# SafeNet ProtectV

## CUSTOMER RELEASE NOTES

| | |
|---|---|
| **Version:** | 4.3.0 |
| **Issue Date:** | 1 December 2017 |
| **Document Number:** | 007-013688-001, Rev. E |
| **Issue Type:** | GA |

## Contents

# Product Description

SafeNet ProtectV provides the industry's first comprehensive solution for securing data in the virtual datacenter and the cloud, enabling organizations the freedom to migrate to virtual and cloud environments, while maintaining full ownership and control of data. This document may at times abbreviate "SafeNet ProtectV" to "ProtectV."

SafeNet ProtectV bridges the physical to virtual security gap by providing virtualized security controls that allow organizations to secure their data and maintain a consistent security policy as they transition to virtual platforms, such as Microsoft Hyper-V and VMware vSphere, and into the cloud. Whether using Microsoft Azure, IBM Bluemix (formerly SoftLayer), or Amazon Web Services EC2 for easy-to-scale capacity, or taking advantage of Amazon VPC to run AWS resources in a virtual network, SafeNet ProtectV ensures cloud-ready security.

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

# Release Description

SafeNet ProtectV 4.3.0 release offers new features and enhancements including:

- Key Rotation (Rekey)
- Command to Change Disk Encryption Password
- Command to Change Private Key Password
- New RESTful APIs
- Updated Commands
- SafeNet ProtectV API Guide
- SafeNet ProtectV Log Monitoring Guide

Refer to the *SafeNet ProtectV Clients Customer Release Notes* for the complete list of supported virtualized platforms. Refer to the *SafeNet ProtectV User's Guide* for details on features included in this release.

# New Features and Enhancements

## Key Rotation (Rekey)

SafeNet ProtectV 4.3.0 includes the key rotation (rekey) feature. 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 on the SafeNet ProtectV Manager Console. When configuring the feature, specify the number of days after which encryption keys should be changed automatically. By default, encryption keys are rotated after 180 days.

## Command to Change Disk Encryption Password

A new command, `pvmctl encryptpvm updatediskpass`, is added to change the password for ProtectV Manager's disk encryption.

## Command to Change Private Key Password

A new command, `pvmctl resetpvmkeypassword`, is added to change the private key password.

## New RESTful APIs

SafeNet ProtectV 4.3.0 includes the following new RESTful APIs to perform tasks from command line:

- `encryptPartition`: Encrypt a partition of a client instance
- `decryptPartition`: Decrypt a partition of a client instance
- `setRekeyPolicy`: Enable/disable and configure the rekey feature
- `getRekeyPolicy`: View existing rekey configuration
- `allowPartitionKey`: Allow keys for a partition to reassign it to a client instance
- `refusePartitionKey`: Refuse keys for a partition to prevent it from reassigning to a client instance
- `getPartitionKeyStatus`: Check whether keys are allowed or denied for a partition of a client instance

The following RESTful APIs are renamed in this release:

- `listInstancesDetails` as `listInstances`
- `encryptOn` as `encryptInstance`
- `encryptOff` as `decryptInstance`

Refer to the *SafeNet ProtectV API Guide* for details.

## Updated Commands

Custom CSR and private key can be imported for client certificate authentication with SafeNet KeySecure. For this, the following commands are updated:

- `pvmctl createcsr`: Create a client Certificate Signing Request (CSR.)
- `pvmctl configks`: Configure ProtectV Manager with SafeNet KeySecure.

## SafeNet ProtectV API Guide

Documentation of the RESTful API commands is removed from the *SafeNet ProtectV User’s Guide*. Existing and newly added API commands are documented in the *SafeNet ProtectV API Guide*.

## SafeNet ProtectV Log Monitoring Guide

This release includes the *SafeNet ProtectV Log Monitoring Guide*. This guide lists and describes audit and services logs generated on the SafeNet ProtectV Manager Console and ProtectV Client instances. The guide also explains logs of CLI authentication events.

# Advisory Notes

- When launching an external ProtectV Manager/Gateway in AWS, ensure to use a security group and a key pair. If they do not already exist, create them during launch. An IAM role is also needed if client authentication from cloud is required.
- If client authentication is enabled and AWS EC2 endpoints are inaccessible from ProtectV Gateway, the gateway cannot authenticate client from cloud. To resolve the issue, do 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 gwconfigclientauth disable`

- It is recommended to launch and configure multiple ProtectