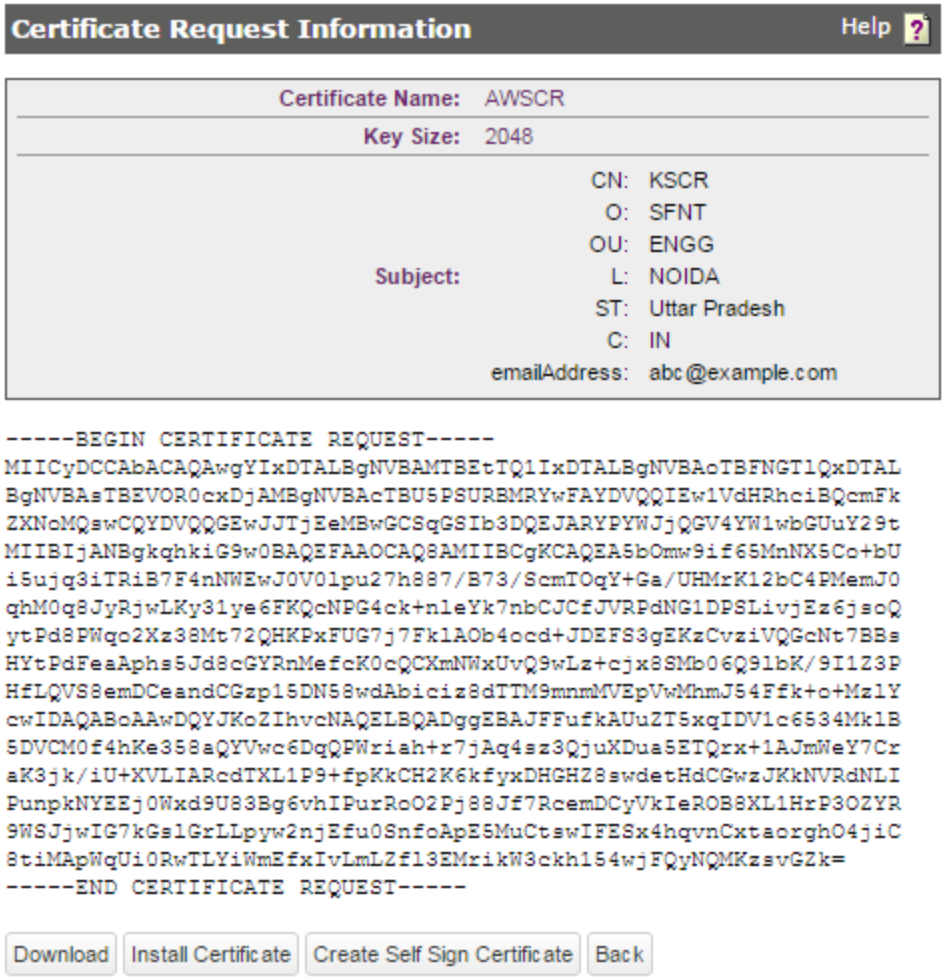


The new entry shows that the **Certificate Purpose** is **Certificate Request** and that the **Certificate Status** is **Request Pending**.

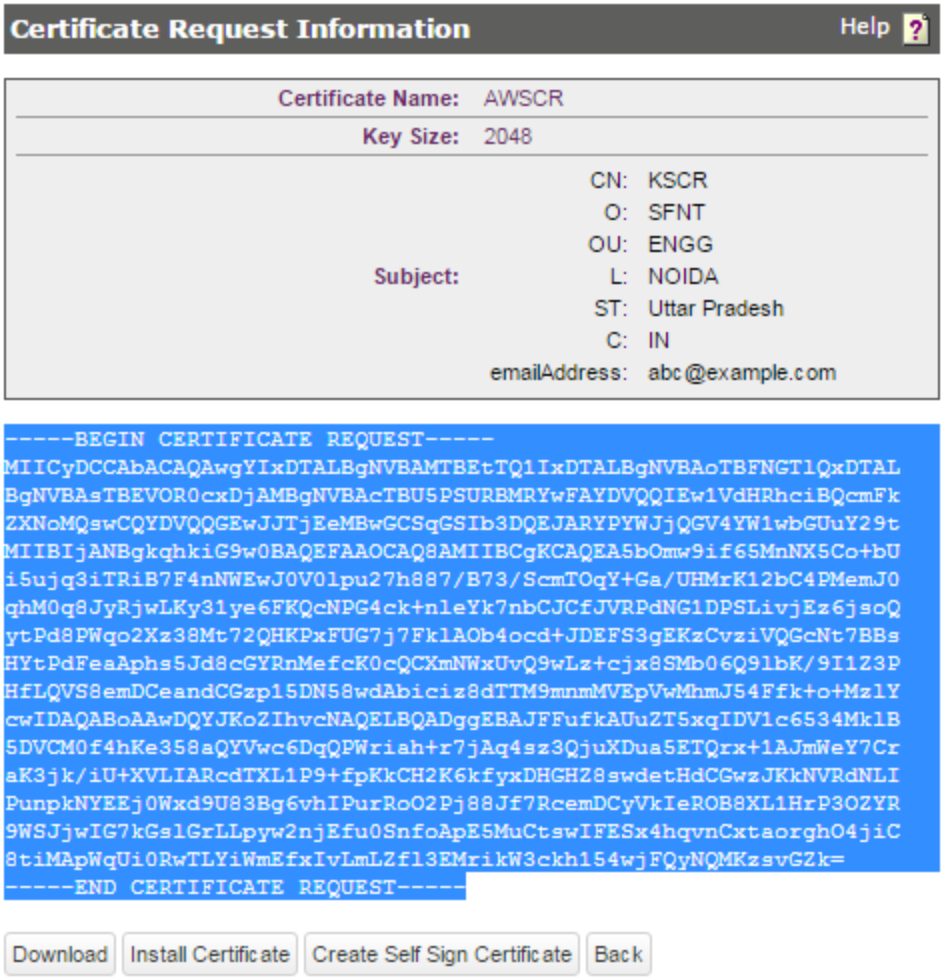
Signing a Server Certificate Request with the Local CA

To sign a server certificate request with the local CA:

1. Log on to the **Management Console** as an administrator with Certificates and Certificate Authorities access controls.
2. Navigate to the **Certificate List** section on the **Certificate and CA Configuration** page (**Security**, **Device CAs & SSL Certificates**, **SSL Certificates**.)
3. Select the certificate request and click **Properties**. The **Certificate Request Information** section is displayed.

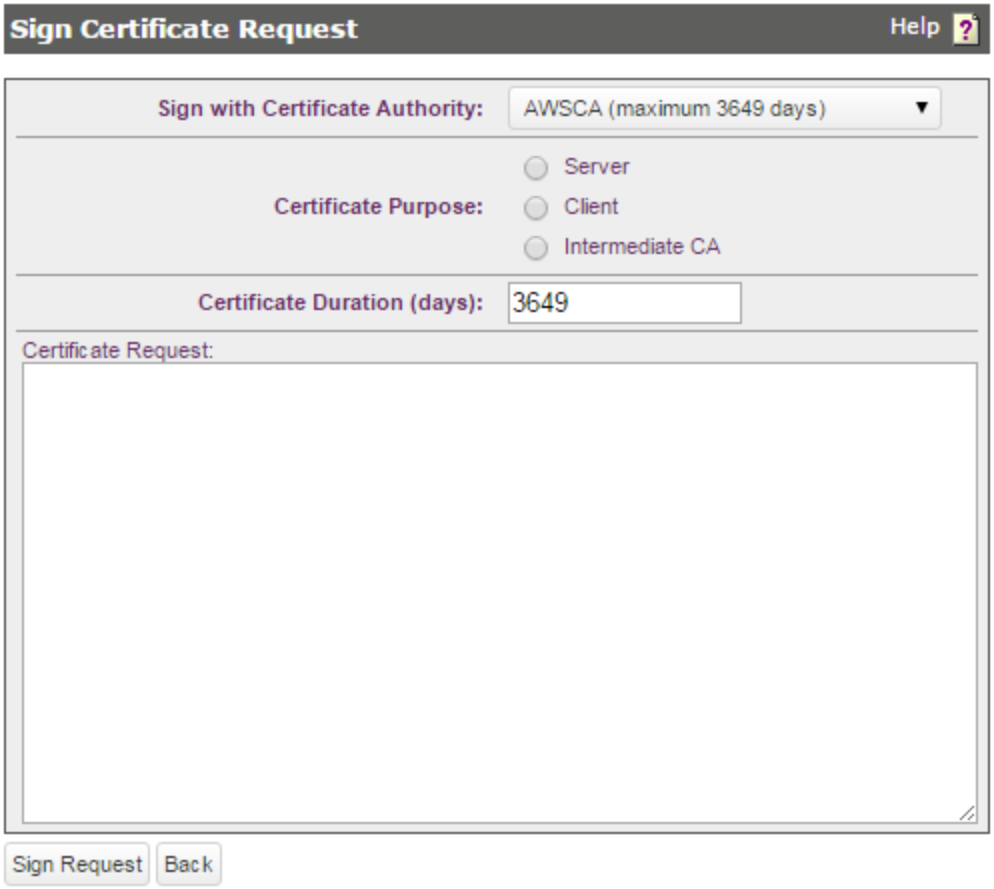


4. Copy the text of the certificate request. The copied text must include the header (`-----BEGIN CERTIFICATE REQUEST-----`) and footer (`-----END CERTIFICATE REQUEST-----`).

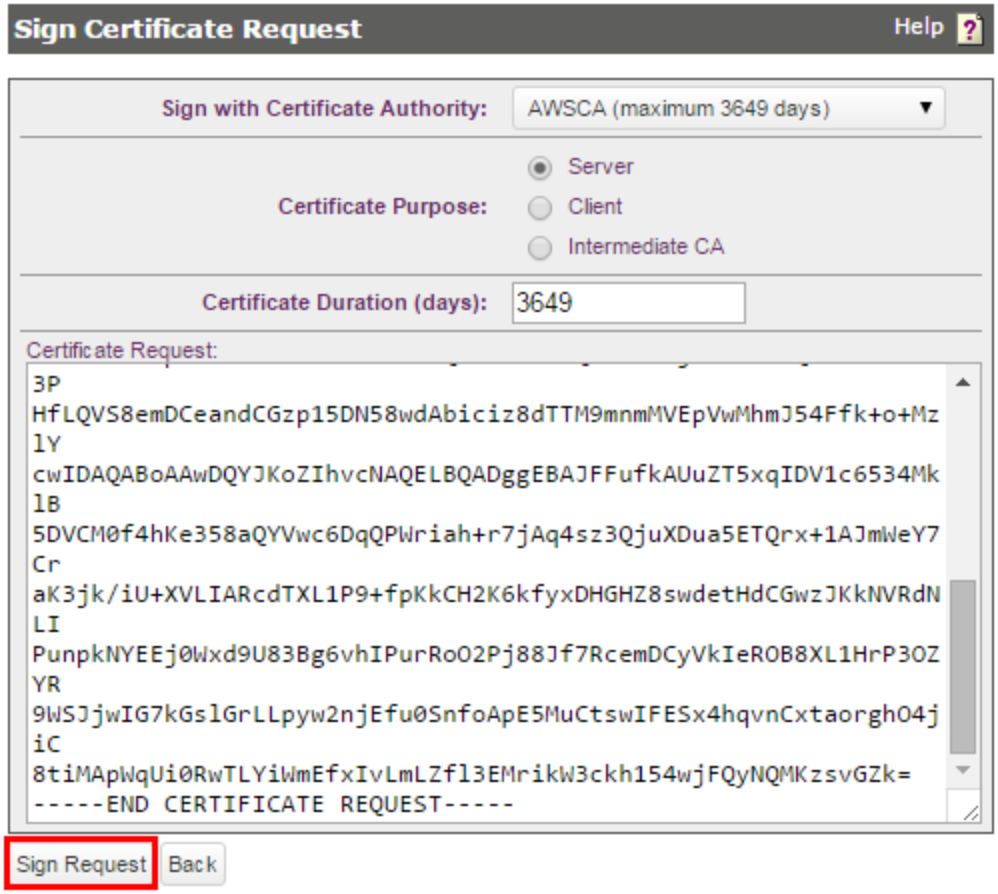


5. Navigate to the **Local Certificate Authority List** (**Security**, **Device CAs & SSL Certificates**, **Local CAs**.)

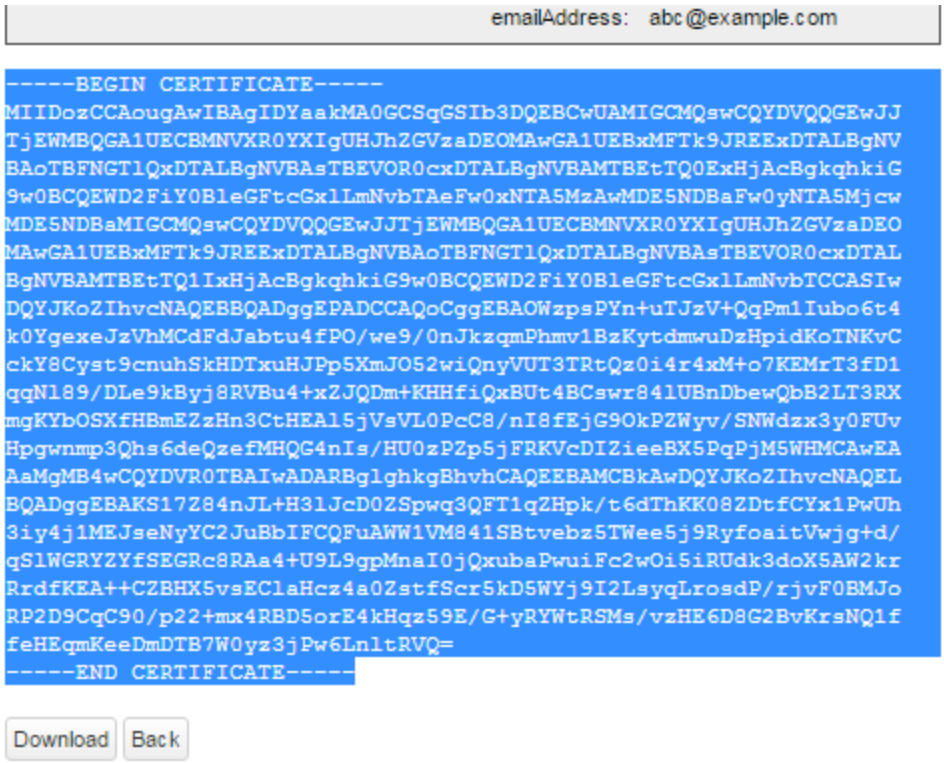
6. Select the local CA and click **Sign Request** to access the **Sign Certificate Request** section.



7. Enter the following details:
   - **Sign with Certificate Authority** – Select the CA that signs the request.
   - **Certificate Purpose** – Select Server.
   - **Certificate Duration (days)** – Enter the life span of the certificate. Default is `3649` days.
   - **Certificate Request** – Paste all text from the certificate request, including the header and footer.

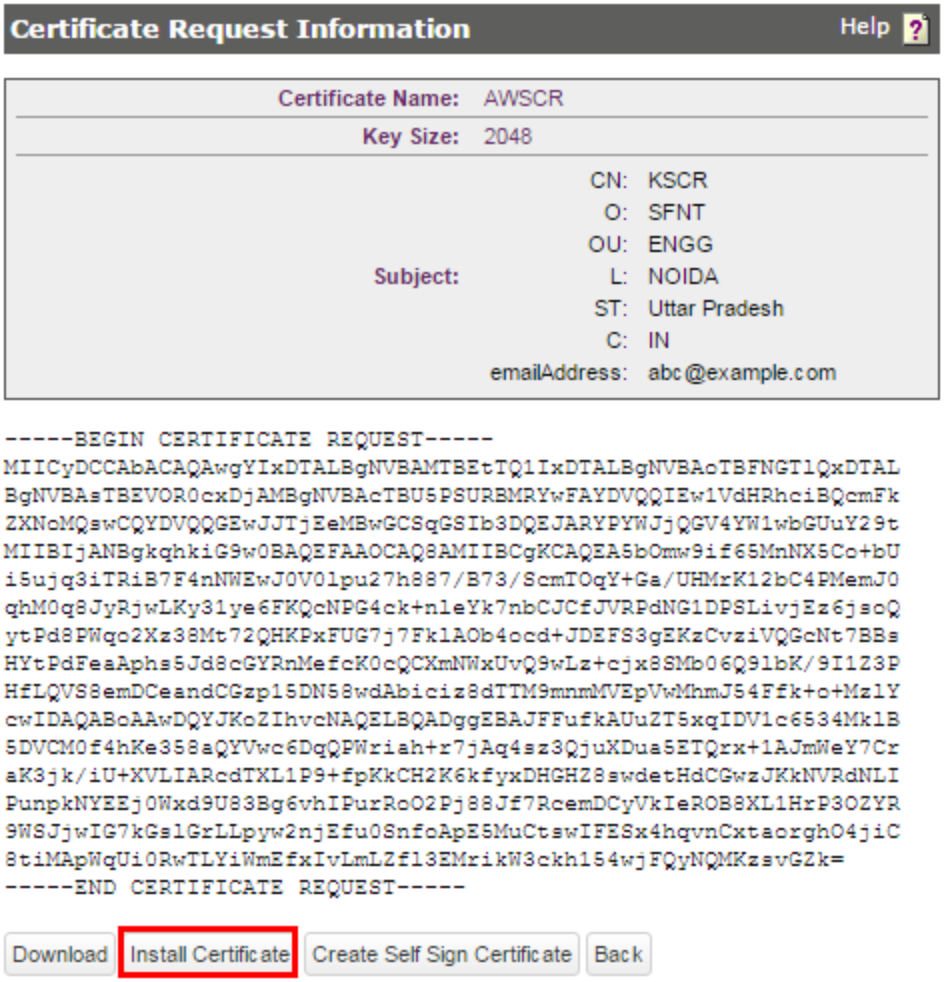


8. Click **Sign Request**. This will take you to the **CA Certificate Information** section.
9. Copy the actual certificate. The copied text must include the header (`-----BEGIN CERTIFICATE-----`) and footer (`-----END CERTIFICATE-----`).

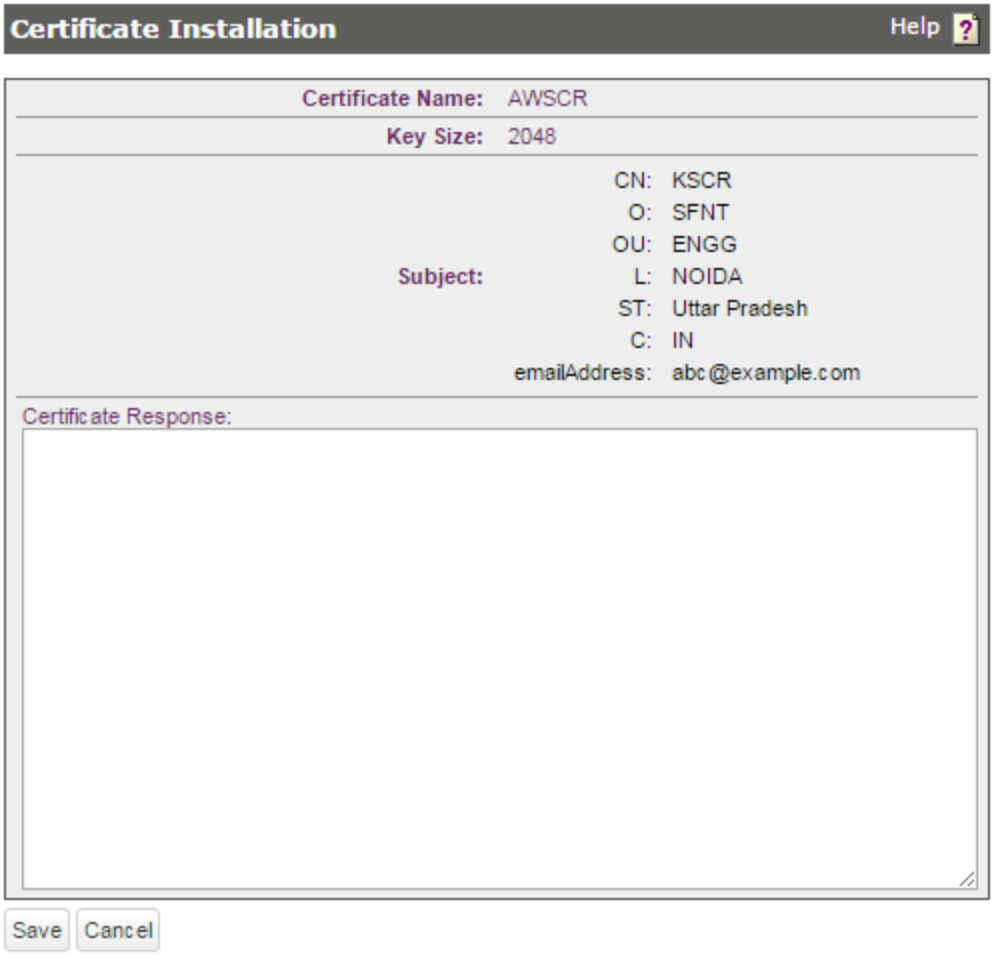


10. Navigate back to the **Certificate List** section (**Security**, **Device CAs & SSL Certificates**, **SSL Certificates**.)

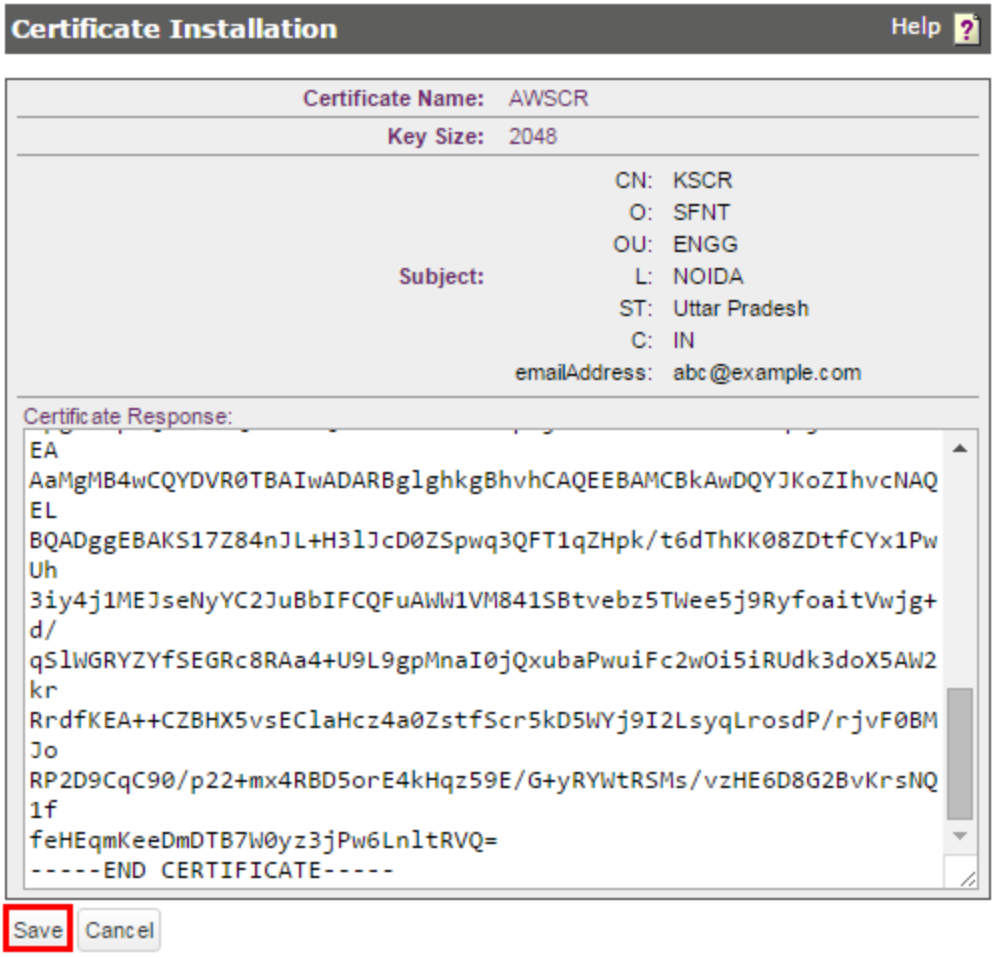
11. Select your certificate request and click **Properties**.



12. Click **Install Certificate**. The **Certificate Installation** screen is displayed.

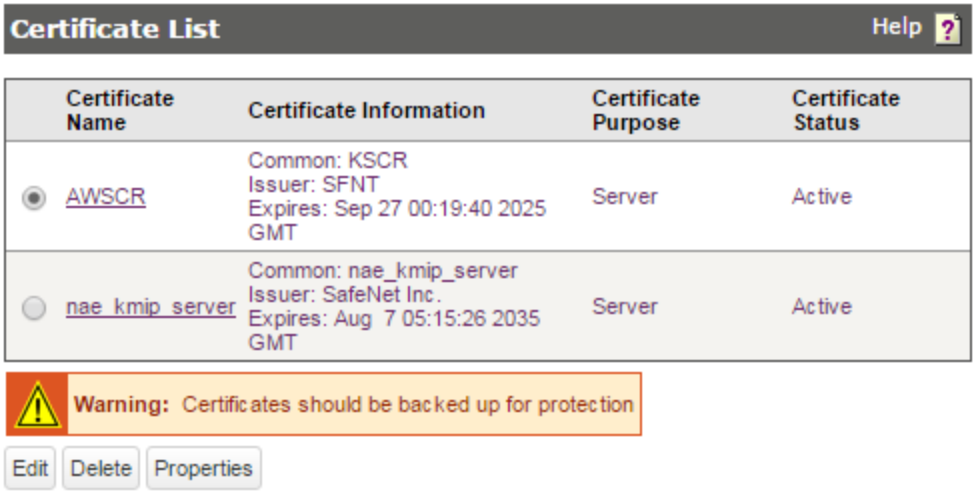


13. Paste the actual certificate in the **Certificate Response** text box.



14. Click **Save**.

The Management Console returns you to the **Certificate List** section. The section will now show that the **Certificate Purpose** is **Server** and that the **Certificate Status** is **Active**.



The certificate can now be used as the server certificate for the SafeNet KeySecure server.

Downloading the Local CA Certificate

To download the local CA certificate from the SafeNet KeySecure appliance:

1. Log on to the **Management Console** as an administrator with Certificate Authorities access control.
2. Navigate to the **Local Certificate Authority List** section of the **Certificate and CA Configuration** page (**Security**, **Device CAs & SSL Certificates**, **Local CAs**.)

3. Select the local CA and click the **Download** button to download the file to your ProtectV Gateway instance. You should place the CA certificate in a secure location and modify access appropriately.

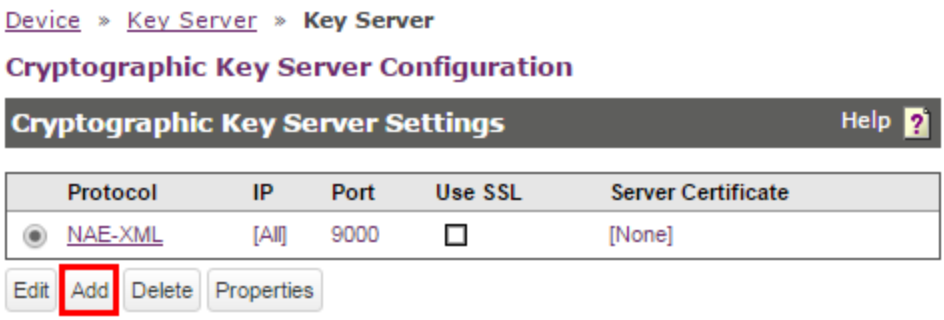
> **Note:** You will need this CA certificate when "Configuring SafeNet ProtectV Manager with SafeNet KeySecure" on page 61.

Refer to the *SafeNet Virtual KeySecure AWS Marketplace Installation Guide* or *SafeNet KeySecure Appliance Administration Guide* for details.

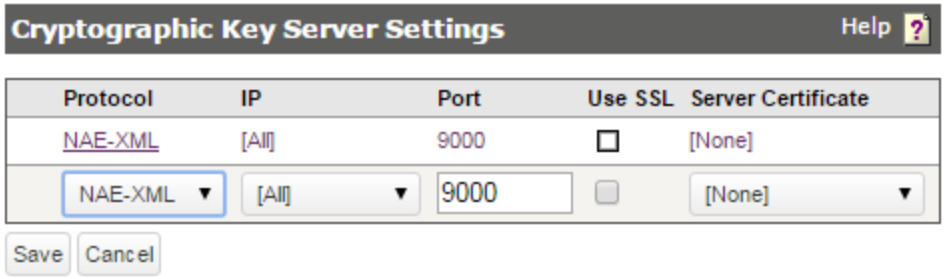
Enabling Key Export on SafeNet KeySecure

To enable key export on SafeNet KeySecure:

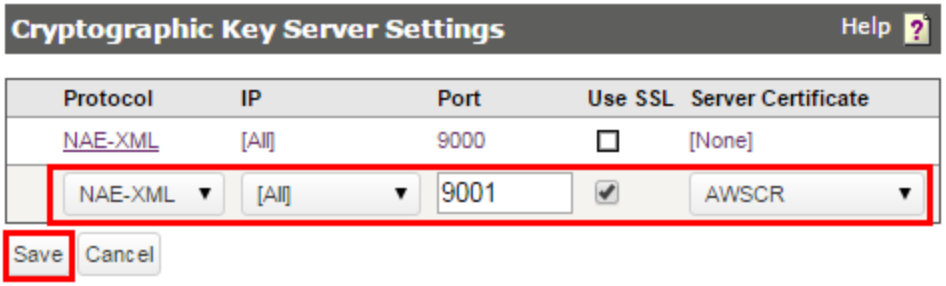
1. Navigate to the **Cryptographic Key Server Configuration** page (**Device**, **Key Server**, **Key Server**.)



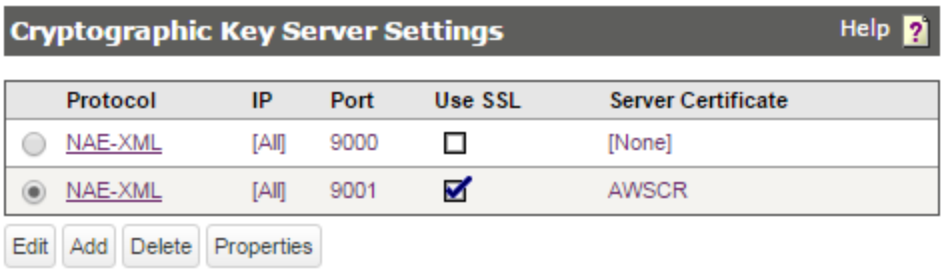
2. Click **Add** under the **Cryptographic Key Server Settings** section.



3. Specify **Port**. By default, `9000` appears. Modify the port; ensure that it is not already in use. This port will be used when configuring Gateways with SafeNet KeySecure.
4. Select **Use SSL**.
5. Select your certificate from the **Server Certificate** drop-down list.



6. Click **Save**. The server certificate is now added.



7. Select the NAE-XML under **Protocol**.
8. Click **Properties**.
9. Under the **Cryptographic Key Server Properties** section, click **Edit**.
10. Select the **Allow Key and Policy Configuration Operations** check box.
11. Select the **Allow Key Export** check box.
12. Click **Save**.

Configuring Authentication Settings

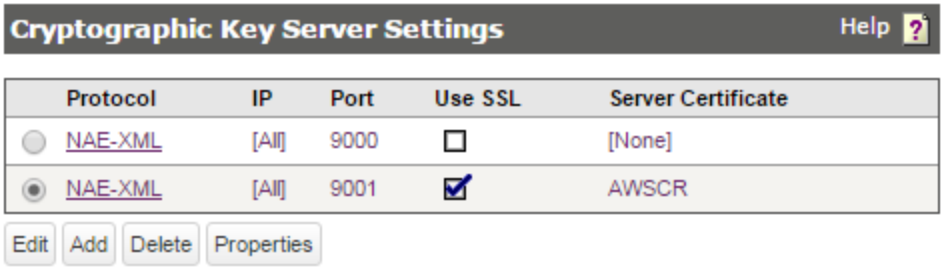
The communication between SafeNet KeySecure and SafeNet ProtectV varies slightly, depending on whether your protocol configuration requires users to authenticate. If you decide not to authenticate, then users have access only to global keys. Global keys are available to everyone, with no authentication required.

If you want to require authentication, then you must create keys for each user or group of users. An authenticated user has access to all global keys, all keys owned by the user, and all keys accessible to groups to which that user belongs. In addition, a group of users can have an authorization policy assigned to it, which restricts the use of the keys accessible by that group to certain time periods or a certain number of operations per hour.

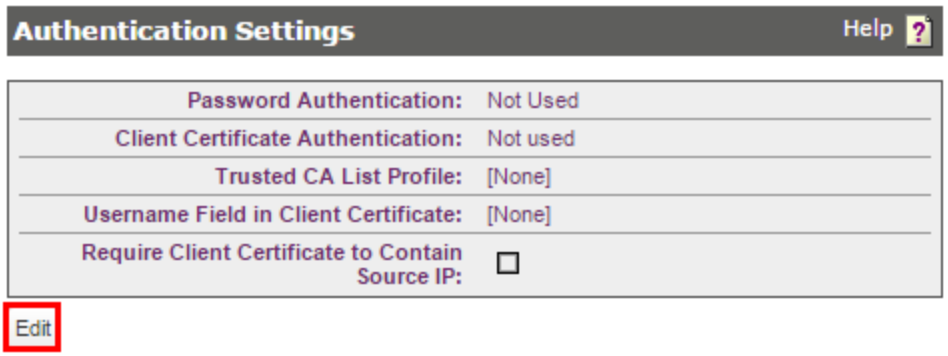
Configure authentication settings on SafeNet KeySecure according to your requirements. Refer to the "Authentication Overview" section in the "Cryptographic Key Servers" chapter of the *SafeNet KeySecure Appliance Administration Guide*.

To configure authentication settings:

1. Navigate to the **Cryptographic Key Server Configuration** page (**Device**, **Key Server**, **Key Server**.)
2. Select your certificate under **Protocol**.



3. Click **Properties**.
4. Navigate to the **Authentication Settings** section.



5. Click **Edit**.
6. Define authentication settings. You can set password authentication, client certificate authentication, or both authentications.

> **Note:** It is recommended to enable both password authentication and client certificate authentication. Refer to the "Authentication Overview" section in the "Cryptographic Key Servers" chapter of the *SafeNet KeySecure Appliance Administration Guide* for details.

– To configure *password authentication*, set **Password Authentication**. The options are:

- **Not Used** – Disables password authentication.
- **Optional** – Makes password authentication optional.
- **Required (most secure)** – Forces password authentication. *This is the recommended setting.* Examples in this document assume this setting.

– To configure *client certificate authentication*:

a. Set **Client Certificate Authentication**. The options are:

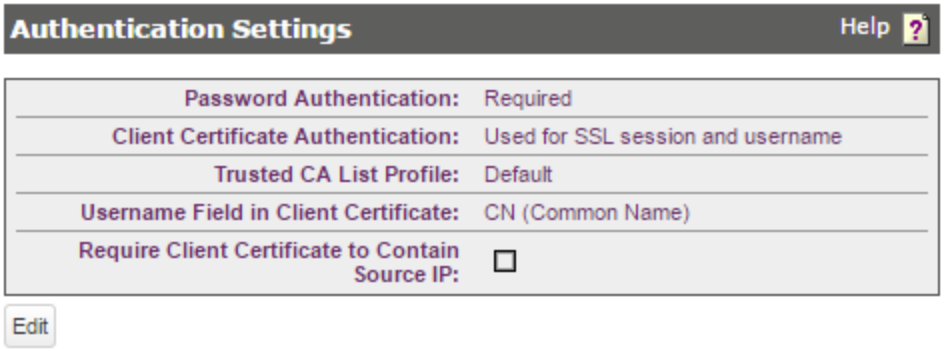
- **Not used** – Disables client certificate authentication.
- **Used for SSL session only** – Requires a client certificate to establish SSL connections.
- **Used for SSL session and username (most secure)** – Requires a client certificate and combination of user name and password to establish SSL connections with SafeNet KeySecure. *This is the recommended setting.* Examples in this document assume this setting.

b. Select a **Trusted CA List Profile** from the drop-down list.

c. Select **CN (Common Name)** from the **Username Field in Client Certificate** drop-down list.

Note: The CN (Common Name) must be the same in server and client certificates, and the same user must exist on SafeNet KeySecure.

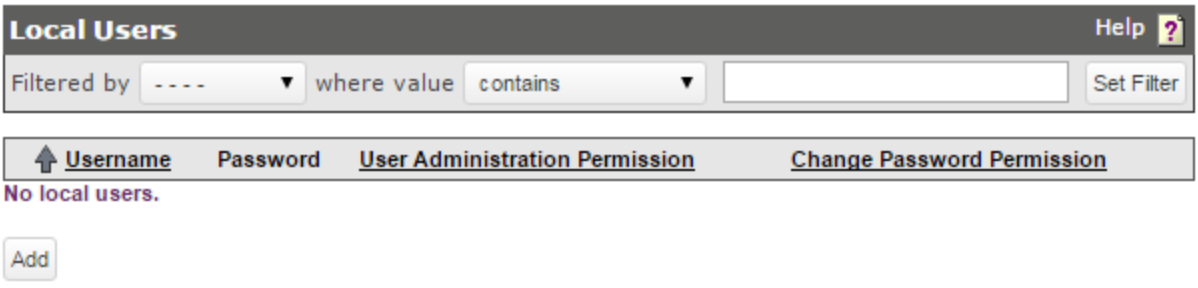
7. Click **Save**. The authentication settings are configured, as shown below.



Creating a Local SafeNet KeySecure User

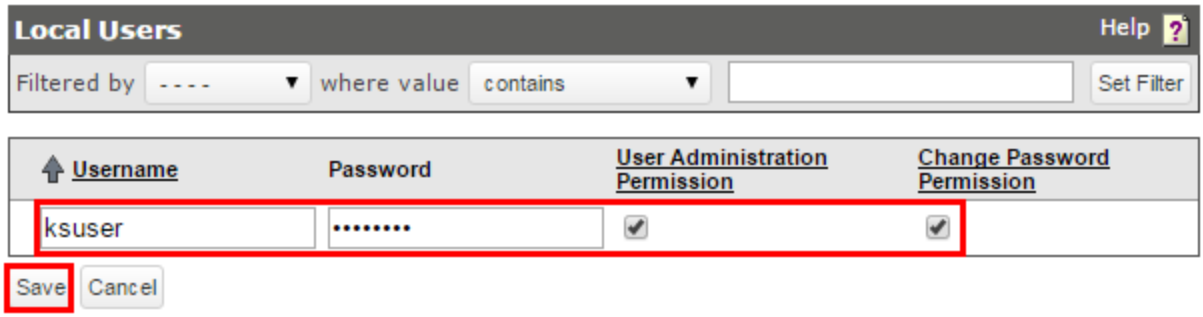
To create a SafeNet KeySecure user:

1. Log on to the **Management Console** as an administrator with Users and Groups access controls.
2. Navigate to the **User & Group Configuration** page (**Security**, **Local Authentication**, **Local Users & Groups**.)

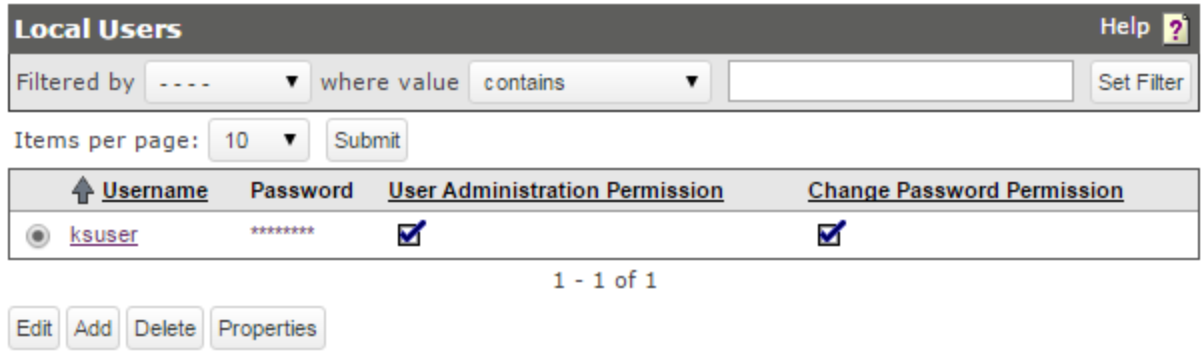


3. Click **Add**.
4. Specify following details.
   – **Username** – Name for the local SafeNet KeySecure user.
   – **Password** – Password for the local SafeNet KeySecure user.

- **User Administration Permission** – Select to grant user administration permissions to the user, if needed.
- **Change Password Permission** – Select to allow the user to change password.



5. Click **Save**. The local SafeNet KeySecure user is created.



You will use this KeySecure user when "Configuring SafeNet ProtectV Manager with SafeNet KeySecure" on page 61.

3
Setting up SafeNet ProtectV Manager

This chapter covers the following information:

Launching SafeNet ProtectV Manager Instance

ProtectV Manager supports Amazon AWS, Microsoft Azure, and IBM Bluemix clouds. It also supports Microsoft Hyper-V and VMware vSphere virtual environments. Launch the ProtectV Manager instance (or virtual machine) in your cloud or virtual environment.

> **Note:** Ensure that port numbers `22`, `443`, and `5432` are open on your ProtectV Manager virtual machines.

> **Note:** It is recommended to launch and configure multiple ProtectV Manager instances to ensure their high availability. If one goes down, another starts providing the services. Refer to "Setting up SafeNet ProtectV Manager Clustering" on page 78 for details.

This section covers the following information:

- "Launching a SafeNet ProtectV Manager VM on vSphere" on page 46
- "Launching a SafeNet ProtectV Manager VM on Hyper-V" on page 48

Launching a SafeNet ProtectV Manager Instance in AWS

Launching a SafeNet ProtectV Manager instance in AWS involves :

1. "Obtaining a Provisioned SafeNet ProtectV Manager AMI" below
2. "Launching a SafeNet ProtectV Manager Instance in AWS" on the next page

Obtaining a Provisioned SafeNet ProtectV Manager AMI

Provisioning builds a customized, AWS region-specific, and confidential ProtectV Manager image. This process is required to place a ProtectV Manager in your target AWS account. Separate provisioning requests must be made if you need multiple ProtectV Managers in one or multiple regions.

From the ProtectV Manager Provisioning user interface, you can customize your AMI for a specific region and add specific boot-authentication security administrators. Only SafeNet-authorized Technical Support Customer Portal users can connect to the ProtectV Manager provisioning web site and gain access to the provisioning system.

To provision a ProtectV Manager:

1. Log on to the Provisioning Server at https://provision.protectv.safenet-inc.com/app with the Technical Support Customer **Portal Username** and **Password** credentials provided by Gemalto, and click **Login**.

   You will land on the **Requests list** tab, which displays any request(s) that you have made, their current status, date of request, region, etc.
2. Click the **New request wizard** tab.
3. Choose a **Product selection** (select ProtectV Manager AWS), and then click **Next**.
4. Choose a **Version selection** (select the latest version), and then click **Next**.
5. Configure these **Environment settings**:
   - Select the **Region** where the ProtectV Manager AMI will be provisioned.
   - Enter the **AWS ID** (Amazon account number) of the user requesting the provisioned ProtectV Manager. Include numbers only—omit dashes, spaces, or leading tab characters.
6. Click **Submit**. The ProtectV Manager provisioning service will now process your request.
7. When the ProtectV Manager image is provisioned, you will receive an e-mail confirmation with a provisioning request number (Request reference ID).

   Note: The **Requests list** tab will display the status of your request. Look for your request reference ID under the **Request ID** column. The status will initially be set to *pending*, then change to *dispatched*, and then to *created* after the image is provisioned.
8. After the image is provisioned, you will receive another e-mail notification with the ProtectV Manager AMI ID. The provisioned ProtectV Manager AMI will be shared with your account for at least two weeks.

Launching a SafeNet ProtectV Manager Instance in AWS

Launch a ProtectV Manager instance using the provisioned ProtectV Manager AMI. Alter launch settings as per your requirements. Ensure to use a security group and a key pair. If they do not already exist, create them during launch.

If client authentication from cloud is required, create an IAM role, as described in the "IAM Roles" section. Assign this IAM role to the ProtectV Manger instance during launch. If this is not done, then client authentication from cloud would not work. You will need to launch a new ProtectV Manager instance to enable the client authentication.

When launching the ProtectV Manager instance in AWS, you may attach a spare volume (disk) of size equal to or greater than the disk selected for the instance. You may also attach the disk later before "Encrypting the ProtectV Manager Disk." The spare disk is needed for moving data before encrypting the disk. After successful encryption, the spare disk may be detached.

Refer to the AWS documentation for details.

The recommended rules for the security group for ProtectV Manager are:

Type	Protocol	Port Range	Source
SSH	TCP	22	0.0.0.0/0
All ICMP	All	N/A	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0
PostgreSQL	TCP	5432	0.0.0.0/0

Note: Rules with source of `0.0.0.0/0` allow all IP addresses to access your instance. It is recommended to set security group rules to allow access from known IP addresses only. Refer to the AWS documentation for details.

Note: Client instances and the ProtectV Manager instance need not be in the same Amazon VPC. However, they must be able to communicate successfully.

Note: ProtectV Manager must have connectivity to AWS EC2 endpoints to call AWS EC2 API DescribeInstances. This API is used for client authentication from cloud and posts requests to AWS EC2 endpoints. Therefore, AWS EC2 endpoints must be accessible from ProtectV Manager.
Refer to http://docs.aws.amazon.com/general/latest/gr/rande.html#ec2_region for details.

After the status of your instance becomes running, you can encrypt the ProtectV Manager disk, as described in "Encrypting the ProtectV Manager Disk." After encrypting the disk, you can configure ProtectV Manager, as described in "Configuring SafeNet ProtectV Manager Instance" on page 60.

Launching a SafeNet ProtectV Manager VM in Azure

Launch a ProtectV Manager VM in Microsoft Azure. Alter launch settings as per your requirements. Refer to the Azure documentation for details.

To launch a ProtectV Manager VM:

1. Sign in to the Azure portal.

2. On the **Hub** menu, click **New**. The **New** page appears.
3. Click **See all** next to **MARKETPLACE**. The **Marketplace** page appears.
4. Under **Everything** on the right, search for **SafeNet ProtectV** in the **Search Everything** field. Available SafeNet ProtectV images are displayed.
5. Click an option to view its details on the right.
6. Click the option that suits your requirements.
7. On the right, at the bottom, click **Create** . The **Basics** screen of the **Create virtual machine** page is displayed.
8. Specify a **Name** for your virtual machine.
9. Specify **pvadmin** as **User name**. This creates a local account on the ProtectV Manager VM. The account is used to log on to and manage the ProtectV Manager VM.
10. Under **Authentication type**, click **SSH public key**. The **SSH Public Key** field appears below.

> **Note:** Do not use password-based authentication.

11. Paste the **SSH Public Key**.
12. Select the **Subscription** type.
13. Select an existing **Resource group** or enter the name for a new one.
14. Specify the **Location** of an Azure datacenter. For example, East US.
15. Click **OK**. The **Choose a size** screen is displayed.
16. Select a size for the VM. Select at minimum **Standard A2** size.
17. Click **Select** to continue. The **Settings** screen is displayed.
18. Specify the storage and networking options. Accept the default settings or change them according to your requirements.
19. Click **OK**.
20. Click **Summary** to review the launch settings.
21. Click **OK** to launch the VM.

> **Note:** Ensure that port numbers 22, 443, and 5432 are open on your ProtectV Manager VM.

The ProtectV Manager VM will be launched in Azure. While Azure creates the VM, you can track the progress under Virtual Machines in the Hub menu.

When the ProtectV Manager VM is launched in Microsoft Azure, you can encrypt the ProtectV Manager disk, as described in "Encrypting the ProtectV Manager Disk." After encrypting the disk, you can configure ProtectV Manager, as described in "Configuring SafeNet ProtectV Manager Instance" on page 60.

Launching a SafeNet ProtectV Manager VM in IBM Bluemix

To launch the ProtectV Manager VM in the IBM Bluemix cloud:

1. Log on to https://control.softlayer.com/.
   - Enter your **Username**.

- Enter **Password**.
- Click **Log In**.

2. Navigate to the **Image Templates** screen (**Devices** > **Manage** > **Images**.)
3. Images in your account appear under the **Template Name** column.
4. On the right, click **Actions** corresponding to the ProtectV Manager image. A shortcut menu appears.
5. Click an option as per your requirements. For example, click **Order Monthly Virtual Server** or **Order Hourly Virtual Server**. The **IBM Bluemix** window appears. In this window, configure your Cloud Server, as follows.
6. Select the **Location** of your **Data Center**. This field is mandatory.
7. Specify the **System Configuration**, as follows:
   - **Computing Instance** (this configuration is mandatory)
   - **RAM** (this configuration is mandatory)
   - **Operating System** (Ubuntu Linux 14.04 LTS is the supported operating system)
   - **First Disk**, **Second Disk**, **Third Disk**, **Fourth Disk**, and **Fifth Disk** (as per your requirements)
8. Specify the **Network Options**.
   - **Public Bandwidth**
   - **Uplink Port Speeds**
   - **Public Secondary IP Addresses**
   - **Primary IPv6 Addresses**
   - **Public Static IPv6 Addresses**
9. Specify the **System Addons**. Specify **Hardware & Software Firewalls**.
10. Specify the **Storage Addons**.
11. Specify the **Service Addons** – **Monitoring**, **Response**, and **Insurance**.
12. Click **ADD TO ORDER**. The **Verification** popup appears verifying the order.

    After the order is verified, the **CHECKOUT** page is displayed. Verify the configuration of your cloud server. If required reconfigure System Configuration, Network Options, and Service Addons.
13. Under the **Advanced System Configuration** section, specify the following:
    - **SSH Keys**: Select an SSH key from the drop-down list. If no key already exists, click Add to create a new key. Refer to the Bluemix documentation for instructions on creating a key.
    - **Host and Domain Names:** Specify **Hostname**, for example, `testpvm`. Also specify **Domain**, for example, `pvm.com`.
14. Verify the billing information.
15. Scroll up the page.
16. On the right, select the following check boxes:
    - **I acknowledge that the Cloud Service terms apply to this order**
    - **I have read and agree to the Third-Party Service Agreement listed below**
17. Click **Submit Order**.

The **Placing Order** popup box appears. After the order is placed successfully, the **ORDER CONFIRMED** screen is displayed. It displays the confirmation message with your order number.

Navigate to the Devices page (Devices > Devices List.) Your newly launched ProtectV Manager VM (for example, `testpvm.pvm.com`) should be available under the Device Name column. The Devices page shows details such as Device Name, Device Type, Location, Start Date, Public IP, and Private IP of your machine.

> **Note:** Ensure that port numbers `22`, `443`, and `5432` are open on your ProtectV Manager VM.

After successful deployment, you can configure ProtectV Manager, as described in "Configuring SafeNet ProtectV Manager Instance" on page 60.

Launching a SafeNet ProtectV Manager VM on vSphere

SafeNet ProtectV package includes an Open Virtual Appliance (OVA) file to help launch a ProtectV Manager VM on vSphere.

When launching the ProtectV Manager VM on vSphere, you may attach a spare volume (disk) of size equal to or greater than the disk selected for the VM. You may also attach the disk later before "Encrypting the ProtectV Manager Disk." The spare disk is needed for moving data before encrypting the disk. After successful encryption, the spare disk may be detached. Refer to the VMware documentation for details on attaching a spare disk to a VM.

This section provides basic instructions to launch a ProtectV Manager VM on vSphere. Refer to the VMware documentation for details on launching a VM on vSphere.

> **Note:** ProtectV Manager supports VMware vSphere/ESXi v5.1 and higher versions. To deploy ProtectV Manager on vSphere/ESXi v5.0 or lower versions, change the virtual machine's hardware version from `vmx-09` to `vmx-08`/`vmx-07`. Use the VMware OVF Tool to change the version in the OVA file.

> **Note:** The default size of a ProtectV Manager's file system (system disk) is 16 GB even if the disk is larger. If needed, you can resize the system disk to use the extended space and create the swap file system on an extended logical volume on VMware vSphere. Refer to "Resizing the System Disk of ProtectV Manager" on page 142 for details.

This section covers the following information:

- "Launching a ProtectV Manager VM Using the Windows Client" below
- "Launching a SafeNet ProtectV Manager VM Using the Web Client" on the next page
- "Troubleshooting" on page 48

Launching a ProtectV Manager VM Using the Windows Client

On vSphere versions older than 6.5, you can launch VMs using the vSphere Windows Client and the Web Client. This section provides instructions to launch a ProtectV Manager VM using the Windows Client.

To launch a ProtectV Manager VM:

1. Open **vSphere Client**.

2. Click **File** > **Deploy OVF Template...** The **Deploy OVF Template** dialog box appears. The **Source** screen of the dialog box is displayed.
3. Specify the location of the OVA file from Gemalto. Use either of the following:
   - Specify the URL to the OVA file.
   - Specify a location using **Browse** button. Click **Browse** to navigate to the OVA file, select the OVA file, and click **Open**.
4. Click **Next**. The **OVF Template Details** screen is displayed.
5. Verify the template details. If needed, navigate back and select the correct OVA file.
6. Click **Next**. The **Name and Location** screen is displayed.
7. Specify a name for the VM. The default name is **ProtectV**.
8. Under the **Inventory Location** section, select the location for the VM.
9. Click **Next**. The **Host / Cluster** screen is displayed.
10. Select the host or cluster where you want to run the VM.
11. Click **Next**. The **Resource Pool** screen is displayed.
12. Select the resource pool in which you want to deploy the VM.
13. Click **Next**. The **Storage** screen is displayed.
14. Select the location to store the VM files.
15. Click **Next**. The **Disk Format** screen is displayed.
16. Select the format in which you want to store the virtual disks.
17. Click **Next**. The **Network Mapping** screen is displayed. The screen displays the default network mapping for the ProtectV Manager VM.
18. Click **Next**. The **Ready to Complete** screen is displayed.
19. Verify the deployment settings. If needed, navigate back and make the required changes.
20. Select **Power on after deployment**.
21. Click **Finish**. Deployment starts and may take a few minutes to complete.

Note: Ensure that port numbers `22`, `443`, and `5432` are open on your ProtectV Manager VM.

After successful deployment, the ProtectV Manager VM appears under the inventory folder in the left pane. Check the IP address of the VM under the Summary tab. When the ProtectV Manager VM is launched on vSphere, you can encrypt the ProtectV Manager disk, as described in "Encrypting the ProtectV Manager Disk." After encrypting the disk, you can configure ProtectV Manager, as described in "Configuring SafeNet ProtectV Manager Instance" on page 60.

Launching a SafeNet ProtectV Manager VM Using the Web Client

Some versions of the vSphere Web clients do not support deployment of OVA files directly. It is recommended to extract the `.ovf`, `.vmdk`, and `.mf` files from the OVA file using the VMware OVF Tool. You can then launch the ProtectV Manager VMs using the extracted files.

To extract files from the OVA file, run:

```
ovftool.exe --lax <source_OVA_file> <destination_OVF_file>
```

Here,

- `<source_OVA_file>`: Represents the OVA file included in the SafeNet ProtectV package.
- `<destination_OVF_file>`: Represents a name for the OVF file.

When launching the ProtectV Manager VM, specify location of the extracted files on the Source screen of the Deploy OVF Template dialog box. Refer to "Launching a ProtectV Manager VM Using the Windows Client" on page 46 for complete walkthrough of the Deploy OVF Template dialog box.

After successful deployment, the ProtectV Manager VM appears under the inventory folder in the left pane. Check the IP address of the VM under the Summary tab. When the ProtectV Manager VM is launched on vSphere, you can encrypt the ProtectV Manager disk, as described in "Encrypting the ProtectV Manager Disk." After encrypting the disk, you can configure ProtectV Manager, as described in "Configuring SafeNet ProtectV Manager Instance" on page 60.

Troubleshooting

After deployment, if ProtectV Manager cannot get the IP address, an error occurs, or you want to change the configuration parameters, perform the following steps:

1. Shut down the virtual machine.
2. Right-click the virtual machine.
3. Click **Edit Settings**. The **Virtual Machine Properties** dialog box appears.
4. Click the **Options** tab.
5. Under the **Settings** column, click **vApp Options**. The **Properties**, **IP Allocation Policy**, **OVF Settings**, and **Advanced** settings appear under **vApp Options**.
6. Click **Properties**. The **vApp Property Configuration** section appears on the right.
7. Update the values of **IP address**, **Netmask**, **Gateway**, **Primary DNS server**, and **Secondary DNS server** appropriately.
8. Power on the virtual machine.

Launching a SafeNet ProtectV Manager VM on Hyper-V

SafeNet ProtectV package includes a Virtual Hard Disk (VHD) file to help launch a ProtectV Manager VM on Hyper-V. The VHD file comes in a zipped file. Extract the zip file and store the VHD file at a location accessible from your Hyper-V Manager.

When launching the ProtectV Manager VM on Hyper-V, you may attach a spare volume (disk) of size equal to or greater than the disk selected for the VM. You may also attach the disk later before "Encrypting the ProtectV Manager Disk." The spare disk is needed for moving data before encrypting the disk. After successful encryption, the spare disk may be detached. Refer to the Hyper-V documentation for details on attaching a spare disk to a VM.

This section provides basic instructions to launch a ProtectV Manager VM on Hyper-V. Refer to the Hyper-V documentation for details on launching a VM on Hyper-V.

To launch a ProtectV Manager VM:

1. Open **Hyper-V Manager**.
2. Under the **Actions** section on right, click **New**. A shortcut menu appears.
3. Click **Virtual Machine...** on the shortcut menu. The **Before You Begin** screen of the **New Virtual Machine Wizard** is displayed.

4. Click **Next** to continue. The **Specify Name and Location** screen of the **New Virtual Machine Wizard** is displayed.
5. Specify a **Name** for the virtual machine.
6. Click **Next** to continue. The **Assign Memory** screen of the **New Virtual Machine Wizard** is displayed.
7. Assign at least **2048** MB **Startup memory**.
8. Click **Next** to continue. The **Configure Networking** screen of the **New Virtual Machine Wizard** is displayed.
9. Select a network adapter from the **Connection** drop-down list.
10. Click **Next** to continue. The **Connect Virtual Hard Disk** screen of the **New Virtual Machine Wizard** is displayed.
11. Select **Use an existing virtual hard disk**.
12. Specify the **Location** of the VHD file from Gemalto. Use either of the following:
    - Specify the path to the VHD file.
    - Specify a location using **Browse** button. Click **Browse** to navigate to the extracted VHD file, select the file, and click **Open**.
13. Click **Next** to continue. The **Completing the New Virtual Machine Wizard** screen of the **New Virtual Machine Wizard** is displayed.
14. Review the details. If needed, navigate back and make the required changes.
15. Click **Finish**. The wizard is closed and the ProtectV Manager virtual machine is created.

> **Note:** Ensure that port numbers `22`, `443`, and `5432` are open on your ProtectV Manager VM.

After a ProtectV Manager VM is successfully created, it appears under the Virtual Machines inventory. Start the VM and note down its IP address. When ProtectV Manager is launched in a non-DHCP environment, it cannot get an IP address automatically. In this case, assign a static IP address to it, as described in "Assigning IP Addresses to ProtectV Manager on Hyper-V and VMware" on the next page for details.

After the IP address is available, you can (optionally) encrypt the ProtectV Manager disk, as described in "Encrypting the ProtectV Manager Disk." After encrypting the disk, you can configure ProtectV Manager, as described in "Configuring SafeNet ProtectV Manager Instance" on page 60.

Logging on to SafeNet ProtectV Manager Instance

After your ProtectV Manager instance is launched, you can log on to it as the `pvadmin` user, as described below.

- On Hyper-V and vSphere, log on using the default password, `pvadmin`. You can change the password later by running `passwd pvadmin`. Remember this password. You will need this password on subsequent logons.

  Alternatively, you can log on as `pvadmin` using the SSH key.
- In AWS, Azure, and Bluemix, log on as `pvadmin` using the SSH key generated/used during launch.

Assigning IP Addresses to ProtectV Manager on Hyper-V and VMware

After ProtectV Manager is deployed on Hyper-V or VMware, by default, an IP address is assigned to it if DHCP is offered. However, if it cannot obtain the IP address, or when DHCP is not offered, you can assign static or dynamic IP addresses to its Network Interface Cards (NICs.) In case of dual NICs, you can either assign static IP addresses to both NICs, or a static IP address to one NIC while a dynamic IP address to the other NIC using DHCP. Both the NICs cannot be assigned dynamic IP addresses.

This section covers the following information:

Assigning IP Address to ProtectV Manager with Single NIC

This section covers the following information:

Assigning Static IP Address to ProtectV Manager with Single NIC

To assign a static IP address to a ProtectV Manager instance with single NIC:

1. Log on as `pvadmin`. This is the default user. Refer to "Logging on to SafeNet ProtectV Manager Instance" on the previous page for details.
2. View the network settings.

   Run: `sudo pvmctl networkpvm show`

   This command displays the current network configuration. If no network interface is available, a message appears stating that no network interface is available for configuration.
3. Configure the network settings:

   Run: `sudo pvmctl networkpvm static --interface=INTERFACE --ipaddr=IPADDR --nwmask=NWMASK --gateway=GATEWAY --defaultgw=DEFAULTGW --dns1=DNS1 --dns2=DNS2`

   Here,

   - `INTERFACE` – Network interface to configure. In case of single network interface, set `--interface=eth0`.
   - `IPADDR` – Static IP address to assign.
   - `NWMASK` – IP address of the network mask.
   - `GATEWAY` – IP address of the network gateway.
   - `DEFAULTGW` – Specify that network gateway is the default gateway. In case of single network interface, set `--defaultgw=yes`.
   - `DNS1` – *(Optional)* IP address of the primary DNS server, if configured.
   - `DNS2` – *(Optional)* IP address of the secondary DNS server, if configured.

For example, run:

```
sudo pvmctl networkpvm static --interface=eth0 --ipaddr=10.164.8.89 --
nwmask=255.255.248.0 --gateway=10.164.8.3 --defaultgw=yes
```

The network configuration is saved.

4. Apply the static configuration changes.

   Run: `sudo pvmctl networkpvm start`

5. Verify the changes.

   Run: `sudo pvmctl networkpvm show`

   For example:

```
sudo pvmctl networkpvm show
INTERFACE=eth0
MODE=static
IPADDRESS=10.164.8.89
NETMASK=255.255.248.0
GATEWAY=10.164.8.3
```

> **Note:** In future, if you want to switch to DHCP, run: `pvmctl networkpvm dhcp --interface=INTERFACE`

Assigning Dynamic IP Address to ProtectV Manager with Single NIC

> **Note:** You may skip this section if DHCP is offered in your environment. In this case, an IP address is automatically assigned to your ProtectV Manager.

To assign dynamic IP address to a ProtectV Manager instance with single NIC:

1. Log on as `pvadmin`. This is the default user. Refer to "Logging on to SafeNet ProtectV Manager Instance" on page 49 for details.
2. View the network settings.

   Run: `sudo pvmctl networkpvm show`

   This command displays the current network configuration. If no network interface is available, a message appears stating that no network interface is available for configuration.

3. Configure the network settings:

   Run: `sudo pvmctl networkpvm dhcp --interface=INTERFACE`

   Here, `INTERFACE` represents the network interface to configure. In case of single network interface, set `--interface=eth0`.

   For example, run:

```
sudo pvmctl networkpvm dhcp --interface=eth0
```

   A dynamic IP address is assigned to the ProtectV Manager console using DHCP.

4. Verify the changes.

   Run: `sudo pvmctl networkpvm show`

   For example:

   ```
   sudo pvmctl networkpvm show
   INTERFACE=eth0
   MODE=dhcp
   ```

Assigning IP Addresses to ProtectV Manager with Dual NICs

When a ProtectV Manager instance has dual NICs (`eth0` and `eth1`,) you may either assign static IP addresses to both the NICs, or assign a static IP address to one NIC while a dynamic IP address to the other NIC.

This section covers the following information:

- "Assigning Static and Dynamic IP Addresses to ProtectV Manager with Dual NICs" below
- "Assigning Static IP Addresses to Both NICs of ProtectV Manager" on the next page

Assigning Static and Dynamic IP Addresses to ProtectV Manager with Dual NICs

This section describes steps to assign a static IP address to `eth0` and a dynamic IP address to `eth1`.

To assign IP addresses to a ProtectV Manager instance with dual NICs:

1. Log on as `pvadmin`. This is the default user. Refer to "Logging on to SafeNet ProtectV Manager Instance" on page 49 for details.
2. View the network settings.

   Run: `sudo pvmctl networkpvm show`

   This command displays the current network configuration. If no network interface is available, a message appears stating that no network interface is available for configuration.
3. Configure static network configurations for `eth0`:

   Run: `sudo pvmctl networkpvm static --interface=INTERFACE --ipaddr=IPADDR --nwmask=NWMASK --gateway=GATEWAY --defaultgw=DEFAULTGW --dns1=DNS1 --dns2=DNS2`

   Here,

   - `INTERFACE` – Network interface to configure. In this example, `--interface=eth0`.
   - `IPADDR` – Static IP address to assign.
   - `NWMASK` – IP address of the network mask.
   - `GATEWAY` – IP address of the network gateway.
   - `DEFAULTGW` – Specify that network gateway is the default gateway. In this example, set `--defaultgw=yes`.

   Note: If the IP address on the other NIC is already assigned using DHCP, then set `--defaultgw=no`.

   - `DNS1` – *(Optional)* IP address of the primary DNS server, if configured.
   - `DNS2` – *(Optional)* IP address of the secondary DNS server, if configured.

For example, run:

```
sudo pvmctl networkpvm static --interface=eth0 --ipaddr=10.164.8.89 --
nwmask=255.255.248.0 --gateway=10.164.8.3 --defaultgw=yes
```

The network configuration is saved.

4. Apply the static configuration changes.

   Run: `sudo pvmctl networkpvm start`

   The specified IP address is assigned to `eth0` of the ProtectV Manager instance.

5. Assign the IP address using DHCP:

   Run: `sudo pvmctl networkpvm dhcp --interface=INTERFACE`

   For example, run:

   ```
   sudo pvmctl networkpvm dhcp --interface=eth1
   ```

   A dynamic IP address is assigned to `eth1` of the ProtectV Manager instance.

6. Verify the changes.

   Run: `sudo pvmctl networkpvm show`

Assigning Static IP Addresses to Both NICs of ProtectV Manager

This section describes steps to assign static IP addresses to both NICs (`eth0` and `eth1`) of the ProtectV Manager instance.

To assign static IP addresses to both NICs of a ProtectV Manager instance:

1. Log on as `pvadmin`. This is the default user. Refer to "Logging on to SafeNet ProtectV Manager Instance" on page 49 for details.

2. View the network settings.

   Run: `sudo pvmctl networkpvm show`

   This command displays the current network configuration. If no network interface is available, a message appears stating that no network interface is available for configuration.

3. Configure static network configurations for `eth0`:

   Run: `sudo pvmctl networkpvm static --interface=INTERFACE --ipaddr=IPADDR --nwmask=NWMASK --gateway=GATEWAY --defaultgw=DEFAULTGW --dns1=DNS1 --dns2=DNS2`

   Here,

   - `INTERFACE` – Network interface to configure. For `eth0`, set `--interface=eth0`.
   - `IPADDR` – Static IP address to assign.
   - `NWMASK` – IP address of the network mask.
   - `GATEWAY` – IP address of the network gateway.
   - `DEFAULTGW` – Specify that network gateway is the default gateway. In this example, set `--defaultgw=yes`.
   - `DNS1` – *(Optional)* IP address of the primary DNS server, if configured.
   - `DNS2` – *(Optional)* IP address of the secondary DNS server, if configured.

   For example, run:

```
sudo pvmctl networkpvm static --interface=eth0 --ipaddr=10.164.8.89 --
nwmask=255.255.248.0 --gateway=10.164.8.3 --defaultgw=yes
```

The network configuration is saved.

4. Configure static network configurations for `eth1`:

   Run: `sudo pvmctl networkpvm static --interface=INTERFACE --ipaddr=IPADDR --nwmask=NWMASK --gateway=GATEWAY --defaultgw=DEFAULTGW --dns1=DNS1 --dns2=DNS2`

   Here,

   - `INTERFACE` – Network interface to configure. For `eth1`, set `--interface=eth1`.
   - `IPADDR` – Static IP address to assign.
   - `NWMASK` – IP address of the network mask. This network mask is different than the network mask specified for `eth0` above.
   - `GATEWAY` – IP address of the network gateway. This gateway is different than the gateway specified for `eth0` above.
   - `DEFAULTGW` – Specify that network gateway not is the default gateway for `eth1`. As you already set the default gateway for `eth0` above, for `eth1`, set `--defaultgw=`**`no`**.
   - `DNS1` – *(Optional)* IP address of the primary DNS server, if configured.
   - `DNS2` – *(Optional)* IP address of the secondary DNS server, if configured.

   For example, run:

   ```
   sudo pvmctl networkpvm static --interface=eth1 --ipaddr=10.164.8.90 --
   nwmask=255.255.248.0 --gateway=10.164.8.4 --defaultgw=no
   ```

   The network configuration is saved.

5. Apply the static configuration changes for both NICs.

   Run: `sudo pvmctl networkpvm start`

   The specified IP addresses and network configurations are assigned to both NICs of the ProtectV Manager instance.

6. Verify the changes.

   Run: `sudo pvmctl networkpvm show`

Clearing Network Configurations

Whenever needed, clear the existing network configurations using the `pvmctl networkpvm clear` command. You can reconfigure the network interface later.

Before clearing network configurations, stop the ProtectV Manager instance by using the `pvmctl stoppvm` command.

To clear the existing network configurations, run:

```
sudo pvmctl networkpvm clear --interface=INTERFACE
```

For example, run:

```
sudo pvmctl networkpvm clear --interface=eth0

Network configuration cleared for eth0
```

Encrypting the SafeNet ProtectV Manager Disk

After the ProtectV Manager instance is launched, you can encrypt its disk before further use. You may skip the encryption if you want to do it later. The process of encrypting the ProtectV Manager disk can be divided into two stages – preparing and encrypting.

This section covers the following information:

1. Preparing for Disk Encryption
2. Encrypting the Disk
3. Unlocking the Encrypted Disk
4. When the Authorized SSH Key is Changed
5. Changing the preboot Password
6. Changing the Disk Encryption Password

Preparing for Disk Encryption

To prepare for the disk encryption:

1. Log on to your ProtectV Manager instance as `pvadmin`. Refer to "Logging on to SafeNet ProtectV Manager Instance" on page 49 for details.

> **Note:** On successful log on, read the End User License Agreement in the `eula.txt` file placed at `/home/pvadmin/`. By using this software, you are consenting to the agreement.
> – To view the list of allowed commands, run the `help` or `?` command.
> – The allowed `sudo` commands are `pvmctl`, `reboot`, `halt`, and `timedatectl`.
> – Use the `timedatectl` command to set system time, date, or time zone.

2. Check the disk encryption status.

   Run: `sudo pvmctl encryptpvm status`

   This command reports whether the ProtectV Manager disk is encrypted.

   For example:

   ```
   sudo pvmctl encryptpvm status

   Disk is not encrypted.
   ```

   The output shows that the disk is not yet encrypted.

3. Check for the available disks.

   Run: `lsblk`

   For example:

   ```
   NAME                                MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
   xvda                                202:0    0     8G  0 disk
   └─xvda1                             202:1    0     8G  0 part /
           xvdb                                202:16   0     8G  0 disk
   loop0                                 7:0    0   100G  0 loop
   └─docker-202:1-149965-pool (dm-0)   252:0    0   100G  0 dm
   loop1                                 7:1    0     2G  0 loop
   └─docker-202:1-149965-pool (dm-0)   252:0    0   100G  0 dm
   ```

In the output above, `xvdb`, represents the spare disk that you attached to the instance (when launching the ProtectV Manager instance in AWS.) This disk will be needed during encryption of the ProtectV Manager disk. Ensure that the size of the spare disk is greater than or equal to the ProtectV Manager disk to be encrypted (in our example, `xvda`.)

Note: The name of the spare disk may be different on your instance.

Note: VMs launched in Microsoft Azure already have an additional disk. You may not need a spare disk when launching the ProtectV Manager VM in Azure. If needed, you can attach the spare disk anytime. Refer to the Azure documentation for details.

Similarly, encrypting the ProtectV Manager disk on vSphere also requires a spare disk. You can attach a spare disk before encrypting the disk. Refer to the VMware documentation for details.

4. Prepare the extra disk for encryption.

   Run: `sudo pvmctl encryptpvm prepare --sparedisk=<spare-disk-name>`

   This command prepares ProtectV Manager to encrypt the root disk on next reboot. The command requires a spare disk (for example, xvdb, xvdc, or xvdf) of same or greater size to be attached before run. An encrypted ProtectV Manager will wait for login from the `pboot` user every time it boots.

   For example:

   ```
   sudo pvmctl encryptpvm prepare --sparedisk=xvdb
   Disk is not encrypted.
   Disk is set for encryption on next reboot.
   Please reboot the system and login as 'pboot' user.
   ```

   The output shows that the disk is set for encryption on next reboot. After reboot, you will need to log on as `pboot` for proceeding with encryption.

   Note: After reboot, if you do not log on to ProtectV Manager as `pboot` for five minutes, ProtectV Manager automatically boots to the OS mode.

5. Reboot the ProtectV Manager instance.

   Run: `sudo reboot`

Changing How IP Address is Assigned to ProtectV Manager on vSphere

On VMware vSphere, when launching your ProtectV Manager virtual machine, you can assign either a static or dynamic IP address to it. ProtectV Manager enters into preboot using this IP address. However, if you later want to change how the IP address is assigned to your ProtectV Manager, refer to "Assigning IP Addresses to ProtectV Manager on Hyper-V and VMware" on page 50.

Encrypting the Disk

After the ProtectV Manager instance is rebooted successfully, your disk is ready for encryption. You can now encrypt the ProtectV Manager disk.

WARNING! It is strongly recommended to take full backup of ProtectV Manager before proceeding with disk encryption. However, if you are encrypting the disk just after the launch of the ProtectV Manager instance, no need to take backup.

SafeNet ProtectV provides two methods to encrypt the ProtectV Manager instance – interactive and non-interactive (command-line.) The interactive method is helpful to understand the encryption process. The non-interactive method is useful for automating the encryption.

Proceed with the encryption method that suits your requirements.

- Interactive Encryption
- Non-interactive Encryption

Interactive Encryption

Note: When encrypting the ProtectV Manager disk in VMware environment, use an `SSH` utility (for example, `PuTTY`) to monitor the progress of the encryption process. The vSphere VM console does not show the encryption progress.

To encrypt the ProtectV Manager disk:

1. Log on to your ProtectV Manager instance as `pboot`.
   - On the ProtectV Manager VM on Hyper-V and vSphere, log on using the default password, `pboot`. You can change the password later, as described in "Changing the preboot Password" on page 59.
   - On the ProtectV Manager instance in Azure and AWS, log on as `pboot` using the SSH key generated/used during launch.

   Note: Every time the ProtectV Manager instance is rebooted, you must log on as `pboot`.

   When you log on as the `pboot` user, ProtectV Manager's **PreBoot Shell** is displayed, as shown below:

```
-------------------------------------------------
Welcome to PreBoot Shell
e : encrypt and reboot
s : skip doing encryption, proceed to regular boot procedure
Select option :
```

   Note: If you want to encrypt the disk, type `e`. To skip encrypting the disk and proceed with normal booting, type `s`. You will be exited from the **PreBoot Shell**. You can now log on as `pvadmin`. You can encrypt the disk later.

2. Type `e` to start encryption.

```
Select option : e
-------------------------------------------------------
WARNING: Abnormal events like power or network failure,
ssh session termination etc may cause ALL data to be lost.
IT IS STRONGLY RECOMMENDED TO TAKE FULL BACKUP BEFORE
PROCEEDING FURTHER.
-------------------------------------------------------
```

```
Type YES to proceed or anything else to skip :
```

3. Type `YES` (case-sensitive) to proceed.

> **CAUTION:** `YES` is case-sensitive. Entering `yes` or `Yes` will close the `ssh` session.

When prompted, enter and confirm password. Remember this password . You need this password to unlock the disk on every reboot. You can change this password later. Refer to "Changing the Disk Encryption Password" on page 60 for details.

> **CAUTION:** Do not close your `ssh` session until encryption completes. Interruption may lead to system not booting up the next time.

```
Type YES to proceed or anything else to skip : YES
Please enter password :
Please confirm password :
Please remember the password.
You will need it to unlock disk every time system boots up.
** Please do not close your ssh session until encryption completes.
Interruption may lead to system not booting up next time.
Step 1 of 3 : 629 seconds elapsed ... done
Step 2 of 3 : 158 seconds elapsed ... done
Step 3 of 3 ... done
```

Depending on the disk size, disk encryption may take 5-10 minutes to complete.

The following output indicates that the disk is encrypted successfully:

```
All steps executed successfully.
ok: Encryption successful.
System will reboot. Please login again to unlock disk.
```

> **Note:** After the ProtectV manager disk is encrypted, you must log on as `pboot` every time the ProtectV Manager instance is rebooted.

After successful reboot, log on as `pboot` to unlock the encrypted disk, as described in "Unlocking the Encrypted Disk."

Non-interactive Encryption

To encrypt the ProtectV Manager disk non-interactively:

Run: `ssh -i <key_pair_name> pboot@<ProtectV Manager IP address> '<password>'`

For example, run:

```
ssh -i AB_Key_Pair1.pem pboot@54.208.156.186 'password'
```

After successful encryption, the system will reboot. After successful reboot, log on as `pboot`, as described in "Unlocking the Encrypted Disk."

Unlocking the Encrypted Disk

After successful reboot, log on as `pboot`to unlock the encrypted disk. You will need to enter the password that was set when encrypting the disk, as shown below.

```
Welcome to PreBoot Shell
Disk is encrypted.
Please enter password to unlock disk :
ok: Disk unlocked successfully.
Proceeding to regular boot procedure.
Please login with os-mode user.
```

After the output shown above, your SSH session will be closed. The disk is now unlocked. You can now log on to ProtectV Manager as `pvadmin` and configure the ProtectV Manager, as described in "Configuring SafeNet ProtectV Manager Instance."

Note: To unlock the ProtectV Manager disk non-interactively, run: `ssh -i <key_pair_name> pboot@<ProtectV Manager IP address> '<password>'`

For example, run: `ssh -i AB_Key_Pair1.pem pboot@54.208.156.186 'password'`

Note: If you had started the ProtectV Manager service before encrypting the disk, you need to rerun the `pvmctl startpvm` command after unlocking the disk. Refer to "Starting the SafeNet ProtectV Manager Service" on page 65.

When the Authorized SSH Key is Changed

After the disk encryption, if the authorized SSH key used to log on to ProtectV Manager is changed, you need to update the preboot environment. To do so:

Run: `sudo pvmctl encryptpvm updateprebootauthkeys`

This command updates the preboot environment with the SSH authorized key file in your home directory. Next reboot onward, the PreBoot Shell will allow login from the updated keys.

Note: Run the `sudo pvmctl encryptpvm updateprebootauthkeys` command only if the disk is already encrypted.

CAUTION: Do not to make the authorized SSH key file empty; otherwise, the system may not allow you to login.

Changing the preboot Password

It is recommended to change the default password of the `preboot` user. You can change the password whenever needed. To do so:

Run: `sudo pvmctl encryptpvm updateprebootuserpass --prebootpass="PREBOOTPASS"`

In this command, `"PREBOOTPASS"` indicates the new password.

CAUTION: The new password must be greater than or equal to eight characters. Remember this password. You will need this password when logging on subsequently.

Changing the Disk Encryption Password

It is recommended to change the disk encryption password regularly. You can change the password whenever needed.

To do so, run:

```
sudo pvmctl encryptpvm updatediskpass --oldpass="OLDPASS" --newpass="NEWPASS"
```

Here,

- `"OLDPASS"` – Existing disk encryption password.
- `"NEWPASS"` – New password for disk encryption.

If passwords are not specified when running the `sudo pvmctl encryptpvm updatediskpass` command, you will be prompted for existing and new passwords during the command run. When prompted, enter and confirm the new password. Remember this password . You need this password to unlock the disk on every reboot.

Note: Disk encryption is specific to a ProtectV Manager instance. Disk of one cluster member might be encrypted; while the disk of other cluster members might not be encrypted. Changing the disk encryption password of a cluster member does not impact other cluster members. You can change the disk encryption password for cluster members individually.

Refer to "Setting up SafeNet ProtectV Manager Clustering" on page 78 for details on ProtectV Manager clustering.

Configuring SafeNet ProtectV Manager Instance

When the ProtectV Manager AMI is launched, a ProtectV Manager is launched with PVMDB, ProtectV Gateway, and REST server.

You can either use the local ProtectV Gateway launched with ProtectV Manager or launch a separate instance using the ProtectV Manager AMI, referred to as external ProtectV Gateway.

- If you plan to use an external ProtectV Gateway, manual configuration is required. Refer to "Setting up SafeNet ProtectV Gateway" on page 85 for details.
- If you plan to use the local ProtectV Gateway, you do not have to launch it explicitly; it is launched with ProtectV Manager. Configuring the ProtectV Manager instance with local ProtectV Gateway involves:

  a. "Configuring SafeNet ProtectV Manager with SafeNet KeySecure" on the next page

  b. "Starting the SafeNet ProtectV Manager Service" on page 65

  These steps are described in subsequent sections.

Note: The ProtectV Manager logs are saved at `/pvm/logs`.
Some PuTTY settings may make `lshell` exit on pressing `CTRL+C` for a `tail -f /pvm/logs/<file>` command. Use `CTRL+Z` instead.

Configuring SafeNet ProtectV Manager with SafeNet KeySecure

While configuring ProtectV Manager with SafeNet KeySecure, you can specify authentication type. ProtectV supports both password-based authentication and client certificate authentication. You can select an option that suits your requirements, or use both.

> **Note:** This section provides instructions to configure ProtectV Manager when both password and client certificate authentication are required.

With SafeNet ProtectV, you can configure client certificate authentication using own (imported) client certificates and private keys or client certificates and private keys created using the `pvmctl` utility. Depending on your requirements, refer to the following sections:

- "Configuring SafeNet ProtectV Manager using Client Certificates Created through pvmctl" on page 63
- "Configuring SafeNet ProtectV Manager using Imported Client Certificates" below

Configuring SafeNet ProtectV Manager using Imported Client Certificates

> **Note:** The CN (Common Name) must be the same in server and client certificates, and the same user must exist on SafeNet KeySecure.

To configure ProtectV Manager with SafeNet KeySecure using an imported client certificate:

1. Create your client Certificate Signing Request (CSR) and private key.
2. Copy the text of the generated client CSR. The copied text must include the header (`-----BEGIN CERTIFICATE REQUEST-----`) and footer (`-----END CERTIFICATE REQUEST-----`).
3. On SafeNet KeySecure, sign the client CSR with the local CA, as follows:
   a. Log on to the **Management Console** as an administrator with Certificates and Certificate Authorities access controls.
   b. Navigate to the **Local Certificate Authority List** (**Security**, **Device CAs & SSL Certificates**, **Local CAs**.)
   c. Select the local CA. This is the local CA that you created in "Creating a Local CA" on page 25.
   d. Click **Sign Request** to access the **Sign Certificate Request** section.
   e. Enter the following details:
      - **Sign with Certificate Authority** – Select the CA that signs the request.
      - **Certificate Purpose** – Select **Client**.
      - **Certificate Duration (days)** – Enter the life span of the certificate. Default is 3649 days.
      - **Certificate Request** – Paste all text from the certificate request, including the header and footer.
   f. Click **Sign Request**. This takes you to the **CA Certificate Information** section.
   g. Copy the actual certificate. The copied text must include the header (`-----BEGIN CERTIFICATE-----`) and footer (`-----END CERTIFICATE-----`).
   h. Paste the copied text into a new file, for example, `importclientcert.crt`. Alternatively, click **Download** to download the certificate.
4. Log on as `pvadmin`. This is the default user.

Note: On successful log on, read the End User License Agreement in the `eula.txt` file placed at `/home/pvadmin/`. By using this software, you consent to the agreement.
– To view the list of allowed commands, run the `help` or `?` command.
– The allowed `sudo` commands are `pvmctl`, `reboot`, `halt`, and `timedatectl`.
– Use the `timedatectl` command to set system time, date, or time zone.

Note: The SafeNet KeySecure CA certificate can be imported to ProtectV Manager using `scp` only as user `pvadmin` with the private key used during launch.

5. Place the certificate on the ProtectV Manager instance. For example, place `importclientcert.crt` at `/home/pvadmin`.
6. Run the `pvmctl configks` command, as follows:

```
sudo pvmctl configks --ksip=KSIP --ksport=KSPORT --ksuser=KSUSER --
kscacert=KSCACERT --kspass="KSPASS" --ksclientcert=KSCLIENTCERT --
ksclientkey=KSCLIENTKEY --passphrase="PASSPHRASE"
```

Here,

- `KSIP` – Private IP address of SafeNet KeySecure.
- `KSPORT` – Port of SafeNet KeySecure. Use the port **associated with your CA certificate**. Refer to "Enabling Key Export on SafeNet KeySecure" on page 36 for details.
- `KSUSER` – Specify the SafeNet KeySecure user that has permission to create keys on SafeNet KeySecure. This SafeNet KeySecure user was created when "Creating a Local SafeNet KeySecure User" on page 39.
- `"KSPASS"` – Specify password for the SafeNet KeySecure user. This SafeNet KeySecure user was created when "Creating a Local SafeNet KeySecure User" on page 39.
- `KSCACERT` – Full path of the CA certificate (`.crt` file) that you generated on SafeNet KeySecure and downloaded to the Gateway instance. Place the CA certificate at `/home/pvadmin`. Refer to "Generating the Local CA Certificate" on page 25 for details.
- `KSCLIENTCERT` – Full path of the imported client certificate. For example, `/home/pvadmin/importclientcert.crt`.
- `KSCLIENTKEY` – Full path of the KeySecure client's private key.
- `"PASSPHRASE"` – Password of the imported client's private key.

Note: When using a SafeNet KeySecure cluster (or multiple KeySecure servers,) specify the clustered KeySecure IP addresses separated by colons. For example, to use three KeySecure servers in a cluster, run:

```
sudo pvmctl configks --ksip=KSIP1:KSIP2:KSIP3 --ksport=KSPORT --
ksuser=KSUSER --kscacert=KSCACERT --kspass="KSPASS" --
ksclientcert=KSCLIENTCERT --ksclientkey=KSCLIENTKEY --
passphrase="PASSPHRASE"
```

Note: Rerunning the `pvmctl configks` command is not needed on subsequent reboots of the ProtectV Manager instance.

Note: If SafeNet ProtectV Clients are to be upgraded, ensure to configure ProtectV Manager 4.x with the same KeySecure server and user with which existing ProtectV Manager was configured.

Note: Upgrade from SafeNet ProtectV 3.0 and SafeNet ProtectV 3.1 is not supported.

For example:

```
pvmctl@ip-172-30-3-69:~$ sudo pvmctl configks --ksip=52.3.148.51 --ksport=9000
--ksuser=ksuser --kscacert=/pvm/config/AWSCA.crt --kspass="ksuserspassword" --
ksclientcert=/home/pvadmin/importedclientcert.crt --
ksclientkey=/home/pvadmin/ksclientkey --passphrase="ksclientkeypass"
```

After configuring the ProtectV Manager with SafeNet KeySecure, start the ProtectV Manager service. Refer to "Starting the SafeNet ProtectV Manager Service" on page 65 for details. However, if you are using an external ProtectV Gateway, refer to "Configuring SafeNet ProtectV Gateway Instance" on page 86.

Configuring SafeNet ProtectV Manager using Client Certificates Created through pvmctl

Note: The CN (Common Name) must be the same in server and client certificates, and the same user must exist on SafeNet KeySecure.

To configure ProtectV Manager with SafeNet KeySecure using client certificate and private key created through `pvmctl`:

1. Log on as `pvadmin`. This is the default user.

   Note: On successful log on, read the End User License Agreement in the `eula.txt` file placed at `/home/pvadmin/`. By using this software, you consent to the agreement.
   – To view the list of allowed commands, run the `help` or `?` command.
   – The allowed `sudo` commands are `pvmctl`, `reboot`, `halt`, and `timedatectl`.
   – Use the `timedatectl` command to set system time, date, or time zone.

   Note: The SafeNet KeySecure CA certificate can be imported to ProtectV Manager using `scp` only as user `pvadmin` with the private key used during launch.

2. Create a client Certificate Signing Request (CSR) and the private key.

   Run: `sudo pvmctl createcsr --ksclientcsr=KSCLIENTCSR --ksclientcn=KSCLIENTCN --passphrase="PASSPHRASE"`

   Here,

   - `KSCLIENTCSR` – Name for the client CSR file.
   - `KSCLIENTCN` – Common Name (CN) for the client certificate.
   - `"PASSPHRASE"` – Password for the private key.

Note: Use `OpenSSL` if you want to create a certificate with user defined DN.

For example:

```
sudo pvmctl createcsr --ksclientcsr=ksclientcsr --ksclientcn=ksclientcn --
passphrase="privatekeypassword"
```

3. Copy the text of the generated client CSR. The copied text must include the header (`-----BEGIN CERTIFICATE REQUEST-----`) and footer (`-----END CERTIFICATE REQUEST-----`).
4. On SafeNet KeySecure, sign the client CSR with the local CA, as follows:
   a. Log on to the **Management Console** as an administrator with Certificates and Certificate Authorities access controls.
   b. Navigate to the **Local Certificate Authority List** (**Security**, **Device CAs & SSL Certificates**, **Local CAs**.)
   c. Select the local CA. This is the local CA that you created in "Creating a Local CA" on page 25.
   d. Click **Sign Request** to access the **Sign Certificate Request** section.
   e. Enter the following details:
      - **Sign with Certificate Authority** – Select the CA that signs the request.
      - **Certificate Purpose** – Select **Client**.
      - **Certificate Duration (days)** – Enter the life span of the certificate. Default is 3649 days.
      - **Certificate Request** – Paste all text from the certificate request, including the header and footer.
   f. Click **Sign Request**. This takes you to the **CA Certificate Information** section.
   g. Copy the actual certificate. The copied text must include the header (`-----BEGIN CERTIFICATE-----`) and footer (`-----END CERTIFICATE-----`).
   h. Paste the copied text into a new file, for example, `ksclientcert.crt`. Alternatively, click **Download** to download the certificate.
5. Place the certificate on the ProtectV Manager instance. For example, place `ksclientcert.crt` at `/home/pvadmin`.
6. Run the `pvmctl configks` command, as follows:

```
sudo pvmctl configks --ksip=KSIP --ksport=KSPORT --ksuser=KSUSER --
kscacert=KSCACERT --kspass="KSPASS" --ksclientcert=KSCLIENTCERT
```

Here,

- `KSIP` – Private IP address of SafeNet KeySecure.
- `KSPORT` – Port of SafeNet KeySecure. Use the port **associated with your CA certificate**. Refer to "Enabling Key Export on SafeNet KeySecure" on page 36 for details.
- `KSUSER` – Specify the SafeNet KeySecure user that has permission to create keys on SafeNet KeySecure. This SafeNet KeySecure user was created when "Creating a Local SafeNet KeySecure User" on page 39.
- `"KSPASS"` – Specify password for the SafeNet KeySecure user. This SafeNet KeySecure user was created when "Creating a Local SafeNet KeySecure User" on page 39.
- `KSCACERT` – Full path of the CA certificate (`.crt` file) that you generated on SafeNet KeySecure and downloaded to the Gateway instance. Place the CA certificate at `/home/pvadmin`. Refer to "Generating the Local CA Certificate" on page 25 for details.

- `KSCLIENTCERT` – Full path of the KeySecure client certificate.

> **Note:** When using a SafeNet KeySecure cluster (or multiple KeySecure servers,) specify the clustered KeySecure IP addresses separated by colons. For example, to use three KeySecure servers in a cluster, run:
> `sudo pvmctl configks --ksip=KSIP1:KSIP2:KSIP3 --ksport=KSPORT --ksuser=KSUSER --kscacert=KSCACERT --kspass="KSPASS" --ksclientcert=KSCLIENTCERT`

> **Note:** Rerunning the `pvmctl configks` command is not needed on subsequent reboots of the ProtectV Manager instance.

> **Note:** If SafeNet ProtectV Clients are to be upgraded, ensure to configure ProtectV Manager 4.x with the same KeySecure server and user with which existing ProtectV Manager was configured.

> **Note:** Upgrade from SafeNet ProtectV 3.0 and SafeNet ProtectV 3.1 is not supported.

For example:

```
pvmctl@ip-172-30-3-69:~$ sudo pvmctl configks --ksip=52.3.148.51 --ksport=9000 --ksuser=ksuser --kscacert=/pvm/config/AWSCA.crt --kspass="ksuserspassword" --ksclientcert=/home/pvadmin/ksclientcert.crt
```

After configuring the ProtectV Manager with SafeNet KeySecure, start the ProtectV Manager service. Refer to "Starting the SafeNet ProtectV Manager Service" below for details. However, if you are using an external ProtectV Gateway, refer to "Configuring SafeNet ProtectV Gateway Instance" on page 86.

Starting the SafeNet ProtectV Manager Service

To start the ProtectV Manager service:

1. Log on as `pvadmin`. This is the default user.
2. Start the ProtectV Manager service.

   Run: `sudo pvmctl startpvm --prikeypass="PRIKEYPASS"`

   Here, `"PRIKEYPASS"` represents the password of the private key. For example, `--prikeypass="password"`. If not specified, you will be prompted for the private key password during the command run.

> **Note:** Running the `pvmctl startpvm` command for the first time sets password for the private key. **Remember this password.** You will need this password when running the `sudo pvmctl startpvm` command subsequently.
>
> The private key password can be changed any time later. Refer to "Changing the Private Key Password" on page 67 for details.

For example: `sudo pvmctl startpvm --prikeypass="password"`

ProtectV Manager is configured successfully with local ProtectV Gateway. You can verify it by opening the Public DNS, Private DNS, or IP address/hostname of your ProtectV Manager instance. For example, open https://ec2-54-165-90-153.compute-1.amazonaws.com/, or https://54.165.90.153/ in the Internet browser.

As a ProtectV administrator, you can now log on to the ProtectV Manager Console, as described in "Logging on as Administrator" below.

Logging on as Administrator

Log on to the ProtectV Manager Console as the default administrator. You will be prompted to change the password on first log on. It is recommended to change the default password.

To log on to the ProtectV Manager Console as administrator:

1. Open the Internet browser.
2. Enter ProtectV Manager's IP address/hostname in the address bar.
3. Press **Enter**. The **SafeNet ProtectV Manager Console** is displayed.
4. Under **Sign In**, enter **Username** and **Password**. The default administrator credentials are **admin**/ **admin**.
5. Click **Submit**. On first successful log on, the **Administrator** page is displayed.
6. Enter new password in the **New Password** and **Confirm Password** fields. Adhere to the password creation rules mentioned on the page.

WARNING! REMEMBER the new password. You will need this password to log on to the ProtectV Manager Console subsequently. Currently, there is no way to retrieve the password if you forget it.

7. Click **Set New Admin Password**. A message appears stating that the changes are applied successfully.

As ProtectV administrator, you can now add:

- Local ProtectV users on the ProtectV Manager Console. Refer to "Managing Users" for details.
- AD users on the ProtectV Manager Console. For this, first configure ProtectV Manager for AD, as described in "Configuring SafeNet ProtectV Manager for AD". Then, you can add AD users on the ProtectV Manager Console, as described in "Managing Users".

Changing Password of the ProtectV Manager Database

The default password for PVMDB (`postgres`) database is `postgres`. You can change it whenever needed. To change the PVMDB password:

Run: `pvmctl updatedbpass --oldpass="OLDPASS" --newpass="NEWPASS"`

Here,

- `"OLDPASS"`: Represents the existing password of the database.
- `"NEWPASS"`: Represents the new password for the database.

Changing the Private Key Password

The private key password is set when the `pvmctl startpvm` command is run for the first time. You can change this password any time.

> **Note:** In a ProtectV Manager cluster, if the private key password is changed on one node, restart the ProtectV Manager service on other nodes of the cluster.
>
> To restart the service:
>
> 1. Stop the ProtectV Manager service. Run `sudo pvmctl stoppvm`.
> 2. Start the ProtectV Manager service. Run `sudo pvmctl startpvm` with the new private key password.
>
> Refer to "Setting up SafeNet ProtectV Manager Clustering" on page 78 for details on ProtectV Manager clustering.

To change the password:

Run: `sudo pvmctl resetpvmkeypassword --existingprikeypass="EXISTINGPRIKEYPASS" --newprikeypass="NEWPRIKEYPASS"`

Here,

- `"EXISTINGPRIKEYPASS"`: Represents the existing password of the private key.
- `"NEWPRIKEYPASS"`: Represents the new password for the private key.

If passwords are not specified when running the `sudo pvmctl resetpvmkeypassword` command, you will be prompted for existing and new passwords during the command run.

Changing SafeNet KeySecure's IP Address

When the IP address of SafeNet KeySecure is changed, reconfigure ProtectV Manager with the KeySecure and restart the ProtectV Manager service for the changes to take effect.

To do so:

1. Stop the ProtectV Manager service.

   Run: `sudo pvmctl stoppvm`

2. Reconfigure ProtectV Manager with SafeNet KeySecure.

   Run the `sudo pvmctl configks` command with the new IP address of SafeNet KeySecure, `--ksip=<NEWKSIP>`.

> **Note:** When using a SafeNet KeySecure cluster (or multiple KeySecure servers,) specify the clustered KeySecure IP addresses separated by colons.
>
> For example, to use three KeySecure servers in a cluster, specify `--ksip=<IP address of KeySecure 1>:<IP address of KeySecure 2>:<IP address of KeySecure 3>` when running `sudo pvmctl configks`.

3. Start the ProtectV Manager service.

   Run: `sudo pvmctl startpvm --prikeypass="PRIKEYPASS"`

   Refer to "Starting the SafeNet ProtectV Manager Service" on page 65 for details.

Pre-shipped Certificates

Note: ProtectV Manager comes with pre-shipped certificates. Use these certificates for evaluation purpose only. You should replace these certificates with own certificates. After replacing certificates, reboot ProtectV Manager. Run: `sudo reboot`

The certificates pre-shipped with ProtectV Manager are available at `/pvm/nginx/ssl/pvmui/`. The key and certificate placed at this location must have `400` permissions.

For example:

```
pvadmin@ip-172-30-1-44:~$ cd /pvm/nginx/ssl/pvmui
pvadmin@ip-172-30-1-44:/pvm/nginx/ssl/pvmui$ ls -l
total 8
-r-------- 1 pvadmin pvadmin 1988 May 17 06:56 server.crt
-r-------- 1 pvadmin pvadmin 3272 May 17 06:56 server.key
```

Backing up the SafeNet ProtectV Manager Database Manually

SafeNet ProtectV provides options to back up and restore the ProtectV Manager database. A ProtectV Manager database can be backed up either manually or automatically through a scheduled backup.

For instructions on scheduling an automatic backup, refer to "Scheduling the SafeNet ProtectV Manager Backup". Follow the instructions in this section to back up the database manually.

Each manual backup is stored in a different folder under `/pvm/db_bkup`. The backup folder is named as `pvdb_bkup_<year>_<time>`; for example, `pvdb_backup_20170501_072307`. A new folder will be created for each backup.

To back up the database connected to ProtectV Manager:

Run: `sudo pvmctl backupdb`

For example:

```
sudo pvmctl backupdb
Local database backup is created successfully in directory /pvm/db_bkup/pvdb_backup_20170501_072307
```

Backup Content

The content of the sample backup folder, `/pvm/db_bkup/pvdb_backup_20170501_072307`, is listed below:

```
ls -l /pvm/db_bkup/pvdb_backup_20170501_072307
total 32
```

```
-rw-r--r-- 1 root root 1707 May 1 07:23 heidi.gz
-rw-r--r-- 1 root root 92 May 1 07:23 heidi_sha1
-rw-r--r-- 1 root root 1326 May 1 07:23 protectv.gz
-rw-r--r-- 1 root root 95 May 1 07:23 protectv_sha1
-rw-r--r-- 1 root root 9369 May 1 07:23 safex.gz
-rw-r--r-- 1 root root 92 May 1 07:23 safex_sha1
```

The `heidi.gz`, `protectv.gz`, and `safex.gz` files with their `sha1` are backed up.

A backup can be restored any time later. Refer to "Restoring a Backup Taken Manually" for details.

Scheduling the SafeNet ProtectV Manager Backup

To schedule a ProtectV Manager database:

1. Check the upload settings for the scheduled backup.

   Run: `sudo pvmctl autodbbackup uploadsettings show`

   This command displays the upload settings.

   For example:

   ```
   sudo pvmctl autodbbackup uploadsettings show
   Upload settings are not configured.
   ```

   The upload settings for automatic backup are not configured. You can configure them now.

2. Specify the upload settings.

   Run: `sudo pvmctl autodbbackup uploadsettings update --protocol=PROTOCOL --host=HOST --username=USERNAME [--keyfile=KEYFILE|--password="PASSWORD"] --destinationdir=DESTINATIONDIR --encpass="ENCPASS"`

   This command sets/updates the upload settings.

   In the command above:

   - `PROTOCOL` – Specify protocol for automatic backup. Either `scp` or `sftp`.
   - `HOST` – Hostname or IP address of the backup machine.
   - `USERNAME` – User name for the protocol.
   - `KEYFILE` – The `SSH` key to be used to log on to the backup machine.
   - `"PASSWORD"` – Login password for the protocol. Specify either password or the SSH key, but not both.
   - `DESTINATIONDIR` – Directory on the backup machine to upload the scheduled backup.
   - `"ENCPASS"` – Password to derive key for encrypting and signing the backup.

   > **Note:** Remember the password (`--encpass="ENCPASS",`) as it will be needed when restoring the scheduled backup file.

   For example:

```
sudo pvmctl autodbbackup uploadsettings update --protocol=scp --
host=54.175.204.92 --username=pvadmin --keyfile=/home/pvadmin/AB_Key_Pair1.pem
--destinationdir=/tmp --encpass="encpass"

Upload settings configured successfully for scheduled backup.
```

The upload settings for the scheduled backup are configured successfully.

3. Check the backup schedule.

   Run: `sudo pvmctl autodbbackup schedulesettings show`

   This command displays the backup schedule.

   For example:

   ```
   sudo pvmctl autodbbackup schedulesettings show

   Backup schedule is not configured.
   ```

   The automatic backup is not yet scheduled. You can configure it now.

4. Specify the backup schedule.

   Run: `sudo pvmctl autodbbackup schedulesettings update --period="daily" --day-of-month=1 --day-of-week="sat" --hour=0 --minute=0`

   This command sets/updates the backup schedule.

   In the command above:

   - `"daily"` – Specify frequency of the scheduled backup. The option could be `hourly`, `daily`, `weekly`, or `monthly`. Default is "`daily`".
   - `1` – The day of month for monthly backups (i.e., when `--period="monthly"`.) Defaut is `1`, that is, on the first day every month.
   - `"sat"` – The day of the week for weekly backups (i.e., when `--period="weekly"`.) Defaut is `sat`, that is, on every Saturday.
   - `0` – Time in hour for the scheduled backup. Needed for all values of `--period=`.
   - `0` – Minutes past the specified hour (`--hour=`) for the scheduled backup. Needed for all values of `--period=`.

   For example, to schedule automatic backup for `23:59` every `Sunday`:

   ```
   sudo pvmctl autodbbackup schedulesettings update --period="weekly" --day-of-week="sun" --hour=23 --minute=59

   Saved automatic backup schedule settings
   ```

   Note: At the scheduled time, a backup file (`pvdb3.x_<date>_<hhmmss>.tgz`) will be created under the location specified by `--destinationdir=DESTINATIONDIR`.

   Note: A backup can be restored any time later. Refer to "Restoring an Automatically Created Scheduled Backup" for details.

Restoring Database Backups

You can restore the PostgreSQL database from available backups, whenever needed. Stop the ProtectV Manager service, restore the backup, and start the ProtectV Manager service.

WARNING! Restoring a ProtectV Manager database will restore ProtectV Manager to a previous state. Any changes made after the backup was taken, will be lost.

Note: If a ProtectV Manager database is restored on a new ProtectV Manager instance, you need to update the `registration.json` file with the IP address of the ProtectV Gateway instance. Refer to "Updating the Registration File" for details.

To restore a backup:

Run: `sudo pvmctl restoredb --dbpath=DBPATH --encpass="ENCPASS"`

Here,

- `DBPATH` – Path and name of the backup directory to restore. When restoring a manual backup, specify absolute path of the backup directory. However, when restoring an automatically created backup, specify the absolute path of the backup file.
- `"ENCPASS"` – Password to decrypt automatically created scheduled backup. Specify `--encpass="ENCPASS"` only if it is different from password saved for scheduled backup encryption.

Note: Specify `--encpass="ENCPASS"` when restoring automatically scheduled backups only. Do not specify `--encpass="ENCPASS"` when restoring manual backups.

Note: The password, `--encpass="ENCPASS"`, MUST be the same password that was specified when the encrypting the backup. This password (`--encpass="ENCPASS"`) is the same that was specified when running `pvmctl autodbbackup uploadsettings update`.

Restoring a Backup Taken Manually

To restore a backup that was taken manually:

1. Stop the ProtectV Manager service. Run `pvmctl stoppvm`.

   Note: Attempts to restore a backup without stopping the ProtectV Manager service will return an error. Stop the service before running `pvmctl restoredb`.

2. Restore the backup.

   Run: `sudo pvmctl restoredb --dbpath=DBPATH`

   For example:

   ```
   sudo pvmctl restoredb --dbpath=/pvm/db_bkup/pvdb_backup_20170501_072307
   Database backup restored successfully. Please start pvm services.
   ```

3. Start the ProtectV Manager service. Run `pvmctl startpvm`.

Restoring an Automatically Created Scheduled Backup

To restore an automatically created scheduled backup:

1. Stop the ProtectV Manager service. Run `pvmctl stoppvm`.

   Note: Attempts to restore a backup without stopping the ProtectV Manager service will return an error. Stop the service before running `pvmctl restoredb`.

2. Copy the automatically backed up database file (for example, `pvdb3.x_<date>_<hhmmss>.tgz`) locally. For example, place the backup file in the `/tmp` directory.
3. Restore the backup.

   Run: `sudo pvmctl restoredb --dbpath=DBPATH --encpass="ENCPASS"`

   For example:

   ```
   sudo pvmctl restoredb --dbpath=/tmp/pvdb3.x_20170502_065501.tgz --
   encpass="encpass"

   Database backup restored successfully. Please start pvm services.
   ```

   ```
   Database backup restored successfully. Please start pvm services.
   ```

4. Start the ProtectV Manager service. Run `pvmctl startpvm`.

Upgrading SafeNet ProtectV Manager

ProtectV Manager versions 3.3.0 and higher can be upgraded to the latest version. To maximize benefits from the upgrade, upgrade your ProtectV Clients as well. New features included in the latest version will be available to you.

To upgrade the ProtectV Manager instance:

1. Back up your ProtectV Manager database manually. Refer to "Backing up the SafeNet ProtectV Manager Database Manually" on page 68 for details.
2. Launch a new ProtectV Manager instance. Use the latest ProtectV Manager AMI from Gemalto. Refer to "Launching SafeNet ProtectV Manager Instance" on page 41 for details.
3. Place the database backup on the newly launched ProtectV Manager instance.
4. Restore the database backup on the new ProtectV Manager instance. Refer to "Restoring Database Backups" on the previous page for details.
5. Configure the new ProtectV Manager instance with SafeNet KeySecure. Ensure that the KeySecure server and user are the same with which the old ProtectV Manager was configured. Refer to "Configuring SafeNet ProtectV Manager with SafeNet KeySecure" on page 61 for details.
6. Start the ProtectV Manager service on the new ProtectV Manager instance. Ensure that the database password and private key are the same with which the old ProtectV Manager was configured. Refer to "Starting the SafeNet ProtectV Manager Service" on page 65 for details.

After successful upgrade, update the registration file of all client instances to establish connection with the new ProtectV Manager instance. Update the IP address of the new ProtectV Manager instance in the registration file. Refer

to "Updating the Registration File" on page 102 (Linux) and "Updating the Registration File " on page 108 (Windows) for details.

To use the features included in the latest SafeNet ProtectV clients, upgrade them on your client instances. Refer to "Upgrading SafeNet ProtectV Clients" on page 109 for details.

Patching SafeNet ProtectV Manager

SafeNet ProtectV allows you to apply security patches to a ProtectV Manager configured with internal database and Gateway. However, to perform this, you need to log on as the root user, `pvsuper`.

WARNING! As the impact of a particular security patch might be unpredictable, risk is involved in applying patches to a released ProtectV Manager. Applying a security patch could potentially render your ProtectV Manager unusable.

Note: It is strongly advised to backup your ProtectV Manager configuration before applying a security patch.

To apply a security patch to ProtectV Manager:

1. Back up your ProtectV Manager. Refer to "Backing up the SafeNet ProtectV Manager Database Manually" on page 68 and "Scheduling the SafeNet ProtectV Manager Backup" on page 69 for details.
2. Log on to your ProtectV Manager instance as `pvsuper`. The default password is `pvsuper`.

   Note: It is strongly recommended to change the default password of the `pvsuper` user at the first login. You can change the password by running `passwd`. Remember this password. You will need this password when logging on to ProtectV Manager as `pvsuper` subsequently.

3. Apply the security patch.

4

Configuring SafeNet ProtectV Manager for Active Directory

Note: Instructions in this chapter are applicable if you plan to configure ProtectV Manager for Active Directory (AD) users. If you want to configure ProtectV Manager for local ProtectV users, you may skip this chapter and proceed "Managing Users" on page 76.

AD users can access the ProtectV Manager Console using their AD credentials. Before they can log on to the ProtectV Manager Console, the ProtectV administrator needs to configure ProtectV Manager for them.

Before proceeding, ensure that AD is already configured in your organization's domain and your AD account exists in the domain. If the AD account does not exist, get one created by your System Administrator.

This chapter covers the following information:

Configuring SafeNet ProtectV Manager for AD

Before AD users can log on to the ProtectV Manager Console, the ProtectV administrator must configure ProtectV Manager to allow AD user login.

To configure ProtectV Manager for AD users:

1. Log on to the ProtectV Manager Console as administrator.
   a. Open the Internet browser.
   b. Enter ProtectV Manager's IP address/hostname in the address bar.
   c. Press **Enter**. The **SafeNet ProtectV Manager Console** is displayed.
   d. Under **Sign In**, enter **Username** and **Password**.
   e. Ensure that **Local Account** is selected at the account type.
   f. Click **Submit**.
2. Click the **Settings** tab. The **LDAP Authentication** section is displayed. This section contains the **Add LDAP Authentication** screen. Fields on this screen are collapsed, by default.
3. In the top right corner of the **Add LDAP Authentication** screen, click (down-arrow) to view the fields.
4. Enter the following information:
   – **Connection Name** – A friendly name for your connection. For example, `AD Account`. This name will appear as an account type on the Home page of the ProtectV Manager Console.
   – **Server URL** – The LDAP URL for your server. For example, "`ldap://172.16.2.2:3268`".

- **Root DN** – The starting point to use when searching for users. For example, “`dc=myco,dc=local`”.
- **Bind DN** – An object which has permission to search under the root DN for users. For example, “`cn=poweruser,cn=Users,dc=myco,dc=local`”.
- **Bind Password** – The password for the Bind DN object (for example, `poweruser`) specified in Bind DN field.
- **UID** – The field which contains the user ID. For AD, it is usually “`sAMAccountName`”.
- **LDAP Filter** – Optional LDAP Filter to specify the set of users who can log on to the ProtectV Manager Console. (For example, "`&(objectclass=user)(memberOf=cn=All America,ou=Global,dc=myco,dc=local)`").

5. Click **Save**. The configuration is complete.

AD users can now log on to the ProtectV Manager Console using their AD accounts. Refer to "Logging on using AD Account" on page 128.

> **Note:** The Home page of the ProtectV Manager Console now shows the account type drop-down list. The available account types are **Local Account** (for local ProtectV users) and **<Connection Name>** (for AD users.) Here, **<Connection Name>** refers to the value you specified in the **Connection Name** field above. This document uses **AD Account** as the Connection Name.

Modifying AD Configuration

To modify AD configuration, if needed:

1. Log on to the ProtectV Manager Console as administrator.
2. Click the **Settings** tab. The **LDAP Authentication** page is displayed.
3. Modify settings, as appropriate. For details on the available fields, refer to "Configuring SafeNet ProtectV Manager for AD" on the previous page.
4. Click **Update**.

The AD configuration is modified. Users can log on to the ProtectV Manager Console with updated AD settings. Refer to "Logging on using AD Account" on page 128.

> **Note:** To delete the AD configuration, click **Delete Configuration**.

5
Managing Users

Before users can log on to the ProtectV Manager Console, their accounts must be created. The ProtectV administrator can add and manage accounts for ProtectV users on the ProtectV Manager Console.

This chapter covers the following information:

Adding New Users

After logging on to the ProtectV Manager Console as administrator, you can create accounts for new ProtectV users.

To add a new ProtectV user:

1. Log on to the ProtectV Manager Console as administrator.
2. Click the **Users** tab.
3. Enter **Username** and **Display Name** for the user.
4. *(Optional)* Under the **Admin** column, select the check box to make the user as administrator. You can also make a user an administrator later. Refer to the "Making a User as an Administrator" section.
5. Enter password in the **Password** and **Confirm Password** fields.
6. Click **New User**. A message appears stating that the user is created successfully. The newly added user appears under the table of users.

After ProtectV users are created, they can log on to the ProtectV Manager Console, as described in the "Logging on as ProtectV User" section.

Changing Password of Other Users

As a ProtectV administrator, you have privileges to change the password of other ProtectV users.

To change the password of a ProtectV user:

1. Log on to the ProtectV Manager Console as administrator.
2. Click the **Users** tab. The list of ProtectV users is displayed.
3. Under the **User** column, click the username link for the user whose password you want to change. The **<Username>** page is displayed.
4. *(Optional)* Change the **Display Name**.

5. Enter new password in the **New Password** and **Confirm Password** fields. Adhere to the password creation rules mentioned on the page.
6. Click **Update User Details**. A message appears stating that the changes are applied successfully.

The ProtectV user can now log on to the ProtectV Manager Console using the new password.

Making a User as an Administrator

As a ProtectV administrator, you can assign the role of administrator to existing users, whenever needed.

To make an existing ProtectV user as an administrator:

1. Log on to the ProtectV Manager Console as administrator.
2. Click the **Users** tab. The list of ProtectV users is displayed.
3. Under the **User** column, click the username link. The **<Username>** page is displayed.
4. *(Optional)* Change the display name and password.
5. Select the **Administrator** check box.
6. Click **Update User Details**. A message appears stating that the changes are applied.

A tick mark appears under the **Admin** column for the user. It indicates that the user is now an administrator.

Deleting a User

As a ProtectV administrator, you can delete ProtectV users, whenever needed.

To delete a ProtectV user:

1. Log on to the ProtectV Manager Console as administrator.
2. Click the **Users** tab. The list of ProtectV users is displayed.
3. Click **Delete User** next to the user you want to delete. A message appears stating that the user is deleted successfully. The user is removed from the table of users.

A ProtectV user with administrator privileges cannot be deleted directly. The user first needs to be made non-administrator. Refer to “Deleting an Administrator Account” for details.

Deleting an Administrator Account

A ProtectV user with administrator privileges cannot be deleted. First revoke administrator privileges and then delete the user.

To delete another administrator account:

1. Log on to the ProtectV Manager Console as administrator.
2. Click the **Users** tab. The list of ProtectV users is displayed.
3. Under the **User** column, click the username link. The **<Username>** page is displayed.
4. Clear the **Administrator** check box.
5. Click **Update User Details**. The tick mark under the **Admin** column for the user has disappeared. It indicates that the user is no longer an administrator.
6. Click **Delete User** next to the user.

6

Setting up SafeNet ProtectV Manager Clustering

Note: Instructions in this chapter are applicable if you plan to configure ProtectV Manager clustering. It is recommended to configure ProtectV Manager clustering. However, if you want to use single ProtectV Manager instance, skip this chapter.

This chapter covers the following information:

Clustering Overview

ProtectV Manager clustering is a configuration where multiple ProtectV Manager instances (nodes) are configured to work together as a group. A cluster can have at least two ProtectV Manager nodes. The first ProtectV Manager node where cluster is created is called the source node. You must add one or more ProtectV Manager nodes to the source node to complete the cluster. These ProtectV Manager nodes are called cluster members or cluster nodes.

The replication password is the same for all members of the cluster; however, the database password may be different on different ProtectV Manager nodes.

Before proceeding, it is recommended to go through "Limitations" on page 83 and "Important Notes" on page 83.

Configuring SafeNet ProtectV Manager Cluster

SafeNet ProtectV allows configuring clusters in two different ways. First, when only the source node is configured (that is, `pvmctl startpvm` is executed,) other nodes are just launched. Second, when all the ProtectV Manager nodes are up and running.

- When only the source node is up and running.

Note: This is the recommended way to configure a cluster.

The source node contains all the ProtectV Manager configuration. All other ProtectV Manager nodes that will be added to the source node to form the cluster are just launched, not yet configured. ProtectV Manager configuration saved on the source node is replicated on these nodes when they are added to the cluster. After the cluster is formed, all cluster nodes have the same configuration as the source node.

- When all ProtectV Manager nodes that will form the cluster are up and running.

  All the ProtectV Manager configuration is retained on the source node. Existing ProtectV Manager configuration saved on other cluster nodes is *erased* when they are added to the cluster. These nodes are then added to the source node to form the cluster. After the cluster is formed, all cluster nodes have the same configuration as the source node.

Refer to "Setting up SafeNet ProtectV Manager" on page 41 for details on launching and configuring ProtectV Manager nodes.

This document explains steps to configure a two-node cluster. These ProtectV Manager nodes are named *SourceNode* and *MemberNode*. Cluster will be created on *SourceNode*, and *MemberNode* will be added to *SourceNode*.

Configuring a cluster involves the following steps:

1. "Creating a Cluster" below
2. "Adding ProtectV Manager Nodes to the Cluster" on page 81

These steps are described in subsequent sections.

Note: Assign static IP addresses to ProtectV Manager nodes that will form a cluster.

CAUTION: Do not interrupt a command or close your `ssh` session until a `pvmctl cluster` command is executed completely. Interruption may lead to unexpected behavior. Refer to the subsequent sections for details on the `pvmctl cluster` commands.

Creating a Cluster

The cluster is created on the source node, *SourceNode*. Ensure that the source node is assigned a static private IP address.

To create a cluster:

1. Log on to *SourceNode* as `pvadmin`.
2. Configure *SourceNode* with SafeNet KeySecure.

   Run: `sudo pvmctl configks --ksip=KSIP --ksport=KSPORT --ksuser=KSUSER --kscacert=KSCACERT --kspass="KSPASS" --ksclientcert=KSCLIENTCERT --ksclientkey=KSCLIENTKEY`

   For example:

   ```
   $ sudo pvmctl configks --ksip=52.21.152.248 --ksport=9000 --ksuser=ksuser --
   kscacert=/pvm/config/AWSCA.crt --kspass="ksuserspassword" --
   ksclientcert=/home/pvadmin/ksclientcert.crt --
   ksclientkey=/home/pvadmin/ksclientkey
   ```

3. Start the ProtectV Manager service.

   Run: `sudo pvmctl startpvm --prikeypass="PRIKEYPASS"`

Note: When specifying passwords from the command line, include them in double-quotes, `" "`. For example, `"PRIKEYPASS"` is correct.

Note: Running the `pvmctl startpvm` command for the first time sets password for the private key. Remember this password. You will need this password when running the `sudo pvmctl startpvm` command subsequently on all other cluster members. This password is the same on all cluster members.

The private key password can be changed any time later. Refer to "Changing the Private Key Password" on page 67 for details.

For example:

```
$ sudo pvmctl startpvm --prikeypass="password"
```

4. Create the ProtectV Manager as the source node of the cluster.

   Run: `sudo pvmctl cluster create --pass="PASS" --hostip=HOSTIP --pubip`

   Here,

   - `"PASS"` – Password for replication. This password is needed to add member nodes to this cluster. If the replication password is not provided, enter and confirm the password when prompted.

     Note: The replication password is the same on all member nodes of the cluster.

   - `HOSTIP` – Specify the public IP address/hostname of *SourceNode*. Do not specify `HOSTIP` if you are creating the cluster using a private IP address.
   - `--pubip` – Enter this flag if `HOSTIP` is a public IP address/hostname.

   For example, when using a public IP address:

   ```
   $ sudo pvmctl cluster create --pass="REPLICATIONPASS" --HOSTIP=52.205.163.100
   --pubip
   ```

   The cluster is successfully created on the source node. It may take some time to be ready. More ProtectV Manager nodes can only be added to the cluster when it is ready.

5. Confirm whether the cluster is ready.

   Run: `sudo pvmctl cluster status`

   Note: When the cluster is ready, you must add more ProtectV Manager nodes to it to complete the cluster. Refer to "Adding ProtectV Manager Nodes to the Cluster" on the next page for details.

6. *(Optional)* Configure external Gateway, as described in "Setting up SafeNet ProtectV Gateway" on page 85. Use the source node as ProtectV Manager for Gateway configuration. While running the `sudo pvmctl gwstart --pvmip=PVMIP` command to configure external Gateway, `PVMIP` is the IP address of the source node.

Adding ProtectV Manager Nodes to the Cluster

A cluster must have at least two nodes. After a cluster is created, more ProtectV Manager nodes must be added to it to complete the cluster. This section describes how to add another cluster node, *MemberNode*, to the cluster created on the source node.

Before adding a node to the cluster, test its connectivity with the source node. On the source node, run: `sudo pvmctl cluster test --testpvmip=TESTPVMIP`

Here, `TESTPVMIP` is the IP address of the cluster member to be added to the cluster.

To add a ProtectV Manager node, *MemberNode*, to the cluster:

1. Log on to *MemberNode* as `pvadmin`.
2. Add *MemberNode* to the cluster.

   Run: `sudo pvmctl cluster add --pass="PASS" --hostip=HOSTIP --sourcepvmip=SOURCEPVMIP --pubip`

   Here,

   - `PASS` – Replication password. This password was set while creating the cluster on the source node. If the replication password is not provided, enter the password when prompted.

     Note: The replication password is the same on all member nodes of the cluster.

   - `HOSTIP` – Specify the public IP address/hostname of *MemberNode*. Do not specify `HOSTIP` if you are creating the cluster using a private IP address.
   - `--pubip` – Enter this flag if `HOSTIP` is a public IP address/hostname.
   - `SOURCEPVMIP` – IP address of the source node. To view the IP address of the *SourceNode*, run `pvmctl cluster list` on the source node. Refer to "Viewing Nodes of a Cluster" on the next page for details.

   For example:

   ```
   $ sudo pvmctl cluster add --pass="REPLICATIONPASS" --HOSTIP=52.205.163.201 --pubip --sourcepvmip=52.205.163.100
   ```

   MemberNode is successfully added to the cluster. It may take some time to be ready.

   Note: If ProtectV Manager is already configured on the current node, stop the ProtectV Manager services by running `pvmctl stoppvm` before configuring *MemberNode* with KeySecure.

3. Confirm whether *MemberNode* is ready.

   Run: `sudo pvmctl cluster status`

4. Configure *MemberNode* with SafeNet KeySecure.

   Run: `sudo pvmctl configks --ksip=KSIP --ksport=KSPORT --ksuser=KSUSER --kscacert=KSCACERT --kspass="KSPASS" --ksclientcert=KSCLIENTCERT --ksclientkey=KSCLIENTKEY`

   For example:

```
$ sudo pvmctl configks --ksip=52.21.152.248 --ksport=9000 --ksuser=ksuser --
kscacert=/pvm/config/AWSCA.crt --kspass="ksuserspassword" --
ksclientcert=/home/pvadmin/ksclientcert.crt --
ksclientkey=/home/pvadmin/ksclientkey
```

5. Start the ProtectV Manager service.

   Run: `sudo pvmctl startpvm --prikeypass="PRIKEYPASS"`

   Here, `"PRIKEYPASS"` is the password as set on the source node.

   For example:

   ```
   $ sudo pvmctl startpvm --prikeypass="password"
   ```

   The ProtectV Manager node is successfully added to the cluster. The cluster configuration is now complete.

   Similarly, you may add more ProtectV Manager nodes to the cluster. Before proceeding, ensure that *all* the existing cluster members are up and running. If any cluster member is down, deregister it, and then add the new ProtectV Manager node to the cluster.

Viewing Nodes of a Cluster

To view the nodes of a cluster, run the `pvmctl cluster list` command. The command also shows whether member nodes are reachable or not.

For example:

```
$ sudo pvmctl cluster list
```

Deregistering Nodes from a Cluster

A cluster node cannot be directly removed from the cluster membership. You need to deregister it first. A cluster node can only be deregistered from another running node of the cluster.

> **Note:** The last node of the cluster cannot be deregistered using the `cluster deregister` command.

To deregister a ProtectV Manager node from the cluster, on the source node, run:

```
pvmctl cluster deregister --otherpvmip=OTHERPVMIP
```

Here, `OTHERPVMIP` represents the IP address of the ProtectV Manager node to be deregistered from the cluster membership.

For example:

```
sudo pvmctl cluster deregister --otherpvmip=52.205.163.201
```

After a ProtectV Manager node is deregistered from the cluster membership, its cluster state needs to be cleared to remove it from the cluster completely. Refer to for "Clearing Cluster State from the Current Node" below details.

Clearing Cluster State from the Current Node

Clear the cluster state of a deregistered ProtectV Manager node to remove it from the cluster completely.

> **Note:** Before clearing the cluster state of the current ProtectV Manager node, ensure that it is deregistered from the cluster by running `cluster deregister` on another cluster node.

To clear the cluster state from the current ProtectV Manager node, run:

```
sudo pvmctl cluster removeself
```

Removing the Last Node from a Cluster

For the last ProtectV Manager node, there is no member node to deregister it. So it cannot be deregistered by running `cluster deregister` on other nodes. It can be done from the last node itself. To deregister the last node from the cluster membership and clear its cluster state, run:

```
sudo pvmctl cluster removeself --force
```

Rejoining a Node to a Cluster

A ProtectV Manager node that is removed from a cluster can rejoin the cluster later. Simply add the ProtectV Manager node to the cluster again by running the `pvmctl cluster add` command. Refer to "Adding ProtectV Manager Nodes to the Cluster" on page 81 for details.

> **WARNING! If ProtectV Manager is already configured on the current node, rejoining the cluster overwrites PVMDB. All the existing database configurations will be lost.**

Limitations

- Clusters can be configured using static IP addresses only. After a cluster is created, the IP addresses of cluster members should not be changed.
- All cluster members must be assigned similar IP addresses – either private or public. If some cluster members are assigned public IP addresses while others are assigned private IP addresses, they cannot communicate with each other.
- All ProtectV Manager nodes in a cluster can be added using the same replication password that was set while creating the cluster on the source node. This password cannot be changed.
- Clustering does not support customer certificates for secure replication channel. Secure replication uses dynamically generated certificates only.
- Restore works only for ProtectV Manager nodes that are not part of a cluster.

Important Notes

- At minimum, a two-node ProtectV Manager cluster is recommended. In case of large number of client instances, appropriately increase the number of member nodes of the ProtectV Manager cluster. Moreover, it is recommended to register client instances with different ProtectV Manager instances in the cluster. Doing this keeps the numbers of client instances per ProtectV Manager manageable and ensures efficient usage of resources.
- Disk encryption is specific to a ProtectV Manager instance. Disk of one cluster member might be encrypted; while the disk of other cluster members might not be encrypted. Changing the disk encryption password of a cluster member does not impact other cluster members. You can change the disk encryption password for cluster

members individually. Refer to "Encrypting the SafeNet ProtectV Manager Disk" on page 55 for details.

- This private key password is the same on all cluster members. Remember this password! This password is needed when running the `sudo pvmctl startpvm` command subsequently on all other cluster members.
- In a ProtectV Manager cluster, if the private key password is changed on one node, restart the ProtectV Manager service on other nodes of the cluster. To restart the service:

  a. Stop the ProtectV Manager service.

     Run `sudo pvmctl stoppvm`.

  b. Start the ProtectV Manager service.

     Run `sudo pvmctl startpvm` with the new private key password.

     Refer to "Changing the Private Key Password" on page 67 for details.
- In SafeNet ProtectV Manager clustering, logs of only those ProtectV Manager instances will be redirected to the Syslog server where the `pvmctl configsyslog` command is run. To redirect logs of all cluster nodes to the Syslog server, run the `pvmctl configsyslog` command on all nodes on the cluster. Refer to "Redirecting Logs to Syslog Server" on page 115 for details.
- In case of ProtectV Manager clusters, turn on global autoscaling on all cluster members individually. Refer to "Turning Global Autoscaling On" on page 134 for details.

Troubleshooting

A Node is Added Using the Incorrect IP Address of the Source Node

A fresh node cannot be added to a cluster if you enter incorrect IP address of the source node. Doing this saves the cluster state on this node, and it cannot be added to the cluster again. To handle this issue:

1. Clear the cluster state from the node by running the `cluster removeself` command.
2. Add the node to the cluster using the correct IP address of the source node.

A Member Node is Added to Another Cluster

When you want to move a member node from a cluster to another cluster, the node cannot be added to the new cluster directly. To handle this issue:

1. Deregister the current node from the cluster by running the `cluster deregister` command on another running node of the cluster.
2. Clear the cluster state from the node by running the `cluster removeself` command.
3. Add the node to the new cluster using the IP address of its source node.

7

Setting up SafeNet ProtectV Gateway

Note: Instructions in this chapter are applicable if you plan to use an external ProtectV Gateway with ProtectV Manager. If you are using a local ProtectV Gateway that is launched and configured with ProtectV Manager, you may skip this chapter.

This chapter covers the following information:

Launching SafeNet ProtectV Gateway Instance

Steps to launch an external ProtectV Gateway is similar to launching a ProtectV Manager. Refer to "Launching SafeNet ProtectV Manager Instance" on page 41 for details.

In AWS, if client authentication from cloud is required, select an existing IAM role or create a new role when launching the ProtectV Gateway instance. An IAM role cannot be specified after launching the instance. Refer to "IAM Roles" on page 19 for details. An IAM role can be reused when launching a ProtectV Gateway instance. However, a policy specific to ProtectV Gateway must be attached to this role. For details on adding multiple policies to an IAM role, refer to the AWS documentation.

After the ProtectV Gateway instance is running, start its service and enroll it with ProtectV Manager, as described in "Configuring SafeNet ProtectV Gateway Instance" on the next page.

Configuring SafeNet ProtectV Gateway Instance

When the status of your instance is running, you can log on to it using a key pair. Configuring your ProtectV Gateway instance with ProtectV Manager requires an enrollment token. This token is used to authenticate ProtectV Gateway with ProtectV Manager.

Creating Gateway Enrollment Token

To create a Gateway enrollment token:

1. Log on to the ProtectV Manager Console.
2. Click the **Tokens** tab.
3. Under **Gateway Enrollment Tokens**, click **Get a New Gateway Enrollment Token**. A ProtectV Gateway enrollment token will be generated, with details similar to the following.

   ```
   ID 33daf262-d64e-407f-aab8-73f34724cffe
   ```

```
Token 8qvLWbniwXDXjyRwLkScLQhJ5As1FwWF
Created 2017-05-01T06:17:28.435393156Z
```

4. Copy the generated Token. For example, `8qvLWbniwXDXjyRwLkScLQhJ5As1FwWF`. This token will be needed when enrolling ProtectV Gateway with ProtectV Manager.

Configuring SafeNet ProtectV Gateway Instance

Before configuring the ProtectV Gateway instance, your ProtectV Manager must be configured with KeySecure. Refer to "Configuring SafeNet ProtectV Manager with SafeNet KeySecure" on page 61 for details.

After configuring the ProtectV Manager with KeySecure, configure the ProtectV Gateway instance. This involves starting the ProtectV Gateway service and enrolling the ProtectV Gateway with ProtectV Manager. Optionally, you can set up ProtectV Gateway to use the proxy server.

To configure the ProtectV Gateway instance:

1. Log on as `pvadmin`. This is the default user.
2. Start the ProtectV Gateway service.

   Run: `sudo pvmctl gwstart --pvmip=PVMIP --prikeypass="PRIKEYPASS"`

   Here,

   - `PVMIP` – Private IP address of ProtectV Manager.
   - `"PRIKEYPASS"` – The password of the private key. For example, `--prikeypass="password"`. If not specified, you will be prompted for the private key password during the command run.

   > **Note:** Running the `pvmctl gwstart` command for the first time sets password for the private key. **Remember this password.** You will need this password when running the `sudo pvmctl gwstart` command subsequently.
   >
   > The private key password can be changed any time later. Refer to "Changing the Private Key Password" on page 67 for details.

   For example:

   ```
   pvadmin@ip-172-30-1-46:~$ sudo pvmctl gwstart --pvmip=172.30.3.57 --
   prikeypass="password"
   ```

   > **Note:** Rerun the `pvmctl gwstart` command every time the IP address of ProtectV Manager changes.

3. *(Optional)* Skip this step if client authentication from cloud needs to be disabled. Set up ProtectV Gateway to use your proxy server for AWS calls. It checks for connectivity to https://aws.amazon.com. Refer to "Using Proxy for AWS Calls" on the next page for details.

   Run: `sudo pvmctl gwconfigproxy set --proxyip=PROXYIP --proxyport=PROXYPORT --proxyusername=PROXYUSERNAME --proxypass="PROXYPASS"`

   Here,

   - `PROXYIP` – IP address or hostname of the proxy server.

- `PROXYPORT` – Port of the proxy server.
- `PROXYUSERNAME` – Proxy server's user.
- `"PROXYPASS"` – Password for the user.

For example:

```
pvadmin@ip-172-30-1-46:~$ sudo pvmctl gwconfigproxy set 10.154.60.19 8888 --
proxyusername=proxyuser --proxypass="proxypassword"
```

4. Check whether ProtectV Gateway is running.

   Run: `sudo pvmctl gwstatus`

5. Enroll ProtectV Gateway with ProtectV Manager.

   Run: `sudo pvmctl gwenroll --enrollmenttoken=ENROLLMENTTOKEN`

   Here, `ENROLLMENTTOKEN` represents the ProtectV Gateway enrollment token, created earlier. Refer to " Creating Gateway Enrollment Token" on page 85 for steps to generate a token.

   For example:

```
pvadmin@ip-172-30-1-46:~$ sudo pvmctl gwenroll --
enrollmenttoken=8qvLWbniwXDXjyRwLkScLQhJ5As1FwWF
```

6. Verify the enrollment status on the ProtectV Manager Console.

   a. Log on to the ProtectV Manager Console.

   b. Click the **Gateways** tab.

   c. View the list of IP addresses under the **Gateways** section.

   The Private IP address of your gateway instance must be listed. It shows that your Gateway instance is enrolled with the ProtectV Manager successfully.

Optionally, you can configure client authentication from cloud to verify the existence of client instances requesting keys and other information from ProtectV Gateway in the AWS account. Refer to "Client Authentication from Cloud" on page 89 for details.

Using Proxy for AWS Calls

A Web proxy is needed only when external Gateway is running in AWS to manage client instances in AWS. It is needed if "client authentication from cloud" is enabled on the external Gateway instance and Amazon EC2 endpoints are inaccessible from external Gateway.

The `pvmctl` command provides the following options to configure external Gateway to use proxy for AWS calls:

- `gwconfigproxy set --proxyip=PROXYIP --proxyport=PROXYPORT --proxyusername=PROXYUSERNAME --proxypass="PROXYPASS"` – Sets proxy for AWS calls.
- `gwconfigproxy unset` – Unsets proxy for AWS calls.
- `gwconfigproxy status` – Gets proxy settings for AWS calls.

Use `pvmctl gwconfigproxy --help` to see more details.

The `gwconfigproxy` commands are described in the following sections:

- "Checking Proxy Settings" on the next page
- "Setting SafeNet ProtectV Gateway for AWS Calls" on the next page

- "Unsetting SafeNet ProtectV Gateway for AWS Calls" below

Checking Proxy Settings

To check the proxy status and, if configured, get proxy settings for AWS calls:

Run: `sudo pvmctl gwconfigproxy status`

For example:

```
pvadmin@ip-172-30-1-46:~$ sudo pvmctl gwconfigproxy status
Proxy is configured.
Proxy Address : ip-10-154-60-19:8888
Proxy user :
```

If proxy is not set up, the status will be `Proxy is not configured`.

For example:

```
pvadmin@ip-172-30-1-46:~$ sudo pvmctl gwconfigproxy status
Proxy is not configured.
```

Setting SafeNet ProtectV Gateway for AWS Calls

You can set up your external ProtectV Gateway instance to use proxy server for AWS calls. It checks for connectivity to https://aws.amazon.com. By default, proxy is not configured for AWS calls.

To set up external ProtectV Gateway for AWS calls:

Run: `sudo pvmctl gwconfigproxy set --proxyip=PROXYIP --proxyport=PROXYPORT --proxyusername=PROXYUSERNAME --proxypass="PROXYPASS"`

Here,

- `PROXYIP` – Private IP address or hostname of the proxy server.
- `PROXYPORT` – Port of the proxy server.
- `PROXYUSERNAME` – Proxy server's user.
- `"PROXYPASS"` – Password for the user.

> **Note:** Username and password are needed if the proxy server requires authentication.

For example:

```
pvadmin@ip-172-30-1-46:~$ sudo pvmctl gwconfigproxy set --proxyip=10.154.60.19 --proxyport=8888 --proxyusername=proxyuser --proxypass="proxyuserpassword"
Successfully updated proxy configuration!
```

Unsetting SafeNet ProtectV Gateway for AWS Calls

To unset external ProtectV Gateway for AWS calls:

Run: `sudo pvmctl gwconfigproxy unset`

For example:

```
pvadmin@ip-172-30-1-46:~$ sudo pvmctl gwconfigproxy unset
Proxy is unset.
Warning: Attempt to connect to internet failed on removing proxy.
```

The `pvmctl gwconfigproxy unset` command unsets the proxy regardless of accessibility to AWS EC2 endpoints from external ProtectV Gateway.

Client Authentication from Cloud

> **Note:** Client authentication from cloud is supported for Amazon AWS only. It is not supported for other clouds and virtual environments. For such environments, ensure that client authentication from cloud is **disabled** on external ProtectV Gateway.

Client authentication from cloud, if enabled for Amazon EC2, uses an AWS EC2 API to verify the existence of client instances requesting keys and other information from external Gateway in the AWS account. If a client instance is found, then only the client instance is registered, and granted keys.

By default, client authentication from cloud is disabled.

ProtectV Gateway uses its instance profile for authentication required to call AWS API `DescribeInstances`. If client authentication from cloud is disabled, then availability of client instance is not checked in cloud.

The `pvmctl` command provides the `gwconfigcloudauth` option to configure client authentication from cloud.

> **Note:** Client authentication from cloud requires that AWS EC2 endpoints are accessible from external ProtectV Gateway. Refer to http://docs.aws.amazon.com/general/latest/gr/rande.html#ec2_region for details.

> **Note:** If client authentication is enabled and AWS EC2 endpoints are inaccessible from external ProtectV Gateway, the gateway cannot authenticate client from cloud. To resolve the issue, perform either of the following:
> – **Enable proxy** by running: `pvmctl gwconfigproxy set --proxyip=PROXYIP --proxyport=PROXYPORT --proxyusername=PROXYUSERNAME --proxypass="PROXYPASS"`
> – **Disable client authentication from cloud** by running: `pvmctl gwconfigcloudauth disable`

Usage of gwconfigcloudauth

To view usage of the `gwconfigcloudauth` option, run:

```
sudo pvmctl gwconfigcloudauth --help
```

For example:

```
pvadmin@ip-172-30-1-46:~$ sudo pvmctl gwconfigcloudauth --help
usage: pvmctl gwconfigcloudauth <command> [<args> ...]

Configures and checks client authentication from cloud.
```

```
Flags:
  --help  Show context-sensitive help (also try --help-long and --help-man).

Subcommands:
  gwconfigcloudauth enable
    Enable client authentication from cloud.

  gwconfigcloudauth disable
    Disable client authentication from cloud.

  gwconfigcloudauth status [<instanceID>] [<instanceRegion>]
    Check configuration for client authentication from cloud. Provide instance ID
and region of a client instance to check end-to-end connectivity with client.
```

You can use the `gwconfigcloudauth` option with its subcommands for:

- "Checking Connectivity with a Client Instance" below
- "Enabling Client Authentication from Cloud" on the next page
- "Disabling Client Authentication from Cloud" on the next page

Checking Connectivity with a Client Instance

You can check configuration for client authentication from cloud. Provide the Instance ID and region of a client instance to check whether the configuration to authenticate a client from cloud is correct.

To check connectivity with a client instance:

Run: `sudo pvmctl gwconfigcloudauth status [--instanceid=INSTANCEID] [--instanceregion=INSTANCEREGION]`

Here,

- `INSTANCEID` – `InstanceID` of the client instance to check end-to-end connectivity.
- `INSTANCEREGION` – Region of the client instance to check end-to-end connectivity.

Example 1:

```
pvadmin@ip-172-30-1-46:~$ sudo pvmctl gwconfigcloudauth status --instanceid=i-961c2b28 --instanceregion=us-east-1

Configuration for client authentication from cloud is Ok!
```

Example 2:

```
pvadmin@ip-172-30-1-46:~$ sudo pvmctl gwconfigcloudauth status

Client Authentication from cloud is enabled.
```

Enabling Client Authentication from Cloud

By default, client authentication from cloud is disabled. You can enable it whenever client authentication from cloud is required.

To enable client authentication from cloud, run: `sudo pvmctl gwconfigcloudauth enable --cloud=<cloudname>`

For example:

```
pvadmin@ip-172-30-1-46:~$ sudo pvmctl gwconfigcloudauth enable --cloud=aws
Client authentication from cloud is enabled.
```

Enabling client authentication from cloud checks for connectivity to https://aws.amazon.com. If connectivity is unavailable, an error occurs.

Disabling Client Authentication from Cloud

By default, client authentication from cloud is disabled. If you enabled it manually, you can later disable it whenever needed.

To disable cloud authentication from cloud:

Run: `sudo pvmctl gwconfigcloudauth disable`

For example:

```
pvadmin@ip-172-30-1-46:~$ sudo pvmctl gwconfigcloudauth disable
Client authentication from cloud is disabled.
```

8
Encrypting Partitions on Linux

This chapter explains how to encrypt partitions on Linux client instances using SafeNet ProtectV.

This chapter covers the following information:

> **Note:** If `/boot` exists on a separate partition, then it must be the first partition on the disk. If `/boot` exists on the same partition as the root partition (/), then this partition must the first partition on the disk.

> **Note:** Raw disks cannot be encrypted.

Refer to the *SafeNet ProtectV Clients Customer Release Notes* for the complete list of supported platforms.

Encrypting Partitions with Existing Data

Partitions using the `ext2`, `ext3`, or `ext4` file system need not be empty for encryption.

SafeNet ProtectV supports encryption of system partitions without a spare disk as long as long as `/boot` and `/` are different partitions for the `ext2`, `ext3`, or `ext4` file system.

If `/boot` and `/` are on the same partition, encryption of the system partition is skipped. Events are logged indicating that a spare disk is required. After adding the spare disk, the system reboot is required for encryption.

> **Note:** Data partitions using the `XFS` file system can be encrypted. Non-empty `XFS` partitions (system and data) require a spare disk of the same or larger size. Empty partitions do not require a spare disk.

Creating an Image Enrollment Token

Deploying SafeNet ProtectV on your client instance requires an image enrollment token. This token is used to authenticate the client instance with ProtectV Manager.

To generate an image enrollment token:

1. Log on to the ProtectV Manager Console.
2. Click the **Tokens** tab.
3. Under **Image Enrollment Tokens**, click **Get a New Image Enrollment Token**. An image enrollment token will be generated, with details similar to the following.

   ```
   ID 64d13da5-20ad-4116-b678-dbd12d33dce5
   Token FLIYYuZ4S1TnGbEmGgdf6T04HVjDd8C9
   Created 2017-05-01T03:54:01.99632226Z
   ```

4. Copy the generated Token. For example, `FLIYYuZ4S1TnGbEmGgdf6T04HVjDd8C9`. You will use this token to enroll the client instance with ProtectV Manager.

Exporting the CA Certificate

A CA certificate is needed to verify the client certificate. You will need this certificate when registering your client instance with ProtectV Manager.

To export the CA certificate for clients to use:

1. Log on to the ProtectV Manager Console.
2. Click the **Tokens** tab.
3. Under **CA Certificate**, click **Get CA Certificate**. The CA certificate, similar to the following, will be displayed.

   ```
   -----BEGIN CERTIFICATE-----
   MIIFDTCCAvegAwIBAgIVALaTxTopPlcGE3nsv/rhdPA6Q4HjMAsGCSqGSIb3DQEB
   CzAgMQswCQYDVQQGEwJVUzERMA8GA1UEChMIUHJvdGVjdFYwHhcNMTYwMjE2MTA1
   MjM3WhcNMjEwNzIxMTA1MjM3WjAgMQswCQYDVQQGEwJVUzERMA8GA1UEChMIUHJv
   dGVjdFYwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDXIbIz22n0eaLm
   +liRVCWPav1348pXFX/u1LxYM1KJCb7dGXAQRsgFad5riR12G5vBz/77duePJPM3
   bA4af3DviB1mAd4htzYR6Ptqh2O/Qiu6npudLkKhIUM/2iEJZIU1nYdmPNq/eida
   qu6/h474Zrt7g15u/RZ5wd1+Tj6sTdMPkj6gf5HMx65vxbpdK5+X0KKpYo2BwZ9D
   fKm94Y3OOcr4GVZTOnukiW8GxoKO7RspsqIsr9Lf/Z5jpU88spO0nQzHojLLv3fX
   8hANRylRZesC2R116exH0tRzjbY8pYKtQxJEpOjv4/iRyoGG/Aysr+IByDSw2FUW
   +0n1NKZLm0BH0M5YAdPILDur7Tvz3PduRPHoGpD6wMbOuUR2phpPVwa7ltvGD/gZ
   0lJxDPere/9Mhr/GCj2G6Z91lHwhUuxau89L5TpY3DIvXN218u1eEAAmr87EcAgM
   1AkjKx01zPkhkcQgocxMXarcn2QO4Cbom8luShl2WzInZ/qgSi5Ub6bpcIodsBoj
   3ObVlT09MF9ZdPafBXKnGZxZzEBZOWlWPywgJT+BCEKSsv4Ildm/V/hgY2jYGC5x
   qbRZacWyGV4hoYjO2kJg8DkNqPltqH+d36huxiZ6RNk0fm5Y4UQcX8QrEcUJCp0e
   ```

```
mUSNlZ1AEwK4OQGjkTKyA1PEBlgwawIDAQABo0IwQDAOBgNVHQ8BAf8EBAMCAIQw
HQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMBMA8GA1UdEwEB/wQFMAMBAf8w
CwYJKoZIhvcNAQELA4ICAQDJ5yXXpX39zrQ1TC4566ofKvLwERi2JnF0ECQGSWr4
rDT6vdbKL9CkILctIH2NHrbz1YQ+9LDfWemjdjUVrYwlJejpH6zTpT3u8ogYFGK2
0zYkS691Dj6yrVgHqZV7kwO8FPSwzvOiCHZj7AzAliZk2FEKYIc2PlhETznRTOqz
pqQ0gTIZLns7+y1+QXRiHf+2y61C8F9BGA35VMX3bgJgEYF+7l4WbvmDwuFlAhY0
jvfSUoqmpYdF+v5fUZeJ0ExFObFd1pAh7TKbxM2FKbxhHMLYdwqe2q4rhorlOs+A
InhrZEe5D7x+TJeRTu5B/aUPxUMffC7KnBErV3NggyMXkzuNhKZ31bKB5TWcOoiY
IHsoSiaiEa/m8qn11NpCSZTdg+roayRKPEtbyBPNRR9aJ7E0P9vnfzB44B2pafl1
qwHCKnuYREF4oFirpymJuwLK6JkpzbcxgYazToQP6QtsTVAw2y2CSGVUgGPXdHSd
Aqm3y4CnW2ztKhAoyql/nkb7/XKnk49XM848A+dhv7VTooKaBpWHwayA1h5i8vbu
cg4eOfZ0FOkc1aMTCh8Fbm05Lope4F9nV0fBlN1BGycaC5m9AtYajEWRgmDIisUi
3KD1r5zptGWxQc0XOOuALggT8HXHPJzmlxgs6vgcnJY4EZ4liGFSWUdS9Si8uffh
kA==
-----END CERTIFICATE-----
```

4. Copy the certificate text. The copied text must include the header (`-----BEGIN CERTIFICATE-----`) and footer (`-----END CERTIFICATE-----`).
5. Paste the certificate text in a file.
6. Save the file as certificate file (`.crt`.) For example, `ca.crt`.

Deploying SafeNet ProtectV on Linux

Deploying SafeNet ProtectV on a Linux client instance involves installing the SafeNet ProtectV client, setting up the network interface, and registering the instance with ProtectV Manager.

1. "Installing the SafeNet ProtectV Client" below
2. "Setting up the Network Interface" on page 96
3. "Registering the Client Instance with SafeNet ProtectV Manager" on page 98

These steps are described in subsequent sections.

> **Note:** For encryption of Linux machines in the IBM Bluemix cloud, either ProtectV Manager or ProtectV Gateway must also be in IBM Bluemix. When registering the Linux clients in IBM Bluemix, specify private IP addresses of ProtectV Manager or ProtectV Gateway in the `registration.json` file.

Installing the SafeNet ProtectV Client

The ProtectV installer for RHEL and SLES 12 SP2 are `rpm` packages; for Ubuntu, it is a `deb` package.

Note: On RHEL 6.7 VMs based on Azure public images published by Red Hat, the default repository picked by `yum` installs `devtools-gcc` instead of `gcc`. So before installing the SafeNet ProtectV Client on such RHEL 6.7 instances, do either of the following:
– Disable the repository by running: `yum-config-manager --disable rhui-rhel-server-rhscl-6-rhui-rpms`
– Install `gcc`

This section covers the following information:

- "Installing Dependencies on RHEL 7.x Instances" below
- "Installing Dependencies on SLES 12 SP2 Instances" on the next page
- "Installing the SafeNet ProtectV Client" on the next page

Installing Dependencies on RHEL 7.x Instances

Before installing the SafeNet ProtectV Client on RHEL 7.x instances, ensure that dependencies, `Busybox` and `Python-crypto`, are installed on these instances.

Installing Python-crypto

Install the `Python-crypto` version greater than `2.0`. This package can be found in the EPEL repository.

To configure the EPEL repository on the Linux instance:

1. Download the repository, `epel-release-<version>.noarch.rpm`.
2. Install the repository. Run: `rpm -ivh epel-release-<version>.noarch.rpm`
3. Verify the repository. Run: `yum repolist`
4. Install the dependency. Run: `yum –enablerepo=epel python-crypto`

Installing Busybox

Download and install the `Busybox` version greater than or equal to `1.12`. For example, `busybox-<version>.el6_6.x86_64.rpm`.

Note: You can also download and compile the package from source.

To install `Busybox`:

1. Download the package, `busybox-<version>.el6_6.x86_64.rpm`.
2. Install the package. Run: `rpm –ivh busybox-<version>.el6_6.x86_64.rpm`
3. Confirm the installed version. Run: `busybox | grep -i "busybox v"`

Note: Compatible versions of `Python-crypto` and `Busybox` are also available at the Gemalto Support portal. Visit the "Dependency package for SafeNet ProtectV RHEL 7.x Client Install" article for details. The article contains a link at the bottom to download the dependencies.

After the dependencies are installed, you can install the SafeNet ProtectV Client on your instances. Refer to "Installing the SafeNet ProtectV Client" on the next page.

Installing Dependencies on SLES 12 SP2 Instances

Before installing the SafeNet ProtectV Client on SLES 12 SP2 instances, ensure that dependency, `Python-crypto`, is installed on these instances. Install the `Python-crypto` version greater than `2.0`.

To install `Python-crypto` on the SLES 12 SP2 instance:

1. Install the public key that verifies RPM packages.

   Run: `rpm --import https://www.mirrorservice.org/sites/apt.sw.be/RPM-GPG-KEY.dag.txt`

2. Download the dependency, `Python-crypto`, from the Gemalto Support portal:
   a. Visit the "Dependency package for SafeNet ProtectV RHEL 7.x Client Install" article.
   b. Click the link at the bottom of the article. A Zip file is downloaded.
   c. Extract the downloaded file. It contains a compatible version of `Python-crypto`.
3. Install the dependency, `Python-crypto`.

   Run: `zypper install ./python-crypto-<version>.x86_64.rpm`

After the dependencies are installed, you can install the SafeNet ProtectV Client on your instances. Refer to "Installing the SafeNet ProtectV Client" below.

Installing the SafeNet ProtectV Client

To install the SafeNet ProtectV Client:

1. Log on to your client instance as `root`.

   On Ubuntu, login as `ubuntu` and switch to `root` (`sudo -s`.)
2. *(Optional)* Copy the CA certificate (the `.crt` file) from the ProtectV Manager instance to your client instance. For example, place the certificate at `/home/ec2-user/ca.crt` or `/home/ubuntu/ca.crt` depending upon your platform. Refer to "Exporting the CA Certificate" for details.
3. *(Ubuntu)* Ensure that `gdebi-core` is already installed on the client. To do so, run:

   ```
   sudo apt-get install gdebi-core
   ```

   You may need to update the packages. Run `apt-get update`.
4. Download the ProtectV installer package from Gemalto. Store it on your client instance.
5. Install the package. Depending on your platform, run the following command:
   - Linux: `sudo yum install <ProtectV-Installer-Package>.rpm`
   - Ubuntu: `sudo gdebi <ProtectV-Installer-Package>.deb`
   - SLES: `zypper install <ProtectV-Installer-Package>.rpm`

Now you can manually specify particular network interface and network gateway for SafeNet ProtectV preboot, if required in your setup. Refer to "Setting up the Network Interface" below for details.

Setting up the Network Interface

After installing the SafeNet ProtectV client, you can specify the network interface for the ProtectV preboot. By default, preboot uses the correct network interface. However, in some cases, for example, on a multi-homed system or a system with unusual name, you need to explicitly set the network interface for preboot. For example, for Bluemix machines, it is mandatory to set the network interface using the `pvsetip` command.

Similarly, a particular network gateway can also be forced for preboot.

Usage: `pvsetip [options]`

- `--version` – Display version information and exit.
- `-h, --help` – Display usage information and exit.
- `-d, --display` – Display pre-boot IP information.
- `-a ADAPTER, --adapter=ADAPTER` – Specify the interface name. This will cause the system settings for the named interface to be used.
- `-f` – Force use of non-system adapter settings for an interface (override system settings). Used in conjunction with the remaining parameters listed below.
- `-i IPADDR, --ipaddress=IPADDR` – (Required input if static IP is used) Set an IP address to use a static IP, or set to "dhcp" to use DHCP. Specify a private IP address.
- `-n NETMASK, --netmask=NETMASK` – (Required input if static IP is used) Set IP Mask.
- `-g GATEWAY, --gateway=GATEWAY` – (Required input if static IP is used) Set default Gateway IP address. Specify a private IP address.
- `-x INTERFACE, --interface=INTERFACE` – (Required input if static IP is used) Set the interface device name for an interface that SafeNet StartGuard can use to communicate with ProtectV Manager.
- `-r` – Save the route configuration of client.
- `-1 DNS1, --dns1=DNS1` – Set the DNS Primary address.
- `-2 DNS2, --dns2=DNS2` – Set the DNS Secondary address.

Note:
– On Linux instances in IBM Bluemix, it is mandatory to run `pvsetip` with private network adapter settings. On Ubuntu instances in IBM Bluemix, you also need to run the command `pvsetip -r`.

CAUTION: If the SafeNet ProtectV client instance uses a network gateway other than the default gateway, use `pvsetip` to ensure that preboot uses correct IP address and gateway for communication, otherwise, the SafeNet ProtectV client instance may get stuck at preboot without any recovery.

The following sections describe how to set a particular interface for preboot and how to force a particular network gateway.

Binding preboot to a Particular Interface

To bind preboot to a particular interface:

1. Run `pvsetip -a eth0`.

   For example:

```
[root@Redhat6 ~]# pvsetip -a eth0
Current preboot ip settings:
INTERFACE=eth0
MACADDR=00:50:56:01:00:12
IPADDR=dhcp
```

```
1
```

2. Verify the details by running `pvsetip -d`.

   For example:

```
[root@Redhat6 ~]# pvsetip -d
Current preboot ip settings:
INTERFACE=eth0
MACADDR=00:50:56:01:00:12
IPADDR=dhcp
```

Forcing a Particular Network Gateway

To force a particular network gateway:

1. Run the following command:

   `pvsetip -i IPADDR -g GATEWAY -n NETMASK -x INTERFACE -f`

   For example:

```
[root@Redhat6 ~]# pvsetip -i 10.121.105.56 -g 10.121.104.1 -n 255.255.252.0 -x eth0 -f
Warning: using system DNS configuration.
Warning: Cannot determine DNS configuration.
Current preboot ip settings:
INTERFACE=eth0
NETMASK=255.255.252.0
MACADDR=00:50:56:01:00:12
IPADDR=10.121.105.56
GATEWAY=10.121.104.1
```

2. Verify the details by running `pvsetip -d`.

   For example:

```
[root@Redhat6 ~]# pvsetip -d
Warning: Cannot determine DNS configuration.
Current preboot ip settings:
INTERFACE=eth0
NETMASK=255.255.252.0
MACADDR=00:50:56:01:00:12
IPADDR=10.121.105.56
GATEWAY=10.121.104.1
```

After setting up the network interface and network gateway, you need to register the client instance with ProtectV Manager. Refer to "Registering the Client Instance with ProtectV Manager" for details.

Registering the Client Instance with SafeNet ProtectV Manager

After installing ProtectV on your instance, register it with ProtectV Manager.

To register the client instance:

1. Navigate to the `/opt/protectv1/bootagent/` directory.
2. Run the following command:

   `sudo ./pvreg <Image-Enrollment-Token> <Gateway IP> [Path-to-CA-Certificate.crt]`

   Here,

- `<Image-Enrollment-Token>` – Represents the image enrollment token to authenticate the client instance with ProtectV Manager. You can generate it on the Images tab of the ProtectV Manager Console. Refer to "Creating an Image Enrollment Token" for details.
- `<Gateway IP>` – Specifies the IP address of the Gateway instance. Specify IPs for multiple Gateways separated by (:) colons. For example, when two Gateway instances are configured, run:

  ```
  ./pvreg Image-Enrollment-Token <Gateway1 IP>:<Gateway2 IP> [Path-to-CA-Certificate.crt]
  ```

  Note: For encryption of Linux machines in the IBM Bluemix cloud, either ProtectV Manager or ProtectV Gateway must also be in IBM Bluemix. When registering the Linux clients in IBM Bluemix, specify private IP addresses of ProtectV Manager or ProtectV Gateway in the `registration.json` file.

- `[Path-to-CA-Certificate.crt]` – *(Optional)* Specifies path to the `.crt` file on your client instance. This is the certificate that you exported in "Exporting the CA Certificate."

  Note: Specifying the CA certificate in the registration file is *optional*. If it is not specified, the client calls SafeNet ProtectV Gateway for root certificate before starting the registration process.

For example:

```
sudo ./pvreg FLIYYuZ4S1TnGbEmGgdf6T04HVjDd8C9 10.69.88.226:10.69.88.227

The registration.json file is created at /opt/protectvl/bootagent/logan. The file content is:

{"registrationToken":" FLIYYuZ4S1TnGbEmGgdf6T04HVjDd8C9","gatewayURLs": ["https://10.69.88.226", "https://10.69.88.227"]}
```

For example, when passing the certificate manually:

```
sudo ./pvreg FLIYYuZ4S1TnGbEmGgdf6T04HVjDd8C9 10.69.88.226:10.69.88.227 /home/ec2-user/ca.crt

The registration.json file is created at /opt/protectvl/bootagent/logan. The file content is:

{"registrationToken":" FLIYYuZ4S1TnGbEmGgdf6T04HVjDd8C9","gatewayURLs": ["https://10.69.88.226", "https://10.69.88.227"], "ca_cert": "/home/ec2-user/ca.crt"}
```

On Ubuntu, `Path-to-CA-Certificate.crt` could be `/home/ubuntu/ca.crt`.

3. Verify the registration. To do so, check whether the `reginfo` file exists at `/boot/pvstore`. If the `reginfo` file exists, the client registration is successful.
4. Reboot the client instance after successful registration.

This will encrypt your volumes/partitions except the root (`/`) partition. It may take some time to encrypt your partitions. Refer to "Verifying Encryption Status" for instructions to verify the encryption status.

Refer to "Encrypting the Root Partition" for instructions on encrypting the root partition.

Note: SafeNet ProtectV supports Linux software RAID. If it is installed after SafeNet ProtectV client is deployed, then run the following command on your RHEL instance:

```
dracut --mdadmconf --force /boot/initramfs-$(uname -r).img $(uname -r)
```

If Linux software RAID is installed before deploying SafeNet ProtectV, then no need to run this command.

Verifying Encryption Status

After SafeNet ProtectV Client image is installed and the instance is rebooted, it takes some time for each partition to encrypt. Verify the encryption status by either Command pvinfo or ProtectV Manager Console, as explained below.

SafeNet ProtectV can be configured to automatically change encryption keys with which partitions are encrypted. Refer to ""Rotating Keys (Rekey)" on page 140" for details.

Command pvinfo

Run the command `sudo pvinfo` on the client instance.

For example:

```
root@ip-10-232-99-203:~# sudo pvinfo
ProtectV Linux <version>
Device    Mount         Size   Protected            fs     ca   System
xvdh      /data   1073741824         yes   crypto_LUKS   True    False
xvdi       swap   1073741824         yes   crypto_LUKS   True    False
xvda1         /   8589934592          no          ext4   True     True
```

The output indicates that all partitions **except the root** (`/`) **partition** are protected.

SafeNet ProtectV Manager Console

Alternatively, use the ProtectV Manager Console.

To verify the encryption status:

1. Log on to the ProtectV Manager Console.
2. Click the **Images** tab.
3. View the images under **Image Name**. The IP address of your client instance must be listed.
4. Click the link under **Image Name**.

The locked icon () indicates that the volume is protected.

Encrypting the Root Partition

To encrypt root partitions, additional steps are performed. You can encrypt root partitions if partitions on your client instance are *already encrypted* or when *launching a new client instance*.

There may be two scenarios:

- `/boot` and root (`/`) exist on the same partition. A work disk is always needed for encryption.
- `/boot` and root (`/`) exist on different partitions. If the file system is `ext3` or `ext4`, a work disk is not needed. When the file system is `xfs`, then a work disk is needed.

When Client Partitions are Already Encrypted

To encrypt the root partition:

1. Attach a raw disk of the same size as your root partition.
2. Reboot your instance.

When Launching a New Client Instance

To encrypt the root partition:

1. Attach a raw disk of the same size as your root partition.
2. Deploy SafeNet ProtectV on the client instance, as described above.

> **Note:** After encryption of your root partition, it is recommended to detach and delete raw disk that you attached during **Step 1**.

Troubleshooting

Registration Unsuccessful

If the registration does not succeed:

1. Check for errors in the `/var/log/protectvl.log` file. Parameters in the `registration.json` file may be incorrect. Refer to "SafeNet ProtectV Client Logs" on page 114 for details on `protectvl.log`.
2. Rerun the `pvreg` command with updated parameters.
3. Reboot the client instance for successful registration.
4. Again reboot the client instance for successful encryption.

Client Instance Does Not Come Up

If due to any reasons, your client instance does not come up after reboot, restart it from console.

Updating the Registration File

At times, you may want to update configuration, such as the IP address of ProtectV Gateway or path of the CA certificate, in the registration file.

To update the registration file:

1. Log on to your client instance as `root`.
2. Navigate to `/opt/protectvl/bootagent/`.
3. Run the following command with correct values:

   ```
   ./pvreg <Image-Enrollment-Token> <Gateway IP> [Path-to-CA-Certificate.crt]
   ```

4. Stop the **SafeNet ProtectV** service.

   ```
   /etc/init.d/protectvl.sh stop
   Stopping ProtectV Client ...
   ```

5. Start the **SafeNet ProtectV** service.

   ```
   /etc/init.d/protectvl.sh start
   Starting ProtectV Client ...
   ```

The values in the registration file are updated.

Uninstalling the ProtectV Client

When a client instance is decrypted, you can uninstall the ProtectV Client from the instance.

To uninstall the ProtectV Client from a client instance:

1. Ensure that the client is decrypted. Refer to "Decrypting Client Instances" on page 132.
2. Log on to your client instance as `root`.
3. Depending on your platform, run the following command:
   - **RHEL/CentOS:** `yum remove pvlinux`
   - **Ubuntu:** `apt-get purge pvlinux`

9
Encrypting Partitions on Windows

This chapter explains how to encrypt partitions on Windows client instances using SafeNet ProtectV. Refer to the *SafeNet ProtectV Clients Customer Release Notes* for the complete list of supported platforms.

This chapter covers the following information:

Creating an Image Enrollment Token

Deploying SafeNet ProtectV on your client instance requires an image enrollment token. This token is used to authenticate the client instance with ProtectV Manager.

Refer to “Creating an Image Enrollment Token” for details.

Exporting the CA Certificate

A CA certificate is needed to verify the client certificate. You will need this certificate when registering your client instance with ProtectV Manager.

Refer to “Exporting the CA Certificate” for details.

Deploying SafeNet ProtectV on Windows

Deploying SafeNet ProtectV on a Windows client instance involves installing the SafeNet ProtectV client and registering the instance with ProtectV Manager.

1. Installing the SafeNet ProtectV Client
2. Registering the Client Instance with SafeNet ProtectV Manager

These steps are described in subsequent sections.

Installing the SafeNet ProtectV Client

Note: Before installing SafeNet ProtectV 4.x on 64-bit Microsoft Windows Server 2008 R2 SP1 and Microsoft Windows 7 SP1 platforms, ensure that Security Update for Windows 64-bit is installed on the systems. After installing this update, the file server must be restarted. Refer to Microsoft Knowledge Base article (KB3033929) for details.

To install the SafeNet ProtectV client:

1. Log on to your client instance as administrator.
2. *(Optional)* Copy the CA certificate (the `.crt` file) from the ProtectV Manager instance to your client instance. For example, place the certificate at `C:\\ca.crt`. Refer to "Exporting the CA Certificate" for details.
3. Download the **SafeNet ProtectV installer** (an `MSI` file for Windows) from Gemalto. Store it on your client instance.
4. Double-click the installer. The **SafeNet ProtectV - InstallShield Wizard** is displayed.
5. Walk through the installer by clicking **Next**. Finish the installation.

Note: When installing the ProtectV Windows client on Bluemix virtual machines, select the public network interface on the SafeNet ProtectV StartGuard IP Address screen of the SafeNet ProtectV InstallShield wizard. The ProtectV Windows client will work with ProtectV Manager irrespective of the cloud.

By default, the private network interface is selected. In this case, ProtectV Manager must be in the Bluemix cloud only. After installation and before "Registering the Client Instance with SafeNet ProtectV Manager" on page 106, you need to run the `setip.exe` program with private network adapter settings. Refer to "Setting up the Network Interface" below for details.

6. Restart the instance when prompted.

Now you need to register the client instance with ProtectV Manager. Refer to "Registering the Client Instance with ProtectV Manager" for details.

Setting up the Network Interface

After installing the SafeNet ProtectV client on Bluemix virtual machines with private network interface, you need to run the `setip.exe` program. You can specify IP mask, Gateway IP, Mac address, and IP addresses of DNS for the ProtectV preboot. By default, preboot uses the correct network interface. However, in some cases, for example, on a multi-homed system or a system with unusual name, you need to explicitly set the network interface for preboot. For example, for Bluemix machines, it is mandatory to set the network interface using the `setip.exe` program. Similarly, a particular network gateway can also be forced for preboot.

Note: Refer to https://www.freebsd.org/releases/11.0R/hardware.html#ethernet for the list of supported network cards.

The following section describes how to set a particular network Gateway for preboot.

Forcing a Particular Network Gateway

To force a particular network gateway:

1. View the details by running `setip.exe /d`.

   For example:

   ```
   C:\Program Files\SafeNet ProtectV\Tools>setip /d
   Safenet ProtectV v4.0.0.451
   Current settings:
   IP Enabled.
   IP Address is set to [10.164.197.214]
   IP Mask is set to [255.255.255.192]
   IP Gateway is set to [0.0.0.0]
   Mac Address is set to [06:7d:21:dd:15:eb]
   DNS Primary is set to [10.0.80.11]
   DNS Secondary is set to [10.0.80.12]
   ```

2. Run the following command:

   ```
   setip /IP <IP address of client> /Mask <IP Mask> /GW <Gateway IP> /MAC <Mac
   Address> /DNS1 <Primary DNS IP> /DNS2 <Secondary DNS IP> /f
   ```

   For example:

   ```
   C:\Program Files\SafeNet ProtectV\Tools>setip /IP 10.164.197.214 /Mask 255.255.255.192 /GW
   10.164.197.193  /MAC 06:7D:21:DD:15:EB /DNS1 10.0.80.11 /DNS2 10.0.80.12  /f
   Safenet ProtectV v4.0.0.451
   Set IP Mask to [255.255.255.192]
   Set IP Gateway to [10.164.197.193]
   Set DNS Primary to [10.0.80.11]
   Set DNS Secondary to [10.0.80.12]
   Mac Address is set to [06:7D:21:DD:15:EB]
   IP Enabled.
   Set IP Address to [10.164.197.214]
   ```

3. Verify the details by running `setip.exe /d`.

   For example:

   ```
   C:\Program Files\SafeNet ProtectV\Tools>setip /d
   Safenet ProtectV v4.0.0.451
   Current settings:
   IP Enabled.
   IP Address is set to [10.164.197.214]
   IP Mask is set to [255.255.255.192]
   IP Gateway is set to [10.164.197.193]
   Mac Address is set to [06:7D:21:DD:15:EB]
   DNS Primary is set to [10.0.80.11]
   DNS Secondary is set to [10.0.80.12]
   ```

CAUTION: If the SafeNet ProtectV client instance uses a network gateway other than the default gateway, use `setip` to ensure that preboot uses correct IP address and gateway for communication, otherwise, the SafeNet ProtectV client instance may get stuck at preboot without any recovery.

After setting up the network interface and network gateway, you need to register the client instance with ProtectV Manager. Refer to "Registering the Client Instance with ProtectV Manager" for details.

Registering the Client Instance with SafeNet ProtectV Manager

After the instance is restarted, register it with ProtectV Manager.

To register the client instance:

1. Open the command prompt.
2. Navigate to `C:\Program Files\SafeNet ProtectV`.
3. Run the following command:

   ```
   pvreg.exe <Image-Enrollment-Token> <Gateway IP> [Path-to-CA-Certificate.crt]
   ```

   Here,

   - `<Image-Enrollment-Token>` – Represents the image enrollment token to authenticate the client instance with ProtectV Manager. Refer to "Creating an Image Enrollment Token" for details.
   - `<Gateway IP>` – Specifies the IP address of the ProtectV Gateway instance. Specify IPs for multiple Gateways separated by (:) colons. For example, when two Gateway instances are configured, run:

     ```
     pvreg.exe <Image-Enrollment-Token> <Gateway1 IP>:<Gateway2 IP> [Path-to-CA-Certificate.crt]
     ```

     Note: When registering the ProtectV Windows clients in Bluemix, specify private IP addresses of Gateways if the private network interface was selected when installing the client.

   - `[Path-to-CA-Certificate.crt]` – *(Optional)* Specifies path to the `.crt` file on your client instance. This is the certificate that you exported in "Exporting the CA Certificate."

     Note: Specifying the CA certificate in the registration file is *optional*. If it is not specified, the client calls SafeNet ProtectV Gateway for root certificate before starting the registration process.

   For example:

   ```
   pvreg.exe FLIYYuZ4S1TnGbEmGgdf6T04HVjDd8C9 10.69.88.226:10.69.88.227

   The registration.json file is created at C:\Program Files\SafeNet ProtectV\logan. The file content is:

   {"registrationToken":"FLIYYuZ4S1TnGbEmGgdf6T04HVjDd8C9","gatewayURLs":["https://10.69.88.226", "https://10.69.88.227"]}
   ```

   For example, when passing the certificate manually:

   ```
   pvreg.exe FLIYYuZ4S1TnGbEmGgdf6T04HVjDd8C9 10.69.88.226:10.69.88.227 "C:\\ca.crt"

   The registration.json file is created at C:\Program Files\SafeNet ProtectV\logan. The file content is:

   {"registrationToken":"FLIYYuZ4S1TnGbEmGgdf6T04HVjDd8C9","gatewayURLs":["https://10.69.88.226", "https://10.69.88.227"], "ca_cert": "C:\\ca.crt"}
   ```

As soon as the `registration.json` file is created, volume encryption starts. It may take some time to encrypt your partitions. Refer to "Verifying Encryption Status" for instructions to verify the encryption status.

Verifying Encryption Status

Verify the encryption status by either Local ProtectV Management Console or ProtectV Manager Console, as explained below.

SafeNet ProtectV can be configured to automatically change encryption keys with which partitions are encrypted. Refer to ""Rotating Keys (Rekey)" on page 140" for details.

Local SafeNet ProtectV Management Console

After ProtectV Client Image is installed and the `registration.json` file is created, volume encryption starts. It takes some time for each partition to encrypt.

To check the encryption status:

1. Remote desktop to the client instance.
2. Navigate to `C:\Program Files\SafeNet ProtectV`.
3. Double-click `LocalMC.exe`.

The **Encryption Status** dialog box is displayed. It shows the percent encrypted for each drive/partition. At the start, the status of a drive is **Encrypting** and the drive icon is **half red**. After the encryption is complete, the status becomes **Encrypted** and the drive icon changes to **red**.

SafeNet ProtectV Manager Console

Alternatively, view the encryption status on the ProtectV Manager Console.

To verify the encryption status:

1. Log on to the ProtectV Manager Console.
2. Click the **Images** tab.
3. View the images under **Image Name**. The IP address of your client instance must be listed.
4. Click the link under **Image Name**.

The locked icon ( ) indicates that the volume is protected.

> **Note:** If the mount point of any encrypted drive on a Windows client is changed, the name of the encryption key will no longer be visible on the ProtectV Manager console. To make the key name visible again, reboot the client instance.

Troubleshooting

Registration Unsuccessful

As soon as the `registration.json` file is created, volume encryption starts. However, if encryption does not start:

1. Check for errors in the `C:\Program Files\SafeNet ProtectV\logan\logan.log` file. Parameters in the registration file may be incorrect. Refer to "SafeNet ProtectV Client Logs" on page 114 for details on `logan.log`.
2. Rerun the `pvreg.exe` command with updated parameters.
3. Reboot the client instance.

Client Instance Does Not Come Up

If due to any reasons, your client instance does not come up after reboot, restart it from console.

Updating the Registration File

At times, you may want to update configuration, such as the IP address of ProtectV Gateway or path of the CA certificate, in the registration file.

To update the registration file:

1. Log on to your client instance as administrator.
2. Navigate to `C:\Program Files\SafeNet ProtectV`.
3. Run the following command with correct values:

   ```
   pvreg.exe <Image-Enrollment-Token> <Gateway IP> [Path-to-CA-Certificate.crt]
   ```

4. Stop the **SafeNet ProtectV** service (logan.exe). To do so, end the **logan.exe** process in the **Windows Task Manager**.
5. Start the **SafeNet ProtectV** service. To do so:
   a. Navigate to `C:\Program Files\SafeNet ProtectV\Logan`.
   b. Double-click **logan.exe**.

The values in the registration file are updated.

Uninstalling the ProtectV Client

When a client instance is decrypted, you can uninstall the ProtectV Client from the instance.

To uninstall the ProtectV Client from a client instance:

1. Ensure that the client is decrypted. Refer to "Decrypting Client Instances" on page 132.
2. Log on to your client instance as administrator.
3. Go to **Control Panel** > **Programs and Features**. The list of installed programs is displayed on the right.
4. Under the **Name** column, right-click **SafeNet ProtectV**. A shortcut menu appears.
5. Click **Uninstall**.
6. Complete the uninstallation wizard.

10
Upgrading SafeNet ProtectV Clients

You can upgrade SafeNet ProtectV Client versions 2.0.5, 3.x, and higher to the latest version.

This chapter covers the following information:

Upgrading SafeNet ProtectV Clients on Linux

SafeNet ProtectV supports upgrade from previous SafeNet ProtectV Client to the latest version.

> **Note:** If SafeNet ProtectV Clients are to be upgraded, ensure to configure ProtectV Manager 4.x with the same KeySecure server and user with which existing ProtectV Manager was configured.

This section covers the following information:

Upgrading SafeNet ProtectV 3.x/4.x Clients

To upgrade a SafeNet ProtectV 3.x/4.x Client on Linux:

1. Log on to your client instance as `root`.

   On Ubuntu, login as `ubuntu` and switch to `root` (`sudo -s`.)
2. *(Ubuntu)* Ensure that `gdebi-core` is already installed on the client. To do so, run:

   ```
   sudo apt-get install gdebi-core
   ```

   You may need to update the packages. Run `apt-get update`.
3. Download the latest SafeNet ProtectV installer package from Gemalto. Store it on your client instance.
4. Upgrade the package. Depending on your platform, run the following command:
   - Linux: `sudo yum update <ProtectV-Installer-Package>.rpm`
   - Ubuntu: `sudo gdebi <ProtectV-Installer-Package>.deb`
5. Reboot the client instance.

Now verify the upgrade. Refer to "Verify the Upgrade" for details.

Upgrading SafeNet ProtectV 2.0.5 Clients

To upgrade a SafeNet ProtectV 2.0.5 Client on Linux:

1. Log on to your client instance as `root`.

   On Ubuntu, login as `ubuntu` and switch to `root` (`sudo -s`.)
2. *(Ubuntu)* Ensure that `gdebi-core` is already installed on the client. To do so, run:

   ```
   sudo apt-get install gdebi-core
   ```

   You may need to update the packages. Run `apt-get update`.
3. Download the latest SafeNet ProtectV installer package from Gemalto. Store it on your client instance.
4. Create the `registration.json` file at `/opt/protectvl`. SafeNet ProtectV is installed in this directory.

   Note: If the registration file is unavailable in the SafeNet ProtectV installation directory, `/opt/protectvl`, the upgrade will not succeed.

   The sample content is given below:

   ```
   {"registrationToken":"FLIYYuZ4S1TnGbEmGgdf6T04HVjDd8C9","gatewayURLs":
   ["https://10.69.88.226", "https://10.69.88.227"]}
   ```
5. Update the values, as appropriate. Refer to "Registering the Client Instance with ProtectV Manager" for details.
6. Upgrade the package. Depending on your platform, run the following command:
   - Linux: `sudo yum update <ProtectV-Installer-Package>.rpm`
   - Ubuntu: `sudo gdebi <ProtectV-Installer-Package>.deb`

   Note: At the final stage of upgrade, the SafeNet ProtectV installer checks for successful registration of the client instance. If the registration is unsuccessful, a warning message is displayed. In this case, the upgrade is successful, but the ProtectV service does not start. To resolve this issue, the registration file needs to be updated. Refer to "Updating the Registration File" for details.
7. Reboot the client instance after successful registration.

Now verify the upgrade. Refer to "Verify the Upgrade" for details.

Verify the Upgrade

To verify the upgrade, run the command `sudo pvinfo` on the client instance.

- ProtectV Linux version should indicate the latest version.
- All partitions that were encrypted before upgrade should be shown as protected.
- Any partitions on disks that were not encrypted before upgrade will be automatically encrypted, one at a time.

Upgrading SafeNet ProtectV Clients on Windows

SafeNet ProtectV supports upgrade from previous SafeNet ProtectV Client to the latest version.

Note: If SafeNet ProtectV Clients are to be upgraded, ensure to configure ProtectV Manager 4.x with the same KeySecure server and user with which existing ProtectV Manager was configured.

This section covers the following information:

- "Upgrading SafeNet ProtectV 3.x/4.x Clients" below
- "Upgrading SafeNet ProtectV 2.0.5 Clients" below
- "Verify the Upgrade" on the next page

Upgrading SafeNet ProtectV 3.x/4.x Clients

To upgrade a SafeNet ProtectV 3.x/4.x client:

1. Log on to your client instance as administrator.
2. Download the latest SafeNet ProtectV installer (an `MSI` file for Windows) from Gemalto. Store it on your client instance.
3. Run the SafeNet ProtectV installer. Do either of the following:
   - Double-click `ProtectV.msi` for an interactive upgrade.
   - From the command prompt, run `msiexec /i ProtectV.msi /q` for a non-interactive experience.

   Note: It is recommended to collect the MSI log. Add `/l*v upgrade.log` to the command line. If any errors occur, check the log for the issues, fix them, and retry the upgrade.
4. An automatic reboot will occur after the upgrade is complete. The system will reboot to the OS without any user action.

   CAUTION: Do not cancel or terminate the upgrade process; allow it to complete.

Now verify the upgrade. Refer to "Verify the Upgrade" for details.

Upgrading SafeNet ProtectV 2.0.5 Clients

To upgrade a SafeNet ProtectV 2.0.5 client:

1. Log on to your client instance as administrator.
2. Download the latest SafeNet ProtectV installer (an `MSI` file for Windows) from Gemalto. Store it on your client instance.
3. Create the `registration.json` file in the same directory as the SafeNet ProtectV installer.

   Note: If the registration file is unavailable in the same directory as the SafeNet ProtectV installer, the upgrade will not succeed.

   The sample content is given below:

```
{"registrationToken":"FLIYYuZ4S1TnGbEmGgdf6T04HVjDd8C9","gatewayURLs":
["https://10.69.88.226", "https://10.69.88.227"]}
```

4. Update the values, as appropriate. Refer to "Registering the Client Instance with ProtectV Manager" for details.
5. Run the SafeNet ProtectV installer. Use either of the following:
   - Double-click `ProtectV.msi` for an interactive upgrade.
   - From the command prompt, run `msiexec /i ProtectV.msi /q` for a non-interactive experience.

> **Note:** It is recommended to collect the MSI log. Add `/l*v upgrade.log` to the command line. If any errors occur, check the log for the issues, fix them, and retry the upgrade.

6. An automatic reboot will occur after the upgrade is complete. The system will reboot to the OS without any user action.

> **CAUTION: Do not cancel or terminate the upgrade process; allow it to complete.**

Now verify the upgrade. Refer to "Verify the Upgrade" for details.

Verify the Upgrade

After upgrade, verify the encryption.

To verify the upgrade:

1. Navigate to `C:\Program Files\SafeNet ProtectV`.
2. Run the `LocalMC.exe` program.
3. Verify the following:
   - All partitions that were encrypted before upgrade should be shown as encrypted.
   - Any partitions on disks that were not encrypted before upgrade will be automatically encrypted, one at a time.

Attaching SafeNet ProtectV 2.0.5 Disks

> **Note:** This section is applicable to SafeNet ProtectV clients for Windows.

> **Note:** System disk of an instance protected with SafeNet ProtectV 2.0.5 cannot be attached to an instance protected with SafeNet ProtectV 4.X.

> **Note:** Data disks (i.e. disks that do not contain the system directory) of an instance protected with SafeNet ProtectV 2.0.5 can be attached to an instance protected with SafeNet ProtectV 4.X.

To attach a data disk of a SafeNet ProtectV 2.0.5 instance to a SafeNet ProtectV 4.X instance:

1. "Detach the Disk from the SafeNet ProtectV 2.0.5 Instance"

2. "Attach the Disk to the Latest SafeNet ProtectV Instance"
3. "Verify Successful Attachment"

These steps are described below.

Detach the Disk from the SafeNet ProtectV 2.0.5 Instance

To detach the disk from the SafeNet ProtectV 2.0.5 instance:

1. Power off the SafeNet ProtectV 2.0.5 client instance (recommended.) Alternatively, make the disk offline using the Disk Manager.
2. Identify the disk (volume) in Amazon AWS.
3. Detach the disk from the SafeNet ProtectV 2.0.5 client instance.

Now you can attach this disk to a SafeNet ProtectV 4.X client instance.

Attach the Disk to the Latest SafeNet ProtectV Instance

To attach the disk to the SafeNet ProtectV 4.X instance:

1. Identify the instance ID of the SafeNet ProtectV 4.X client instance.
2. Attach the disk (detached above) to it.
3. Make the disk online. Use the Disk Manager to ensure that the disk is online.
4. **DO NOT format the disk.** If a message requesting the disk be formatted appears, cancel it.

Verify Successful Attachment

To verify the disk attachment:

1. Navigate to `C:\Program Files\SafeNet ProtectV`.
2. Run the `LocalMC.exe` program.
3. Verify the following:
   - Any previously encrypted partitions on the attached disk should be shown as encrypted.
   - Any partitions on the disk that were not encrypted before attachment will be automatically encrypted, one at a time.

10 Logging

This chapter covers the following information:

SafeNet ProtectV Manager Logs

ProtectV Manager saves audit and services logs at `/pvm/logs`. Audit logs are also displayed under the "Audit Logs" tab on the SafeNet ProtectV Manager Console.

SafeNet ProtectV Manager Log Rotation

SafeNet ProtectV automatically rotates ProtectV Manager logs, as described below:

- **Audit logs** – A maximum of 10000 recent records are displayed on the Audit Logs tab. Older records are rotated automatically.
- **Services logs** – A new log file is generated daily, at `12:00` AM. A maximum of five log files (of only five days) are stored. Log files older than five days are deleted automatically. The log files are named as `pvm.<yyyymmdd>.log`; for example, `pvm.20170711.log` and `pvm.20170712.log`.

SafeNet ProtectV Client Logs

SafeNet ProtectV saves logs generated on client instances in client log files. Different log files are created on Linux and Windows client instances, as described below:

- **Linux** – Client logs are saved in the `/var/log/protectvl.log` file. This file contains logs of cryptographic operations (encryption, decryption, and rekey.) Additionally, the file stores logs of communication between ProtectV Manager and the client instance. These logs include information such as getting keys, policies, and partition information.
- **Windows** – Client logs are saved in the following files:
  - `C:\Program Files\SafeNet ProtectV\TraceLogs\ProtectV.log`. This file stores all client logs including logs of cryptographic operations (encryption, decryption, and rekey,) partition changes, and ProtectV services.

- `C:\Program Files\SafeNet ProtectV\logan\logan.log`. This file contains logs of communication between ProtectV Manager and the client instance. The logs include information such as metadata, policy, and changes to encryption keys.

Clients Log Rotation

SafeNet ProtectV saves logs generated on client instances in client log files (refer to "SafeNet ProtectV Client Logs" on the previous page.) SafeNet ProtectV automatically rotates each client log file as soon as it becomes 16 MB in size. Maximum six log files (including the log file being written) are stored (backed up.) After the sixth log file is full, the oldest log file is replaced by the latest log file. The rotated log files are named `<log-file>.log.1`, `<log-file>.log.2`, ..., and `<log-file>.log.5`.

For example, on Linux client instances, SafeNet ProtectV rotates the Linux client log file (`protectvl.log`) as soon as it becomes 16 MB in size. Six log files (including the log file being written, `protectvl.log`) are created. After the size of sixth log file becomes 16 MB, the oldest log file is replaced by the latest log file. The rotated log files are named `protectvl.log.1`, `protectvl.log.2`, ..., and `protectvl.log.5`.

The same log rotation mechanism applies to client log files (`ProtectV.log` and `logan.log`) generated on Windows client instances.

Redirecting Logs to Syslog Server

SafeNet ProtectV provides an option to redirect audit and services logs to a dedicated Syslog server. This feature requires that the Syslog server is already up and running in your setup.

SafeNet ProtectV supports the `syslog-ng` implementation of the Syslog protocol for Linux platforms. It is recommended to use `syslog-ng 3.5.3` with SafeNet ProtectV.

> **Note:** SafeNet ProtectV supports the `tcp`, `udp`, and `tls` protocols for the Syslog server. The `tcp` and `tls` protocols are supported by the `syslog-ng` implementation only.

You can configure the ProtectV Manager instance to redirect logs to the Syslog server as soon as the instance is launched or any time later. After configured, the ProtectV Manager instance starts redirecting the specified logs to the Syslog server.

> **Note:** Ensure that firewalls are configured to allow traffic between the Syslog server and the ProtectV Manager instance.

Configuring ProtectV Manager for TCP and UDP

This section provides steps to configure ProtectV Manager for the Syslog server using the TCP or UDP protocol for communication.

To redirect logs to the Syslog server:

1. Add Syslog settings such as the Syslog port and protocol to the Syslog server's configuration file.

Note: This document provides sample code to update the configuration file on the **syslog-ng Open Source Edition** application. Update the configuration file according to your Syslog application.

Add the following to the configuration file:

```
source s_remote { network(ip(0.0.0.0) port(<tcp_port>));  network(ip(0.0.0.0) port(<udp_
port>) transport("udp")); };
destination d_remote { file("<log file path>"); };
log { source(s_remote); destination(d_remote); };
```

Here,

- `ip(0.0.0.0)` – IP address, `0.0.0.0`, indicates that the Syslog server is ready to accept requests on any of the network interfaces.
- `port(<tcp_port>)` – Port of the Syslog server for `tcp`. Ensure that this port is open to allow traffic between the Syslog server and the ProtectV Manager instance. The default port for `tcp` is `601`.
- `port(<udp_port>)` – Port of the Syslog server for `udp`. Ensure that this port is open to allow traffic between the Syslog server and the ProtectV Manager instance. The default port for `udp` is `514`.
- `file("<log file path>")` – Path and name of the file to store logs coming from the ProtectV Manager instance. Specify a location on your Syslog server. For example, `/var/log/pvm.log`.

For example:

```
source s_remote { tcp(ip(0.0.0.0) port(601));  network(ip(0.0.0.0) port(514) transport
("udp")); };
destination d_remote { file("/var/log/pvm.log"); };
log { source(s_remote); destination(d_remote); };
```

2. Configure the ProtectV Manager instance for the Syslog server.

   Run: `sudo pvmctl configsyslog --serverip=SERVERIP --serverport=SERVERPORT --serverprotocol="SERVERPROTOCOL" --logtype="LOGTYPE"`

   Note: In SafeNet ProtectV Manager clustering, logs of only those ProtectV Manager instances will be redirected to the Syslog server where the `pvmctl configsyslog` command is run. To redirect logs of all cluster nodes to the Syslog server, run the `pvmctl configsyslog` command on all nodes on the cluster.

   Here,

   - `SERVERIP` – IP address or hostname of the Syslog server.
   - `SERVERPORT` – Port of the Syslog server. The default port for TCP is `601`, for UDP, the default port is `514`. This port must be added to the security group of ProtectV Manager.
   - `"SERVERPROTOCOL"` – Protocol for communication with the ProtectV Manager instance. The default protocol is `tcp`.
   - `"LOGTYPE"` – Type of logs to redirect to the Syslog server. Specify `"all"` to redirect audit and services logs. The default log type is `audit`. This means that only the audit logs will be redirected to the Syslog server, by default.

Configuring ProtectV Manager for TLS

Configuring ProtectV Manager for Syslog server using the TLS protocol for communication requires creation of the server key and CA certificate on the Syslog server.

To redirect logs to the Syslog server:

1. Create the CA certificate on the syslog-ng server.

   Run: `openssl req -x509 -sha256 -nodes -days 3660 -newkey rsa:4096 -keyout <server key> -out <CA certificate>.crt`

   Here,

   - `<server key>` – Full path for the server key. A server key with the specified name will be created at the specified location. For example, `/home/ubuntu/syslog-ng-tls/server.key`.
   - `<CA certificate>.crt` – Full path for the CA certificate. A CA certificate with the specified name will be created at the specified location. For example, `/home/ubuntu/syslog-ng-tls/server.crt`.

2. Add Syslog settings such as the Syslog port, protocol, server key, and server cetificate to the Syslog server's configuration file.

   > **Note:** This document provides sample code to update the configuration file on the **syslog-ng Open Source Edition** application. Update the configuration file according to your Syslog application.

   Add the following to the configuration file:

   ```
   source s_remote {
     network(ip(0.0.0.0) port(<tls_port>)
         transport("tls")
              tls( key-file("<server key>")
              cert-file("<CA certificate>.crt")
              peer-verify(optional-untrusted))
     );
   };destination d_remote { file("<log file path>"); };
   log { source(s_remote); destination(d_remote); };
   ```

   Here,

   - `ip(0.0.0.0)` – IP address, `0.0.0.0`, indicates that the Syslog server is ready to accept requests on any of the network interfaces.
   - `port(<tls_port>)` – Port of the Syslog server for `tls`. Ensure that this port is open to allow traffic between the Syslog server and the ProtectV Manager instance. The default port for `tls` is `6514`.
   - `<server key>` – Full path of the server key created above. For example, `/home/ubuntu/syslog-ng-tls/serverkey.key`.
   - `<CA certificate>.crt` – Full path of the CA certificate created above. For example, `/home/ubuntu/syslog-ng-tls/servercacert.crt`.
   - `file("<log file path>")` – Full path for the file to store logs coming from the ProtectV Manager instance. Specify a location on your Syslog server. For example, `/var/log/pvm.log`.

   For example:

   ```
   source s_remote {
     network(ip(0.0.0.0) port(6514)
   ```

```
        transport("tls")
             tls( key-file("/home/ubuntu/syslog-ng-tls/serverkey.key")
             cert-file("/home/ubuntu/syslog-ng-tls/servercacert.crt")
             peer-verify(optional-untrusted))
    );
};destination d_remote { file("/var/log/pvm.log"); };
log { source(s_remote); destination(d_remote); };
```

3. Place the CA certificate on the ProtectV Manager instance. For example, place the CA certificate at ProtectV Manager's `/home/pvadmin`.
4. Configure the ProtectV Manager instance for the Syslog server.

   Run: `sudo pvmctl configsyslog --serverip=SERVERIP --serverport=SERVERPORT --serverprotocol="SERVERPROTOCOL" --servercacert=SERVERCACERT --logtype="LOGTYPE"`

   > **Note:** In SafeNet ProtectV Manager clustering, logs of only those ProtectV Manager instances will be redirected to the Syslog server where the `pvmctl configsyslog` command is run. To redirect logs of all cluster nodes to the Syslog server, run the `pvmctl configsyslog` command on all nodes on the cluster.

   Here,

   - `SERVERIP` – IP address or hostname of the Syslog server.
   - `"SERVERPROTOCOL"` – Protocol used for communication with the ProtectV Manager instance. When using `tls`, set `--serverprotocol="tls"`.
   - `SERVERPORT` – Port of the Syslog server. The default port for `tls` is `6514`. This port must be added to the security group of ProtectV Manager.
   - `SERVERCACERT` – *The CA certificate is mandatory for the `tls` protocol.* Full path of the Syslog server's CA certificate (`.crt` file) on the ProtectV Manager instance. For example, `/home/pvadmin/servercacert.crt`.
   - `"LOGTYPE"` – Type of logs to redirect to the Syslog server. Specify `"all"` to redirect audit and services logs. The default log type is `audit`. This means that only the audit logs will be redirected to the Syslog server, by default.

SSH Events

When ProtectV Manager is configured for Syslog server, logs of `SSH` events automatically start redirecting to the Syslog server. These events include login attempts to ProtectV Manager using `SSH`.

> **Note:** Logs of `SSH` events are *never* stored on ProtectV Manager. Also, login attempts from the SafeNet ProtectV Manager Console are not logged.

Sample `SSH` logs are:

```
Oct 4 18:46:47 10.164.12.210 sshd[19013]: Accepted password for pvadmin from 10.164.115.15 port 54792 ssh2
```

```
Oct 4 18:46:47 10.164.12.210 sshd[19013]: pam_unix(sshd:session): session opened for user pvadmin by (uid=0)
```

```
Oct 4 18:47:27 10.164.12.210 sshd[19013]: pam_unix(sshd:session): session closed
for user pvadmin
```

11
SNMP Traps

SNMP agents alert the SNMP Manager of specific events taking place on managed objects using unsolicited SNMP messages.

> **Note:** Before you can use SNMP traps with SafeNet KeySecure, the SNMP Manager must be installed and configured.

Traps for SafeNet KeySecure

The following table lists traps implemented for SafeNet KeySecure:

Trap	Description
`keySecCreateKeyTrap`	Returns the following alert if a key cannot be created on SafeNet KeySecure. `Failed to create a new key using key service`
`keySecGetKeyTrap`	Returns the following alert if a key cannot be retrieved from SafeNet KeySecure. `Unable to get key from keyservice`

APPENDIX A
Utilities

This appendix describes the following utilities included in SafeNet ProtectV:

pvmctl

Use the `pvmctl` command to configure ProtectV Manager with ProtectV Gateway and ProtectV PostgreSQL database. This command also allows configuration of ProtectV Gateway with SafeNet KeySecure. Additionally, this command helps you configure web proxy and client authentication from cloud (for AWS). Moreover, the command provides option to back up and restore the PostgreSQL database. This command also provides options to configure ProtectV Manager clustering.

The following table lists `pvmctl` command options:

This command…	Does this...

`pvmctl --help`
OR
`pvmctl help`
	Provides basic help about `pvmctl` and its options.

`pvmctl --help-long`	Provides full help about `pvmctl` including usage, arguments, and description.

`pvmctl help <command>`
OR
`pvmctl <command> --help`
	Provides help about a `<command>`.
	Here, `<command>` could be: `gwstart`, `gwconfigproxy`, `backupdb`, `restoredb`, or `gwenroll`, etc.

`pvmctl version`	Shows the version of ProtectV Manager.
`pvmctl cluster create --pass="PASS" --hostip=HOSTIP --pubip`	Creates the current ProtectV Manager node as the first node (source node) of the cluster. Refer to "Creating a Cluster" on page 79 for details.
`pvmctl cluster test --testpvmip=TESTPVMIP`	Tests a node's connectivity with the source node of the ProtectV Manager cluster. Refer to "Adding ProtectV Manager Nodes to the Cluster" on page 81 for details.
`pvmctl cluster add --pass="PASS" --hostip=HOSTIP --sourcepvmip=SOURCEPVMIP --pubip`	Adds the current ProtectV Manager node to the existing cluster. Refer to "Adding ProtectV Manager Nodes to the Cluster" on page 81 for details.

This command…	Does this...
`pvmctl cluster list`	Lists the ProtectV Manager nodes in the cluster. Refer to "Viewing Nodes of a Cluster" on page 82 for details.
`pvmctl cluster deregister --otherpvmip=OTHERPVMIP`	Deregisters a ProtectV Manager node from the cluster membership. This command is not needed on the last node of cluster. Refer to "Deregistering Nodes from a Cluster" on page 82 for details.
`pvmctl cluster removeself`	Clears the cluster state from current deregistered ProtectV Manager node. Before clearing the cluster state, `deregister` should be run on some other ProtectV Manager node. However, to clear the cluster state of the last node, run `removeself --force`. Refer to "Clearing Cluster State from the Current Node" on page 82 for details.
`pvmctl cluster status`	Confirms whether a cluster or a member node is ready. Refer to "Creating a Cluster" on page 79 and "Adding ProtectV Manager Nodes to the Cluster" on page 81 for details.
`pvmctl networkpvm show`	Shows the existing network configuration. Refer to "Assigning IP Addresses to ProtectV Manager on Hyper-V and VMware" on page 50 for details.
`pvmctl networkpvm static --interface=INTERFACE --ipaddr=IPADDR --nwmask=NWMASK --gateway=GATEWAY --defaultgw=DEFAULTGW --dns=DNS1 --dns=DNS2`	Configures the network for static IP settings. Refer to "Assigning IP Addresses to ProtectV Manager on Hyper-V and VMware" on page 50 for details.
`pvmctl networkpvm dhcp --interface=INTERFACE`	Configures the network for DHCP IP settings. Refer to "Assigning IP Addresses to ProtectV Manager on Hyper-V and VMware" on page 50 for details.
`pvmctl networkpvm clear --interface=INTERFACE`	Clears the existing configurations from the specified network interface. Refer to "Assigning IP Addresses to ProtectV Manager on Hyper-V and VMware" on page 50 for details.
`pvmctl networkpvm start`	Applies the modified static network interface configurations and starts the network service. Refer to "Assigning IP Addresses to ProtectV Manager on Hyper-V and VMware" on page 50 for details.
`pvmctl configsyslog --serverip=SERVERIP --serverport=SERVERPORT --serverprotocol="SERVERPROTOCOL" --servercacert=SERVERCACERT --logtype="LOGTYPE"`	Configures ProtectV Manager to redirect logs to the Syslog server. Refer to "Redirecting Logs to Syslog Server" on page 115 for details.

This command…	Does this...
`pvmctl encryptpvm status`	Reports whether the ProtectV Manager disk is encrypted. Refer to "Preparing for Disk Encryption" for details.
`pvmctl encryptpvm prepare --sparedisk=SPAREDISK`	Prepares ProtectV Manager to encrypt the root disk on next reboot. The command requires a spare disk (for example, xvdb, xvdc, or xvdf) of same or greater size to be attached before run. An encrypted ProtectV Manager waits for login from `pboot` user every time it boots. Refer to "Preparing for Disk Encryption" for details.
`pvmctl encryptpvm updateprebootauthkeys`	Updates the preboot environment with `ssh` authorized key file in your home directory. Next reboot onward, the PreBoot Shell will allow login from these keys. Run this command only if the disk is already encrypted. Refer to "When the Authorized SSH Key is Changed" for details.
`pvmctl encryptpvm updateprebootuserpass --prebootpass="PREBOOTPASS"`	Changes the password of the preboot user. Refer to "Changing the preboot Password" for details.
`pvmctl encryptpvm updatediskpass`	Changes the password for ProtectV Manager's disk encryption. Refer to "Changing the Disk Encryption Password" on page 60.
`pvmctl startpvm --prikeypass="PRIKEYPASS"`	Starts the ProtectV Manager service. Refer to "Starting the SafeNet ProtectV Manager Service" for details.
`pvmctl resetpvmkeypassword`	Changes the private key password. Refer to "Changing the Private Key Password" on page 67.
`pvmctl status`	Shows the status of ProtectV components. If something goes wrong, this command may be helpful in identifying the issue.
`pvmctl stoppvm`	Stops all ProtectV Manager services.
`pvmctl backupdb`	Backs up the ProtectV Manager database. Saves the backup locally. Refer to "Backing up the PostgreSQL Database" for details.
`pvmctl restoredb --dbpath=DBPATH --encpass="ENCPASS"`	Restores manual or scheduled backup of the SafeNet ProtectV database. Refer to "Restoring Database Backups" for details.
`pvmctl updatedbpass --oldpass="OLDPASS" --newpass="NEWPASS"`	Updates password for the ProtectV Manager database. Refer to "Changing Password of the ProtectV Manager Database" on page 66 for details.
`pvmctl autodbbackup uploadsettings show`	Displays the scheduled backup upload settings. Refer to "Scheduling the ProtectV Manager Backup" for details.
`pvmctl autodbbackup uploadsettings update --protocol=PROTOCOL --`	Sets/updates the scheduled backup upload settings. Refer to "Scheduling the ProtectV Manager Backup" for details.

This command…	Does this...
`host=HOST --username=USERNAME --encpass="ENCPASS" [--keyfile=KEYFILE|--password="PASSWORD"] --destinationdir=DESTINATIONDIR`	
`pvmctl autodbbackup schedulesettings show`	Displays the automatic backup schedule. Refer to "Scheduling the ProtectV Manager Backup" for details.
`pvmctl autodbbackup schedulesettings update --period="daily" --day-of-month=1 --day-of-week="sat" --hour=0 --minute=0`	Sets/updates the automatic backup schedule. Refer to "Scheduling the ProtectV Manager Backup" for details.
`pvmctl gwstart --pvmip=PVMIP --prikeypass="PRIKEYPASS"`	Configures ProtectV Gateway with ProtectV Manager. Rerun the `pvmctl gwstart` command every time the IP address of ProtectV Manager changes. Refer to "Configuring SafeNet ProtectV Gateway Instance" for details.
`pvmctl gwenroll --enrollmenttoken=ENROLLMENTTOKEN`	Enrolls ProtectV Gateway with ProtectV Manager. It requires an enrollment token, which can be generated on the ProtectV Manager Console. Refer to "Configuring SafeNet ProtectV Gateway Instance" for details.
`pvmctl gwstatus`	Checks whether ProtectV Gateway is running. Refer to "Configuring SafeNet ProtectV Gateway Instance" for details.
`pvmctl gwconfigproxy set --proxyip=PROXYIP --proxyport=PROXYPORT --proxyusername=PROXYUSERNAME --proxypass="PROXYPASS"`	*(This command is optional and for AWS only.)* Skip this step if client authentication from cloud needs to be disabled. Set up Gateway to use your proxy server for AWS calls. It checks for connectivity to https://aws.amazon.com. Refer to "Setting SafeNet ProtectV Gateway for AWS Calls" for details.
`pvmctl gwconfigproxy status`	*(This command is optional and for AWS only.)* Checks the proxy status and, if configured, gets proxy settings for AWS calls. Refer to "Checking Proxy Settings" for details.
`pvmctl gwconfigproxy unset`	*(This command is optional and for AWS only.)* Unsets the proxy server for AWS calls. The `pvmctl gwconfigproxy unset` command unsets the proxy regardless of accessibility to https://aws.amazon.com from ProtectV Gateway. Refer to "Unsetting SafeNet ProtectV Gateway for AWS Calls" for details.
`pvmctl createcsr --ksclientcsr=KSCLIENTCSR --ksclientcn=KSCLIENTCN --passphrase="PASSPHRASE"`	Create a client Certificate Signing Request (CSR.) Refer to "Configuring SafeNet ProtectV Manager with SafeNet KeySecure" for details.

This command…	Does this...
`pvmctl configks --ksip=KSIP --ksport=KSPORT --ksuser=KSUSER --kscacert=KSCACERT --kspass="KSPASS" --ksclientcert=KSCLIENTCERT --ksclientkey=KSCLIENTKEY --passphrase=PASSPHRASE`	Configures ProtectV Manager with SafeNet KeySecure. It enables ProtectV Manager to distribute keys. Refer to "Configuring SafeNet ProtectV Manager using Client Certificates Created through pvmctl" and "Configuring SafeNet ProtectV Manager using Imported Client Certificates" on page 61 for details.
`pvmctl gwconfigcloudauth status [<instanceID>] [<instanceRegion>]`	*(This command is optional and for AWS only.)* Checks configuration for client authentication from cloud. Provide the Instance ID and region of a client instance to check whether the configuration to authenticate a client from cloud is correct. Checks connectivity with a client instance. Refer to "Checking Connectivity with a Client Instance" for details.
`pvmctl gwconfigcloudauth disable`	*(This command is optional and for AWS only.)* Disables client authentication from cloud; it is enabled by default. This feature works only if AWS EC2 endpoints are accessible from ProtectV Gateway. Refer to "Disabling Client Authentication from Cloud" for details.
`pvmctl gwconfigcloudauth enable --cloud=<cloudname>`	*(This command is optional and for AWS only.)* Enables client authentication from cloud, if it is disabled. **Note:** Client authentication from cloud is supported for Amazon AWS only. Refer to "Enabling Client Authentication from Cloud" for details.

pvinfo

After SafeNet ProtectV Client image is installed and the instance is rebooted, it takes some time for each partition to encrypt.

To check the encryption status:

1. SSH to the Linux instance.
2. Run the following command:

   `sudo pvinfo`

   For example:

```
root@ip-10-232-99-203:~# sudo pvinfo
SafeNet ProtectV Linux <version>
Device    Mount         Size   Protected            fs     ca    System
xvdh      /data   1073741824         yes   crypto_LUKS   True    False
xvdi       swap   1073741824         yes   crypto_LUKS   True    False
```

```
xvda1          /    8589934592          no          ext4    True      True
```

The output indicates that all partitions **except the root** (`/`) **partition** are protected.

Local SafeNet ProtectV Management Console

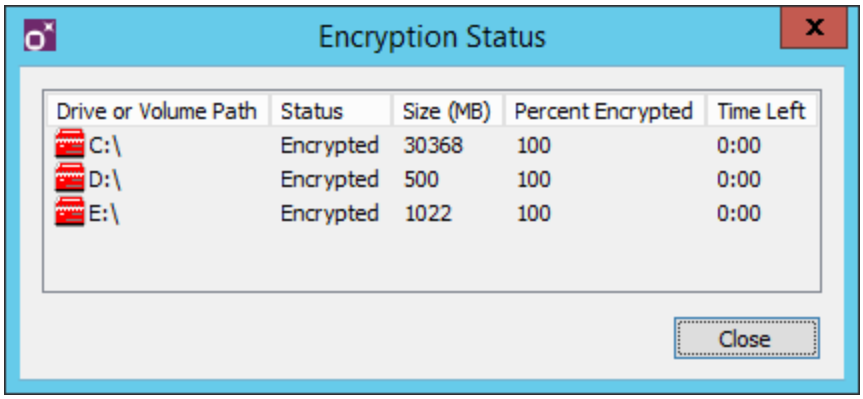
After the ProtectV Client Image is installed and the `registration.json` file is created on Windows instances, volume encryption starts. It takes some time for each partition to encrypt. Use the Local ProtectV Management Console utility to check the encryption status of partitions on Windows instances.

To check the encryption status:

1. Remote desktop to the client instance.
2. Navigate to `C:\Program Files\SafeNet ProtectV`.
3. Double-click **LocalMC.exe**. The **Encryption Status** dialog box is displayed.

The **Encryption Status** dialog box shows the percent encrypted for each drive/partition. At the start, the status of a drive is **Encrypting** and the drive icon is **half red**.

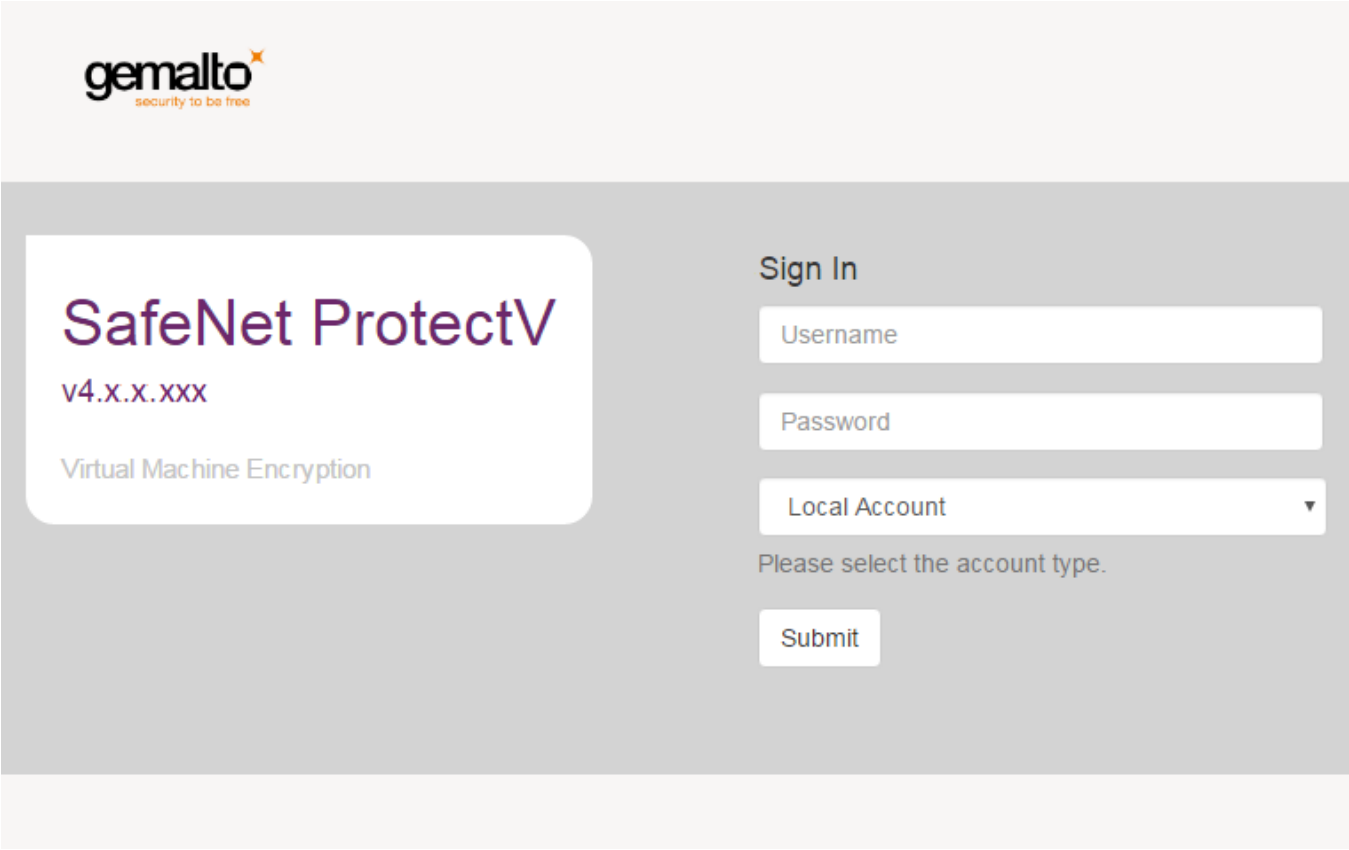
After the encryption is complete, the status becomes **Encrypted** and the drive icon changes to **red**, as shown below.



APPENDIX B
SafeNet ProtectV Manager Console

Overview

After ProtectV Manager is configured, access it from an Internet browser using its IP address/hostname. The home page is shown below.



As ProtectV administrator, log on to the SafeNet ProtectV Manager Console. Then, you can configure ProtectV Manager for AD users on the Settings tab, as described in the "Configuring SafeNet ProtectV Manager for Active Directory" chapter. You can also create ProtectV users on the Users tab, as described in the "Managing Users" chapter. The Settings and Users tabs are available only to ProtectV administrators.

After your ProtectV or AD accounts are added, you can log on to the ProtectV Manager Console. Refer to the "Logging on as SafeNet ProtectV User" or "Logging on using AD Account" section depending on your type. Contact your SafeNet ProtectV administrator or System Administrator for login credentials. After logging on, you can change your password, as described in the "Changing Your Password" section.

Logging on as SafeNet ProtectV User

Log on to the ProtectV Manager Console to perform your activities.

To log on as a ProtectV user:

1. Open the Internet browser.
2. Enter ProtectV Manager's IP address/hostname in the address bar.
3. Press **Enter**. The **SafeNet ProtectV Manager Console** is displayed.
4. Under **Sign In**, enter **Username** and **Password**. Contact your ProtectV administrator for login credentials.
5. Ensure that **Local Account** is selected at the account type.
6. Click **Submit**. On first successful log on, the **Images** tab is displayed.

It is recommended to change the password at first log on. However, you may change the password any time, as described in the "Changing Your Password" section.

Refer to "SafeNet ProtectV Manager Interface" on the next page for description of various tabs on the ProtectV Manager Console.

Logging on using AD Account

Log on to the ProtectV Manager using your AD account to perform your activities.

To log on using your AD account:

1. Open the Internet browser.
2. Enter ProtectV Manager's IP address/hostname in the address bar.
3. Press **Enter**. The **SafeNet ProtectV Manager Console** is displayed.
4. Under **Sign In**, enter **Username** and **Password**.
5. Select **AD Account** as the account type. Here, **AD Account** represents the **Connection Name** specified when "Configuring SafeNet ProtectV Manager for AD."
6. Click **Submit**.

Refer to "SafeNet ProtectV Manager Interface" on the next page for detailed description of various tabs on the SafeNet ProtectV Manager Console.

Note: As soon as an AD user logs on to ProtectV Manager for the first time, it appears under the **Users** tab (visible to ProtectV administrators.) A tick mark appears under the **AD User** column indicating that the user is an AD user.

Changing Your Password

It is a good practice to change your password frequently. You can change the password any time on the ProtectV Manager Console. The ProtectV administrator can also change password on behalf of other users. Refer to "Changing Password of Other Users" for details.

To change your password:

1. Log on to the ProtectV Manager Console.

2. Click the display name link in the top right corner. The **<Username>** page is displayed.
3. Enter new password in the **New Password** and **Confirm Password** fields. Adhere to the password creation rules mentioned on the page.
4. Enter new password in the **New Password** and **Confirm Password** fields. Adhere to the password creation rules mentioned on the page.

> **Note:** AD users cannot change their password. For them, the **New Password** and **Confirm Password** fields are unavailable.

5. Click **Update User Details**. A message appears stating that the changes are applied successfully.

SafeNet ProtectV Manager Interface

The tabs available on the SafeNet ProtectV Manager Console are:

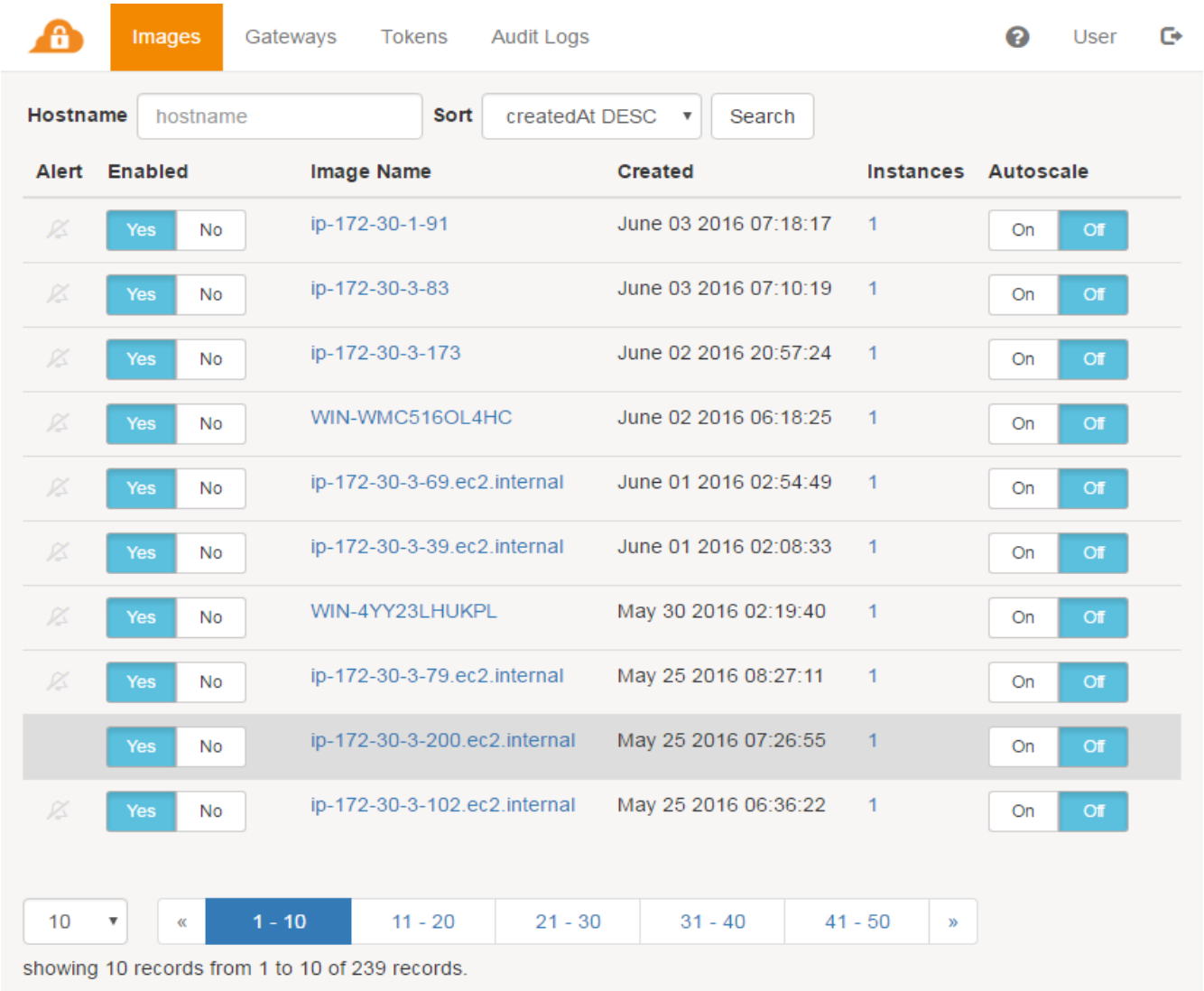
Tab	Description
Images	Displays the list of registered ProtectV Client images. On successful log on, the Images tab is displayed. By default, no image is registered.
Gateways	Displays the list of registered ProtectV Gateways. By default, no gateway is registered.
Tokens	Allows you to create tokens to enroll ProtectV Gateways and ProtectV Client images with ProtectV Manager. The generated enrollment tokens are listed under this tab. By default, no tokens are displayed. Additionally, you can create the CA certificate on this tab.
Audit Logs	Displays the audit information. You can specify search criteria to retrieve specific information.
Users	(Available only to ProtectV administrators) Displays the list of available ProtectV users. The ProtectV administrators can create, modify, and delete ProtectV users on this tab.
Settings	(Available only to ProtectV administrators) Allows configuring ProtectV Manager for AD authentication. Administrators can also update configuration to use modified AD settings. When not required, they can delete the AD authentication settings. The rekey feature can also be enabled and configured on this tab.

The ProtectV Manager Console also contains the following items:

Icon/Link	Description
	Takes to the home page.
	Click to access the online help.
<Display Name>	**Display Name** of the logged on user. For initial administrator, the display name is **Admin**.
	Click to log out. This button is in the top right corner of the window.

Images

The **Images** tab displays the list of registered SafeNet ProtectV Client images. By default, no image is registered. The tab also displays the encryption status of client instances.



The tab displays the following items:

- **Hostname** – Text field to search for ProtectV Client images by hostnames.
- **Sort** – Drop-down list to help arrange ProtectV Client images in ascending or descending order of their creation time.
- **Search** – Returns the search results.
- **Refresh** ( ) – Refreshes the list of ProtectV Client images.
- **Turn on autoscaling for new images** – (Visible only to ProtectV administrators.) Check box to turn autoscaling on/off for the new ProtectV Client images that are registered subsequently. Select the check box to turn global autoscaling on, clear it to turn global autoscaling off.

- **Alert** – Alerts that the disk associated with the image/instance will not be granted a key unless both the instance and the parent image are authorized/enabled.
- **Enabled** – Displays whether an image is authorized for key. If **Yes**, then only partitions on instances made from the image will be encrypted.
- **Image Name** – Name of the ProtectV Client image. Click to view more details about the image.
- **Created** – Time of the image creation.
- **Instances** – Number of running instances of the image.
- **Autoscale** – Displays whether new clones of the associated image will be granted keys. By default, it is turned **Off**, that is, the new clones will not be granted keys. To turn autoscaling on for new clones of the image, click **On**; encryption keys will be granted to new clones.

> **Note:** It is recommended to turn **Autoscale** on for an image before creating its clones. If **Autoscale** is turned on *after* creating new clones, keys will not be granted to them.

- **Delete** ( ) – (Visible only to ProtectV administrators.) Deletes the image.
- **Drop-down** (10) – Allows displaying specific number of images. Default is **10** records.

Viewing Details of an Image

On the SafeNet ProtectV Manager Console, you can view instances that are based on a particular client image. Further, you can view the details of partitions, such as encryption status, name, and size, of instances.

To view the details of an image:

1. Click an image under the **Image Name** column. The following details are shown:
   - **Alert** – Alerts that the disk associated with the image/instance will not be granted a key unless both the instance and the parent image are authorized/enabled. Click to view the cloned image. You may allow making the clone accessible. The cloned image is not accessible until it is allowed.
   - **Authorized** – Displays whether the cloned instance is authorized for encryption key. If **Yes**, then only the instance will be granted encryption keys. The instance will be up only after receiving the encryption key.
   - **Encryption** – Allows decrypting the client instance. It also allows you to encrypt the client instance that you decrypted manually. For the encrypted client instance, **Yes** is selected; for the decrypted client instance, **No** is selected.
   - **IP** – IP address assigned to the client instance.
   - **Type** – Type of the client instance. **Windows** or **Linux**.
   - **Instance Name** – Name of the instance.
   - **Client Version** – Shows the version of the SafeNet ProtectV Client installed on the instance.
   - **Last Connected** – When the instance was connected last time.
2. Under Instances, click to expand details of the instance. The following partition details are shown:
   - **Status** – Locked icon ( ) under status indicates that the partition is encrypted. An unlocked icon indicates that the partition is not yet encrypted.
   - **Name** – Shows the volume name.

- **Encryption** – Allows decrypting/encrypting the volume. It also allows you to encrypt the volume that you decrypted manually. For the encrypted volume, **Yes** is selected; for the decrypted volume, **No** is selected.
- **Friendly Name** – Shows the friendly name for the partition.
- **Size** – Shows the volume size.
- **Key Name** – Shows the name of the key used for encryption.
- **Last Rekeyed** – Shows the date and time when the encryption key was changed.

Attaching/Detaching Partitions

Encrypted partitions can be detached from one client instance and attached to another instance encrypted with SafeNet ProtectV. However, the encryption key will not be automatically available to this partition. The SafeNet ProtectV Manager Console provides option to allow or refuse the encryption key to the partition.

Note: To encrypt a newly attached non-encrypted partition to a client instance protected with SafeNet ProtectV:
1. Format the partition. It creates file system on the partition. As soon as the new partition is formatted, it becomes visible on the SafeNet ProtectV Manager Console. The partition will remain unencrypted until the client instance is rebooted.
2. Reboot the client instance to encrypt the partition.

Note: Do not move encrypted system partitions or boot volumes (for example, C:\ drive) from one instance to another.

To allow the encryption key to the attached partition:

1. Sign in to the **ProtectV Manager Console**.
2. Click the **Images** tab.
3. Click an image under the **Image Name** column.
4. Click ⊞ to expand.
5. Click **Allow It!** to the right of the attached partition.

   The encryption key is allowed to the partition, and the button becomes **Refuse It!**

Note: Clicking the **Refuse It!** button next to a partition revokes the encryption key from the partition.

Decrypting Client Instances

On the SafeNet ProtectV Manager Console, you can decrypt either entire client instances or their specific partitions. By default, all partitions of client instances are designated for decryption. All partitions of the instance become plaintext after decryption. This section describes steps to decrypt entire client instances. Refer to "Decrypting/Encrypting Specific Partitions" on the next page for details on decrypting or encrypting specific partitions.

Note: After decryption, if ProtectV Manager goes down, the decrypted client instance would not come up after the next reboot. To manage the decrypted client instances from the ProtectV Manager Console, ensure that ProtectV Manager is up and running.

To decrypt all partitions of a client instance:

1. Sign in to the **ProtectV Manager Console**.
2. Click the **Images** tab.
3. Click an image under the **Image Name** column. The list of client instances based on the selected image appears.
4. Click **No** under the **Encryption** column corresponding to your client instance. The **No** button appears selected (Yes No .)

A message appears stating that decryption will happen on the next client reboot. Until the client instance is rebooted, the instance remains encrypted. After the client instance is rebooted, you can verify the successful decryption on the SafeNet ProtectV Manager Console.

Note: To again encrypt a decrypted client instance, click **Yes** under the **Encryption** column. The decrypted client instance will be encrypted with a new key.

After decryption, the client instance remains registered with ProtectV Manager. You can now uninstall the ProtectV Client from the client instance. Refer to "Uninstalling the ProtectV Client" on page 102 for steps to uninstall the ProtectV Client from Linux and "Uninstalling the ProtectV Client" on page 108 for steps to uninstall the ProtectV Client from Windows.

Clones of a Decrypted Client Instance

When a decrypted instance is cloned, SafeNet ProtectV encrypts the cloned instance during the first reboot. If needed, decrypt the cloned instance, as described in "Decrypting Client Instances" on the previous page.

Decrypting/Encrypting Specific Partitions

In addition to decrypting or encrypting entire instances, you can decrypt or encrypt specific partitions of client instances on the SafeNet ProtectV Manager Console.

Encryption of a Windows instance starts as soon as it is registered. By default, all partitions of the instance will be encrypted. After the first encryption, you can specify partitions for decryption. Similarly, you can specify which decrypted partitions to encrypt.

A Linux instance, on the other hand, requires reboot to initiate encryption. Before the instance is rebooted, you can specify which partitions to encrypt on the SafeNet ProtectV Manager Console.

To decrypt/encrypt a partition of a client instance:

1. Sign in to the **ProtectV Manager Console**.
2. Click the **Images** tab.
3. Click an image under the **Image Name** column. The list of client instances based on the selected image appears.
4. Expand your instance to view its partitions.
5. Under the **Encryption** column corresponding to the partition you want to decrypt/encrypt:
   - Click **No** to decrypt the partition. The **No** button appears selected (

Yes No .) The selected partition will be decrypted on the next client reboot. Until the client instance is rebooted, the partition remains encrypted. After the client instance is rebooted, you can verify the successful decryption on the SafeNet ProtectV Manager Console.

Note: To again encrypt a decrypted partition, click **Yes** under the **Encryption** column. The decrypted partition will be encrypted with a new key on next client reboot.

– Click **Yes** to encrypt the partition. The **Yes** button appears selected (Yes No .) The selected partition will be encrypted on the next client reboot. Until the client instance is rebooted, the partition remains decrypted. After the client instance is rebooted, you can verify the successful encryption on the SafeNet ProtectV Manager Console.

Note: To decrypt an encrypted partition, click **No** under the **Encrypted** column. The encrypted partition will be decrypted on next client reboot.

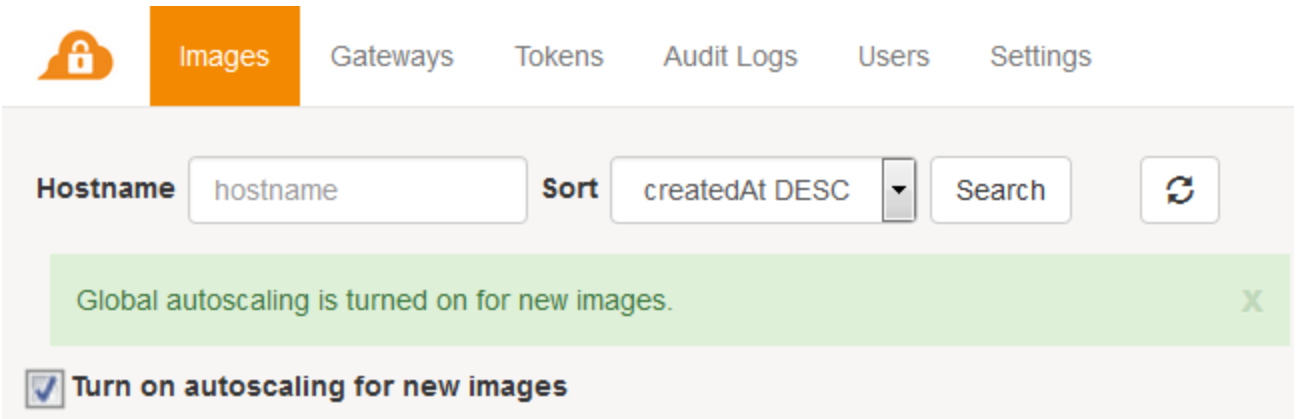
Turning Global Autoscaling On

On the SafeNet ProtectV Manager Console, a ProtectV user can turn autoscaling on for individual ProtectV Client images. A ProtectV administrator can turn autoscaling on for *individual* ProtectV Client images or for *all* ProtectV Client images that are registered subsequently.

Note:
– Global autoscaling feature does not persist over SafeNet ProtectV Manager upgrades. If the SafeNet ProtectV database is restored from previous SafeNet ProtectV versions, you need to *again* turn on global autoscaling manually, as described above.
– In case of ProtectV Manager clusters, turn on global autoscaling on *all* cluster members individually.

To turn global autoscaling on for client instances:

1. Sign in to the **ProtectV Manager Console**.
2. Click the **Images** tab.
3. Select the **Turn on autoscaling for new images** check box, as shown below. This check box is visible to ProtectV administrators.



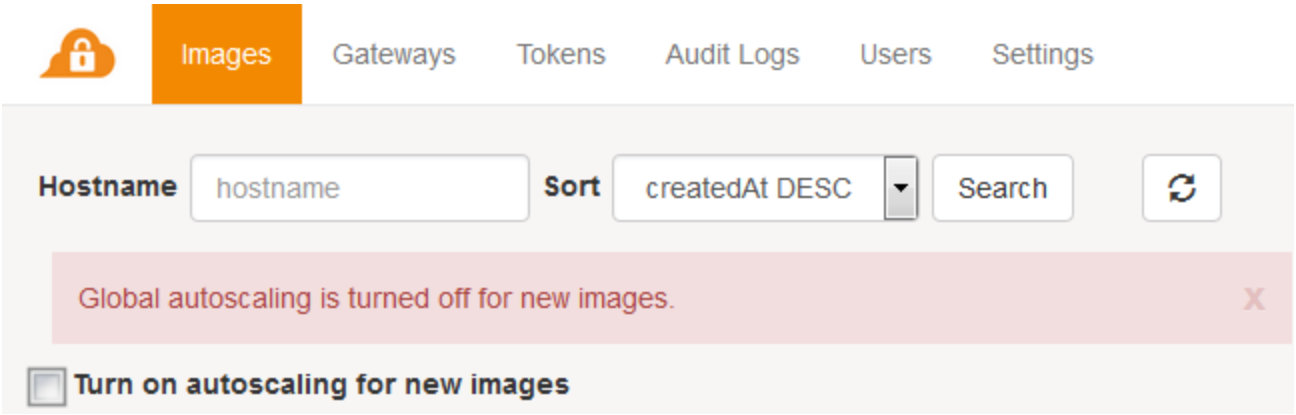
A message appears stating that global autoscaling is turned on for new images. Autoscaling is turned on for all ProtectV Client images that will be registered with SafeNet ProtectV Manager now onward.

Turning Global Autoscaling Off

On the SafeNet ProtectV Manager Console, a ProtectV user can turn autoscaling off for individual ProtectV Client images. A ProtectV administrator can turn autoscaling off for *individual* ProtectV Client images or for *all* ProtectV Client images that are registered subsequently.

To turn global autoscaling off for client instances:

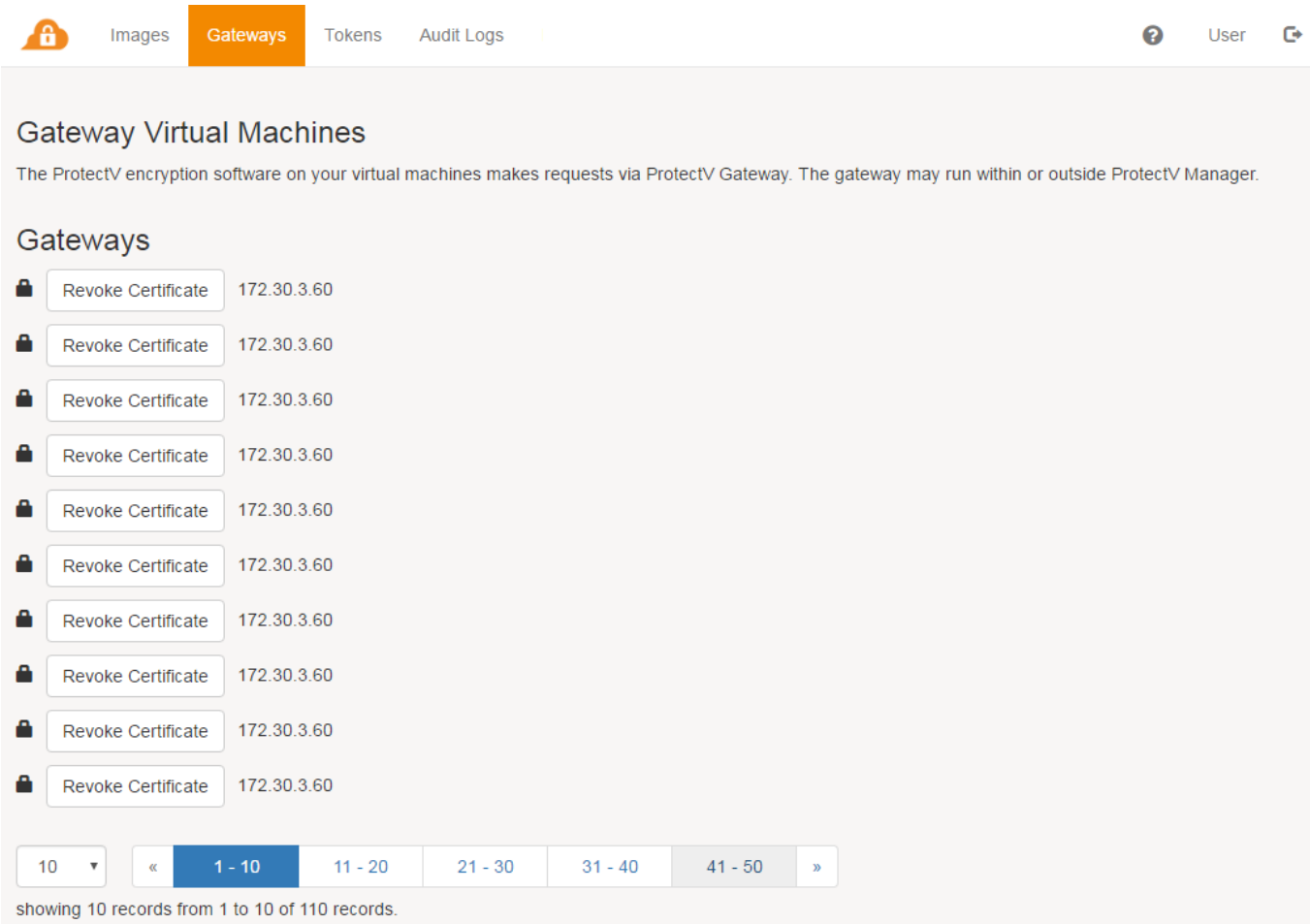
1. Sign in to the **ProtectV Manager Console**.
2. Click the **Images** tab.
3. Clear the **Turn on autoscaling for new images** check box, as shown below. This check box is visible to ProtectV administrators.



A message appears stating that global autoscaling is turned off for new images. Autoscaling is turned off for all ProtectV Client images that will be registered with SafeNet ProtectV Manager now onward.

Gateways

The **Gateways** tab displays the list of registered ProtectV Gateways. By default, no Gateway is registered. For each registered Gateway instance, a **Revoke Certificate** button is displayed with the instance's IP address.

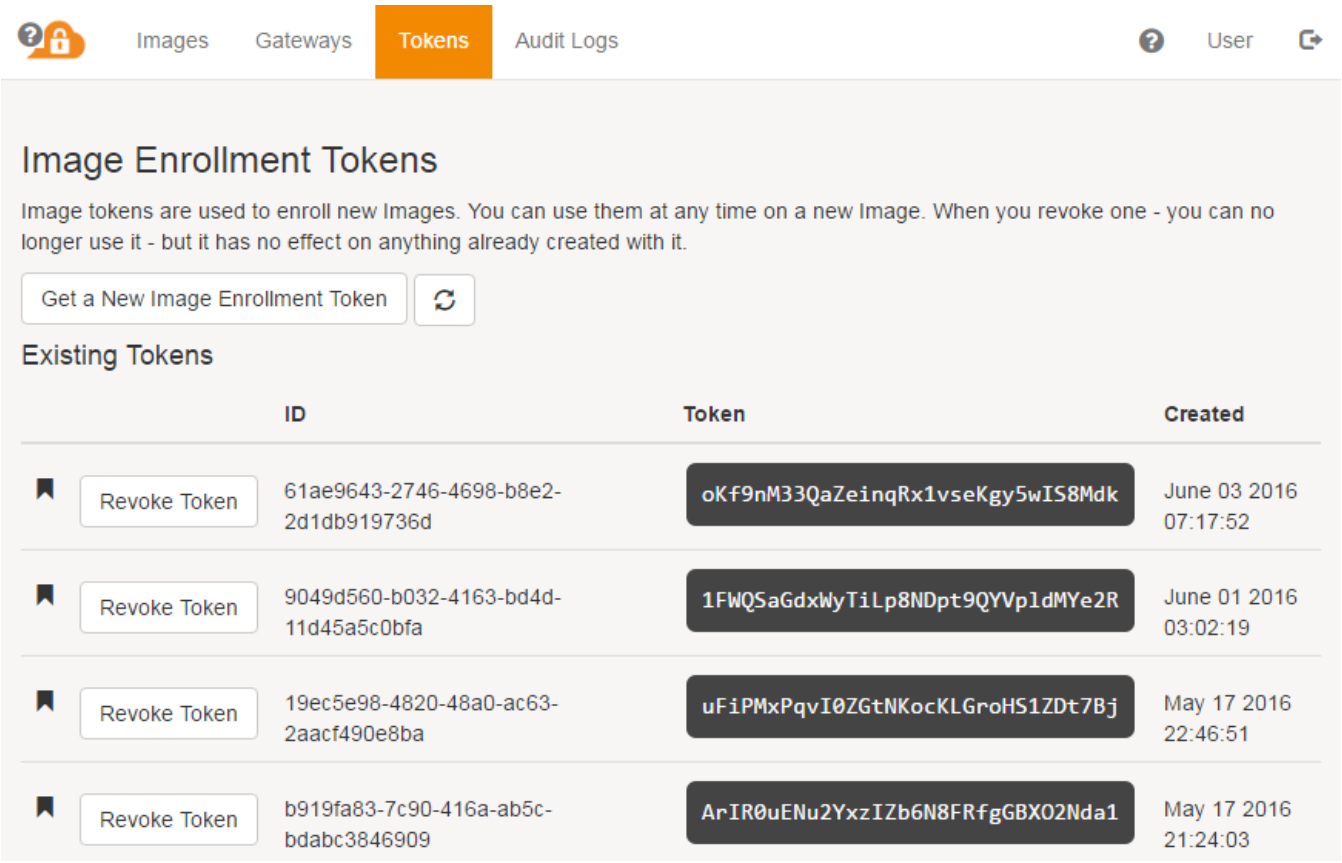


To revoke the certificate from a Gateway instance, click the **Revoke Certificate** button to the left of it.

Tokens

The **Tokens** tab allows you to create tokens to enroll ProtectV Gateways and ProtectV Client images with ProtectV Manager. The generated enrollment tokens are listed under this tab. By default, no tokens are displayed.

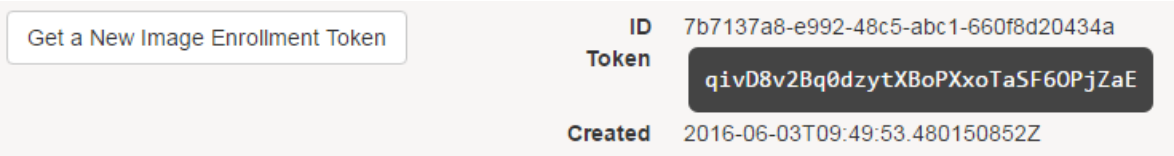
You can also export the CA certificate on the **Tokens** tab.



The **Tokens** tab is divided into the **Image Enrollment Tokens**, **Gateway Enrollment Tokens**, and **CA Certificate** sections. Use the **Refresh** ( ) button to refresh the displayed enrollment tokens.

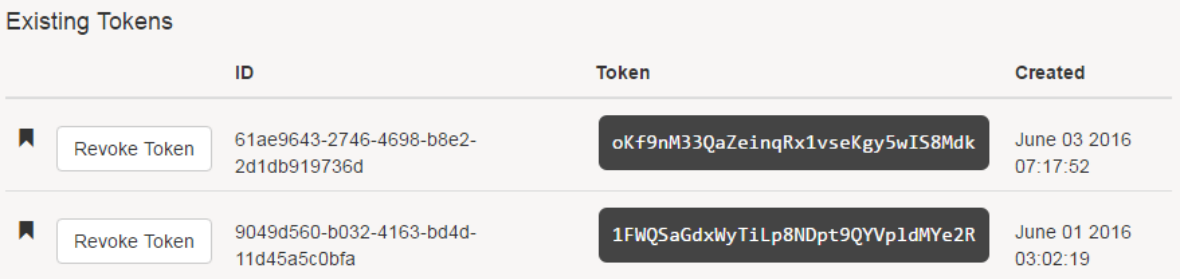
Image Enrollment Tokens Section

- Provides the **Get a New Image Enrollment Token** button. Click to generate a new image enrollment token. Every token has **ID**, **Token**, and **Created** details.



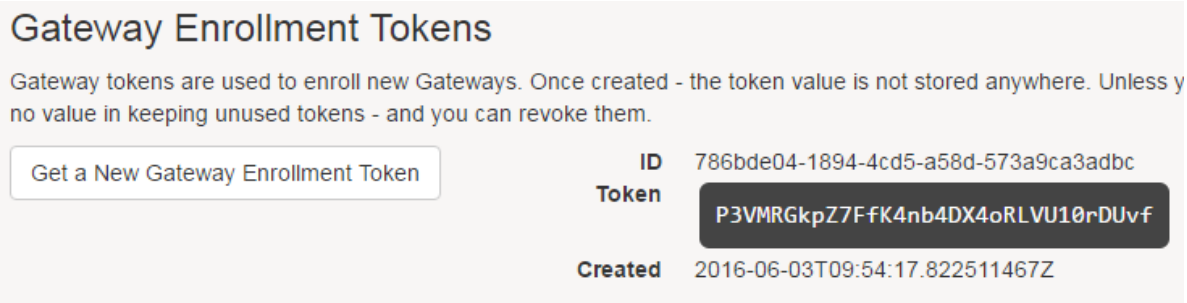
  An Image Enrollment Token is required when deploying SafeNet ProtectV on client instances. It is needed for registering the client with SafeNet ProtectV. Refer to "Deploying SafeNet ProtectV on Linux" on page 94 and "Deploying SafeNet ProtectV on Windows" on page 103 for details.

- Displays the generated tokens. Multiple image enrollment tokens can be generated. The **Revoke Token** button is displayed for the in-use token.



Gateway Enrollment Tokens Section

- Provides the **Get a New Gateway Enrollment Token** button. Click to generate a new gateway enrollment token. Every token has **ID**, **Token**, and **Created** details.

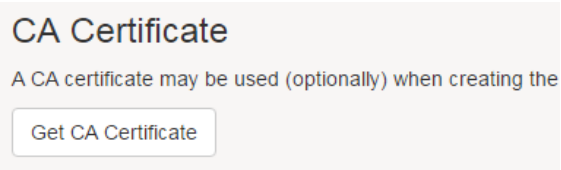


  A Gateway Enrollment Token is required when "Configuring SafeNet ProtectV Gateway Instance" on page 85.

- Displays only one enrollment token. If left unused, it becomes unavailable and appears under the **Unused Gateway Enrollment Tokens** section. Create a new token every time you enroll a Gateway.

CA Certificate Section

- Provides the **Get CA Certificate** button. Click to export a CA certificate. The CA certificate begins with the header (`-----BEGIN CERTIFICATE-----`) and ends with the footer (`-----END CERTIFICATE-----`).



  A CA certificate is needed when creating the `registration.json` file on your client instances. (A CA Certificate is optional when creating `registration.json`.) Refer to "Deploying SafeNet ProtectV on Linux" on page 94 and "Deploying SafeNet ProtectV on Windows" on page 103 for details.

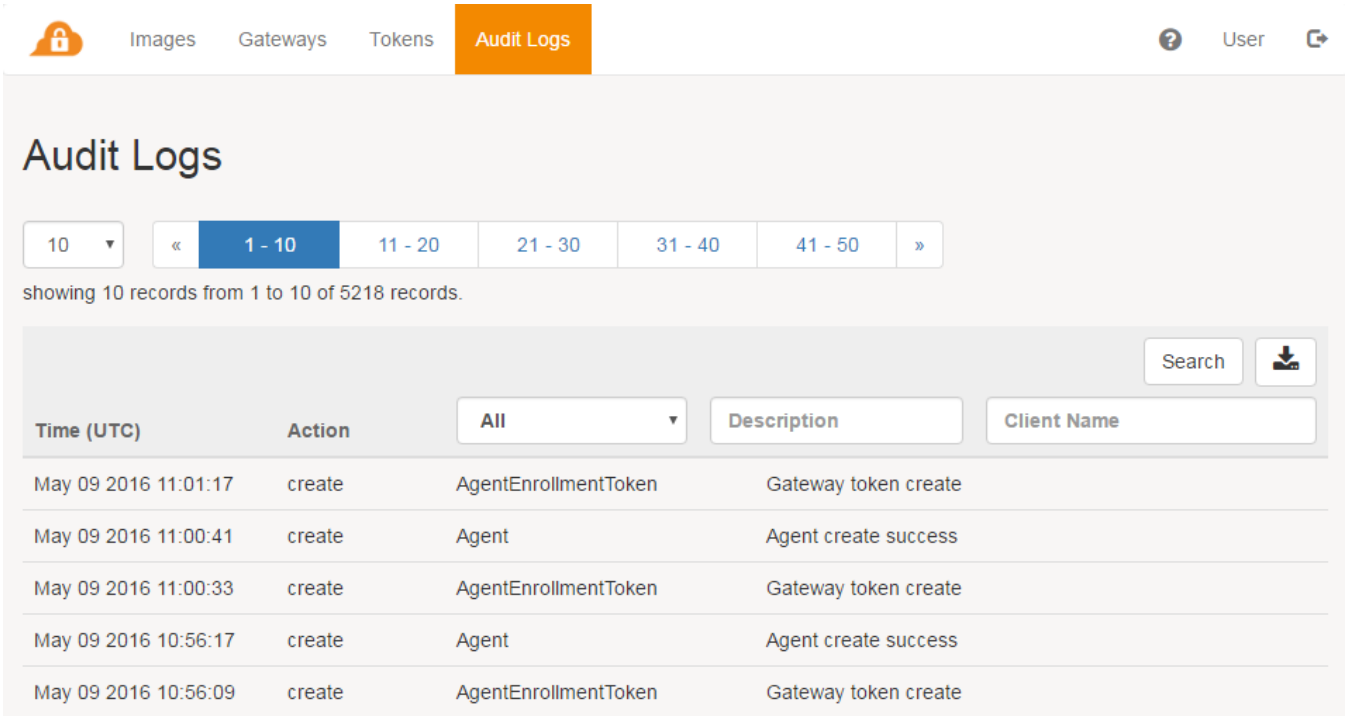
- Displays the content of the CA certificate.

```
-----BEGIN CERTIFICATE-----
MIIFETCCAvmgAwIBAgIVAPEE7eXCzZ7SsoSvtAZR04l02aKcMA0GCSqGSIb3DQEB
CwUAMCAxCzAJBgNVBAYTAlVTMREwDwYDVQQKEwhQcm90ZWN0VjAeFw0xNjAzMTYw
ODQ1MzlaFw0yMTA4MjEwODQ1MzlaMCAxCzAJBgNVBAYTAlVTMREwDwYDVQQKEwhQ
cm90ZWN0VjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAMT3P8a7pjf5
XiObQ9JJwu8jdCHgDcLbxSA6bz5JT+yR/YQ/jT8tXUeNMCoCboCSEhQy1Wn0adOC
kQoXtCtW7k5El7zlcJAyfiho6PYvnsVnpTEzGUgiCpTDZAHUR6GVr+kxhPWfqcGO
H3KNrwoyzgHqgjlVFBtAPCr3b8m155VpnAh4q/U5wJC1LGVMzqwp5DE1F+fAf2o1
NudtJOJ+x1awlx9E+bwsyAwJHlBACLouFBDd7iLld80H7n2AH95D5P/zt7mp89qT
u2dV52Ww0CuKWov1FeybhO82iZTAreg5x+a8Iub9HgbHbcMyUhxmsBMyrOsVK+/9
LbIKf06AECiqAjJJWBq0Q8csLopBIsDd4hpr/O+5OuvWjKmj7XudAOlfBJyfHx0Z
O0iC9tbRLc3U/jQ+cuR/E8KHWcj2R7Dh5G+WyGMdsx/xCCsmlvYGTxVcjem/i0vQ
qUpKm0qOWDP1oRKUKwz0Md3w3WcmFSgYGggoDuizEjIqQsYNw3zjVsw+8jmSKAu6
XUMFd+YesheynyJUc/a3qlNtJ54aaM3oyATRADlv+r+LWphkyAR8m1JerjX8w6uq
ym3OlitVFlr2oGmU3IFoXWgy7yqMQgbYLJthvK7JBakoZqIQtqUaiVRFDx4VPgRj
DZENKmI68n8+X0elYqiV/x4cDAJL0Gl7AgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIC
hDAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwEwDwYDVR0TAQH/BAUwAwEB
/zANBgkqhkiG9w0BAQsFAAOCAgEANcEQ8IJU6fSUkNVGO9JA+Rdx+ljVBYH/8jWh
CoAhhfikeQPcN1hitxvozZt/uarQxD7KZ4k908Mj0hdZjeJUUIGNDdrQGkVpJ+tY
wMXw4UyYJDnU8t1GnvNrnaQpNZmUC/1Kou9QcHEOSkHYhw33anLC2Ph1nweCeEmW
uAqKhu1/ah04oF1xywCV4BDs37DoydG/6/sgIEIKf7OsTyOSTjtfetuN0klYJ0h+
GLxq/flnsoDTkk4p8CWAZBB7JtKu+Pbs5/Cctuw3UDu8Deu1CPvAuorCo4LcBvkv
fj4qCv01Pm5Y13cGV3dXe5S95zKQmMI9xPk5iqtDF2dwDN4FNPxG/A1fWnCjjqUS
UFPgSnvuIuYj36BPeNT4mTr7Ewd/uIGHMikJSXRR+fmcPI7ieWC1Ue/QCPeI5YOc
6+awQTs1nWw2tcle20wzLhlUmfqgB2gvgRpt2NFCrTdxhkltKxIdHTlDuDUMRybr
Kb0Yn3eQyiDcqwemfJDn9P14OeHG9nyJVI+UPaQ/1ZqJoqeGNbrTGzgKFzU2h6yU
nLz9Gqa/2VsPh8Os9x03lzEtvOXSaKxV4+3XuZy30iB6Y6eh56P8xjOnAb3jinMW
KRlN7iyzapORVYyu65+bjo2AWU0w/8TjrB3SXLctg1cf3UoVtnE9PNwNHSgNujnj
xOS3Q3c=
-----END CERTIFICATE-----
```


When copying the certificate, the copied text must include the header (`-----BEGIN CERTIFICATE-----`) and footer (`-----END CERTIFICATE-----`).

Audit Logs

The **Audit Logs** tab displays logs of operations (actions) on SafeNet ProtectV client instances. The logs display the time and name of actions, objects on which the action is performed, description of the action, and the name of client on which the action is performed. The logs are arranged in reverse chronological order – the latest at the top.



By default, **10** records are displayed. You can change the number of records to display on screen in the drop-down list. You can also use pagination to navigate records.

Time (UTC) displays the action time in the Coordinated Universal Time (UTC) format. **Action** displays the action performed on SafeNet ProtectV client instances. Click the **Refresh** ( ) button to refresh the displayed logs.

Searching for Audit Logs

To search for audit logs:

1. From the drop-down list, select the search object. The available options are **Key**, **Client Enrollment Token**, **Client, Instance**, **Agent Enrollment Token**, and **Token**. **All** is the default option; audit logs related to all objects will be displayed.
2. Specify full or partial **Description** of the action. This filters logs based on the description.
3. Specify full or partial **Client Name**. This filters logs specific to the specified SafeNet ProtectV client.
4. Click **Search**. Audit logs meeting the search criteria are displayed.
5. Click the **Download CSV** ( ) button. The search results are downloaded in a CSV file.

Rotating Keys (Rekey)

Key rotation (also known as rekey) is the process of re-encrypting partitions with a new encryption key. The rekey feature is disabled by default.

As a ProtectV administrator, you can enable and configure the feature. When configuring the feature, specify the number of days (also known as the rekey interval) after which encryption keys should be changed automatically. By default, encryption keys are rotated after 180 days.

> **Note:** Key rotation re-encrypts only the encrypted partitions of registered client instances; the plaintext partitions are skipped.

This section covers the following information:

1. "Configuring the Rekey Feature" below
2. "Disabling the Rekey Feature" on the next page

Configuring the Rekey Feature

To configure the rekey feature:

1. Sign in to the **ProtectV Manager Console** as administrator.
2. Click the **Settings** tab.
3. Navigate to the **Rekey Configuration** section.
4. Click **On** to enable the feature. The **Rekey Configuration** screen is displayed.
5. In the **Rekey Interval (Days)** field, enter the number of days after which the encryption key should be changed. The default value is 180 days.
6. Click **Save**. A message is displayed stating that the rekey configuration is saved successfully.

The rekey feature is enabled and configured.

Disabling the Rekey Feature

To disable the rekey feature:

1. Sign in to the **ProtectV Manager Console** as administrator.
2. Click the **Settings** tab.
3. Navigate to the **Rekey Configuration** section.
4. Click **Off**. A message is displayed stating that the rekey configuration is saved successfully.

The rekey feature is disabled.

APPENDIX C
Resizing the System Disk of ProtectV Manager

Note: This appendix is applicable to ProtectV Manager instances launched on VMware vSphere.

The default size of a ProtectV Manager's file system (system disk) is 16 GB even if the disk is larger. If needed, you can resize the system disk to use the extended space and create the swap file system on an extended logical volume on VMware vSphere.

Resize the system disk before starting the ProtectV Manager VM or registering ProtectV clients with it. Therefore, resize the system disk immediately after launching the ProtectV Manager VM from the supplied OVA file.

Resizing the system disk of a ProtectV Manager VM involves configurations on the VMware vSphere Client and the ProtectV Manager VM console.

Resizing the Disk on VMware vSphere

To resize the system disk of a ProtectV Manager VM on VMware vSphere:

1. Log on to **vSphere Client**.
2. Deploy the ProtectV Manager's OVA file. Walk through the Deploy OVF Template wizard until the **Ready to Complete** screen. Refer to "Launching a ProtectV Manager VM Using the Windows Client" on page 46.
3. On the **Ready to Complete** screen, verify the deployment settings. If needed, navigate back and make required changes.

WARNING! Do not select the "Power on after deployment" check box.

4. Click **Finish**. Deployment starts and may take a few minutes to complete. After successful deployment, the ProtectV Manager VM appears under the inventory folder in the left pane.
5. In the left pane, right-click the VM, and select **Edit Settings...** The **<VM-Name> - Virtual Machine Properties** dialog box is displayed.
6. On the **Hardware** tab, click **Hard disk 1** in the left pane. The disk details are displayed on the right.
7. Under the **Disk Provisioning** section, change the **Provisioned Size** to the desired size.
8. Click **OK**. The VM is reconfigured to reflect the changes.
9. **Power On** the VM.

Resizing the Disk on the ProtectV Manager VM Console

After modifying the disk size on the VMware vSphere client, configure the ProtectV Manager VM for the changes to take effect. This involves the following tasks:

1. "Logging on to the ProtectV Manager VM as pvsuper" below
2. "Deleting the Partition Table" below
3. "Recreating the Partition Table with the Extended File System" below
4. "Creating Additional Partitions" on the next page
5. "Disabling the Swap Partition" on the next page
6. "Performing Online Resizing" on the next page
7. "Activating the New Swap Partition" on page 145
8. "Updating /etc/fstab with the UUID of New Swap" on page 145

Logging on to the ProtectV Manager VM as pvsuper

To log on to the ProtectV Manager VM as pvsuper:

1. Log on to ProtectV Manager as `pvadmin`.
2. Run `ssh pvsuper@localhost`. Accept the `SSH` fingerprint of key if logging on for the first time. The default password for the `pvsuper` user is `pvsuper`.
3. Switch to `root` (run `sudo su`.)

Deleting the Partition Table

To delete the partition table:

1. Run `fdisk /dev/sda`.
2. Enter **p** to print the partition table.
3. Delete all partitions.
   a. Enter **d** to delete a partition.
   b. Specify the partition number to delete.
   c. Perform the above two steps to delete all partitions. Continue deletion until the message "`No partition is defined yet!`" is displayed. The message indicates that no more partitions exist.
4. Enter **w** to write changes to the disk. The message "`The partition table has been altered!`" confirms the change.

Recreating the Partition Table with the Extended File System

To recreate the partition table with the extended file system:

1. Run `fdisk /dev/sda`.
2. Enter **p** to print the partition table.
3. Enter **n** to add a new partition.
4. Enter **p** to specify that the partition is primary.

5. Enter **1**.
6. Press **Enter** and select the default sector.
7. Enter the size by which you want to increase the file system with + symbol (for example, enter **+20G** to increase the size to 20 GB.)

Creating Additional Partitions

In the same command prompt, create an extended partition with a logical partition on it. To do so:

1. Enter **n** to add a new partition.
2. Enter **e** to select extended partition.
3. Enter **2**.
4. Press **Enter** to select the default first sector.
5. Press **Enter** to select the default last sector.
6. Enter **n** to add a new partition.
7. Enter **l** to specify that a logical partition will be created on the extended partition.
8. Press **Enter**to select the default first sector.
9. Press **Enter** to select the default last sector.
10. Enter **p** to print the partition table. In the end, you should have `sda1`, `sda2`, and `sda5`. The partitions, `sda2` and `sda5`, will have the same sectors.
11. Enter **w** to write changes to the disk.

Disabling the Swap Partition

To disable the swap partition:

1. Open `/etc/fstab` in the VI editor.
2. Comment out the entry for the swap partition.

   #`UUID=f06b25c8-16b3-4762-b8ca-17bf7e04ada4 none swap sw 0 0`
3. Save the file.
4. Reboot the ProtectV Manager VM by running `sudo reboot`.

Performing Online Resizing

To perform online resizing of partition:

1. Log on to ProtectV Manager as `pvsuper`.
   a. Log on to ProtectV Manager as `pvadmin`.
   b. Run `ssh pvsuper@localhost`. Accept the `SSH` fingerprint of key if logging on for the first time. The default password for the `pvsuper` user is `pvsuper`.
   c. Switch to `root` (run `sudo su`.)
2. Resize the `sda1` file system to increase the partition size by running `resize2fs /dev/sda1`. This command performs online resizing.

3. Confirm the changes by running `df -Th`. The output should indicate the increased size of `/dev/sda1`.

Activating the New Swap Partition

To activate the new swap partition:

1. Run `mkswap -c /dev/sda5`.
2. Run `swapon /dev/sda5`.
3. Run `swapon -s`.

Updating /etc/fstab with the UUID of New Swap

To update the `/etc/fstab` file with the new swap's UUID:

1. Find the UUID of the new swap partition by running `blkid`.

   For example:

   ```
   root@pvm:/home/pvsuper# blkid
   /dev/sda1: UUID="c5218613-b57a-411b-b1b2-41ccacc256f7" TYPE="ext4"
   /dev/sda5: UUID="8b173999-2980-4f8d-8495-4de47f4e9866" TYPE="swap"
   ```

2. Open `/etc/fstab` in the VI editor.
3. Uncomment the entry for the swap partition.
4. Replace the existing UUID with the one identified by running `blkid` above.

   For example:

   ```
   # swap was on /dev/sda5 during installation
   UUID=8b173999-2980-4f8d-8495-4de47f4e9866 none swap sw 0 0
   ```

5. Save the file.
6. Reboot the ProtectV Manager VM for the changes to take effect. Run `sudo reboot`.

APPENDIX D
Securing ASM Disks of Oracle RAC

This appendix provides instructions to secure Oracle Real Application Clusters (Oracle RAC) with Automatic Storage Management (ASM) using SafeNet ProtectV.

This appendix describes the following two scenarios:

- Shared disks on all virtual machines that will form Oracle RAC are encrypted individually (by using SafeNet ProtectV.) Oracle RAC and ASM are configured on the encrypted shared disks. Refer to "Configuring Oracle RAC with ASM on Encrypted Shared Disks" below for details.
- Oracle RAC and ASM are already up and running. All the shared disks are encrypted by using SafeNet ProtectV and added to the ASM disk group of Oracle RAC. Refer to "Adding Encrypted Shared Disks to ASM Disk Group" on page 148 for details.

Note: Procedures in this appendix are verified on Oracle RAC 12C and Red Hat Enterprise Linux 7.2 (64-bit) platforms running on VMware.

Note: iSCSI disks are not supported.

Configuring Oracle RAC with ASM on Encrypted Shared Disks

Configuring Oracle RAC with ASM on encrypted shared disks involves the following activities:

1. "Preparing Shared Disks" below
2. "Encrypting Shared Disks" on the next page
3. "Creating Shared Disks for ASM" on the next page
4. "Synchronizing Shared ASM Disks" on page 148
5. "Installing Oracle RAC" on page 148

Preparing Shared Disks

Make sure that the partitions on shared disks, which will form the ASM disk group, are of the same size. These partitions would be encrypted by using SafeNet ProtectV (as described in "Encrypting Shared Disks" on the next page) and used for creating shared disks for ASM.

After creating partitions on the shared disks, create the `ext4` file system on these partitions. Run the `mkfs ext4` command to create the file system.

Encrypting Shared Disks

To encrypt shared disks:

1. Individually encrypt required shared disks on all SafeNet ProtectV Client instances that form Oracle RAC.

   Encryption involves:

   a. Configuring SafeNet ProtectV components

   b. Installing the SafeNet ProtectV Client

   c. Setting up the network interface

   d. Registering client instances with ProtectV Manager

   Refer to relevant sections in this document for details.

2. After registration, **shut down** all the client instances.
3. Boot any of the client instances. Wait until the instance is booted successfully. Check that the disk is encrypted by running the `pvinfo` command (refer to " Verifying Encryption Status" on page 100.)
4. Allow keys to other protected instances. (On the ProtectV Manager Console, click **Allow It!** for other client instances.)
5. Boot the client instances, **one by one**.

   SafeNet ProtectV creates device mappers (`/dev/mapper/<ENCRYPTED_DISK_PARTITION>_secured`) for disk partitions being encrypted. For example, when encrypting `/dev/sd`**`b`**`1`, SafeNet ProtectV creates `/dev/mapper/sd`**`b`**`1_secured`. Similarly, a device mapper named `/dev/mapper/sd`**`c`**`1_secured` is created when encrypting `/dev/sd`**`c`**`1`.

6. *(Optional)* Wipe out the ext4 file system that you created when "Preparing New Shared Disks" on page 149. If this step is skipped, Oracle can still take the partition.

   Use the `dd` command to wipe the file system. For example, run:

   ```
   dd if=/dev/zero of=/dev/mapper/sdb1_secured bs=1M count=256
   ```

Creating Shared Disks for ASM

Create shared disks for ASM (also called as “shared ASM disks” in this document) using the shared disks encrypted in the above step.

To create shared disks for ASM:

1. Run the `oracleasm createdisk` command, as shown below:

   ```
   oracleasm createdisk <NAME_FOR_NEW_ASM_DISK> /dev/mapper/<ENCRYPTED_DISK_
   PARTITION>_secured
   ```

   Here, `<NAME_FOR_NEW_ASM_DISK>` represents the shared ASM disk that will be created from `< ENCRYPTED_DISK_PARTITION>_secured` and added to the ASM disk group.

   > **Note:** Run the `oracleasm createdisk` command for each encrypted disk that you want to add to the ASM disk group.

   For example, to create a shared ASM disk (`PVDISK1`,) run:

```
oracleasm createdisk PVDISK1 /dev/mapper/DISK_PARTITION1_secured
Marking disk "PVDISK1" as an ASM disk: [ OK ]
```

The shared ASM disk (`PVDISK1`) is created.

To create another shared ASM disk (`PVDISK2`,) run:

```
oracleasm createdisk PVDISK2 /dev/mapper/DISK_PARTITION2_secured
Marking disk "PVDISK2" as an ASM disk: [ OK ]
```

Similarly, create as many shared ASM disks as needed in the ASM disk group.

2. Verify the created shared disks.

   To verify the first shared ASM disk (`PVDISK1`,) run:

```
ls /dev/oracleasm/disks/PVDISK1 -ltr
brw-rw---- 1 grid asmadmin 253, 6 Aug 24 12:54 /dev/oracleasm/disks/PVDISK1
```

   To verify the second shared ASM disk (`PVDISK2`,) run:

```
ls /dev/oracleasm/disks/PVDISK2 -ltr
brw-rw---- 1 grid asmadmin 253, 6 Aug 24 12:56 /dev/oracleasm/disks/PVDISK2
```

   Similarly, verify the creation of all the remaining shared ASM disks.

Synchronizing Shared ASM Disks

Synchronize the shared ASM disks created above.

To synchronize the disks:

1. Run the `oracleasm scandisks` command, as shown below:

```
# oracleasm scandisks
Reloading disk partitions: done
Cleaning any stale ASM disks...
Scanning system for ASM disks...
```

2. Verify the synchronized shared ASM disks, as shown below.

```
# oracleasm listdisks
PVDISK1
PVDISK2
```

Installing Oracle RAC

Install Oracle RAC using the encrypted shared ASM disks. Refer to "Oracle Real Application Clusters Installation Guide" for details. Add the shared ASM disks created in the above step to form the ASM disk group.

Adding Encrypted Shared Disks to ASM Disk Group

Before proceeding with the procedure described below, make sure that Oracle RAC with ASM is up and running.

Activities involved in adding encrypted shared disks to the ASM disk group of Oracle RAC are:

1. "Preparing New Shared Disks" below
2. "Encrypting Newly Prepared Disks" on the next page
3. "Creating Shared Disks for ASM" on the next page
4. "Adding Shared ASM Disks to the Running ASM Disk Group" on the next page

Preparing New Shared Disks

Add new shared disks of size **2 MB larger** than the disks in the ASM disk group. For example, if each disk in the ASM disk group is **20 GB** in size, then each new disk to be added to the group must exactly be **20 GB + 2 MB** in size.

SafeNet ProtectV reserves 4096 sectors (512 bytes each in size) or 2 MB on shared disks being added. Therefore, to achieve the same size as the size of disks in the ASM disk group, after encrypting newly added shared disks, the new disk size **must** be 2 MB + the actual size of the ASM disk.

For example, the size of shared disks in the ASM disk group is 21.5 GB (that is, 21471690752 bytes or 41936896 sectors.) The number of sectors on all disks (existing and newly added) in the ASM disk group must match. In this example, the number of sectors on each ASM disk must be **41936896**.

The following sample shows the size of an existing ASM disk:

```
# oracleasm querydisk /dev/oracleasm/disks/PVDISK_SDB1
Device "/dev/oracleasm/disks/PVDISK_SDB1" is marked an ASM disk with the label
"PVDISK_SDB1"


Disk /dev/oracleasm/disks/PVDISK_SDB1: 21.5 GB, 21471690752 bytes, 41936896
sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

When preparing new shared disk partitions, ensure that the number of sectors on them is 41936896 + 4096 = **41940992**.

The following sample shows the size of a prepared shared disk:

```
# fdisk -l /dev/sdc1


Disk /dev/sdc1: 21.5 GB, 21473787904 bytes, 41940992 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

The above sample shows that the disk is 2 MB greater than the ASM disks.

After creating partitions on the shared disks, create the ext4 file system on these partitions. Run the `mkfs ext4` command to create the file system.

Note: The Oracle RAC administrator must prepare the equal number of disks as currently in the ASM disk group. For example, if the ASM disk group consists of five disks, it is recommended to prepare five disks. The plaintext (non-encrypted) disks can be removed from the disk group later.

Encrypting Newly Prepared Disks

Refer to "Encrypting Shared Disks" on page 147 for details.

Verify the size of shared disk after encryption. Notice that the disk size is equal to the size of ASM disks, as SafeNet ProtectV has consumed 4096 sectors (2 MB.)

The following sample shows the size of an encrypted shared disk:

```
# fdisk -l /dev/mapper/sdc1_secured
Disk /dev/mapper/sdc1_secured: 21.5 GB, 21471690752 bytes, 41936896 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

Creating Shared Disks for ASM

Refer to "Creating Shared Disks for ASM" on page 147 for details.

Verify the size of encrypted shared ASM disk. Notice that the disk size is equal to the size of ASM disks, as SafeNet ProtectV has consumed 4096 sectors (2 MB.)

The following sample shows the size of the encrypted existing ASM disk:

```
# oracleasm querydisk /dev/oracleasm/disks/PVDISK_SDC1
Device "/dev/oracleasm/disks/PVDISK_SDC1" is marked an ASM disk with the label
"PVDISK_SDC1"
Disk /dev/oracleasm/disks/PVDISK_SDC1: 21.5 GB, 21471690752 bytes, 41936896
sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

Adding Shared ASM Disks to the Running ASM Disk Group

Add the shared ASM disks created in the above step to the running ASM disk group. Refer to "Automatic Storage Management Administrator's Guide" for details.

Note: Before adding newly created encrypted shared ASM disks to the running ASM disk group and removing non-encrypted ASM disks, take backup of data and follow the instructions recommended by Oracle to synchronize data in the newly added disks.

INDEX

L

M

N

O

P

R

S

T

U

V

W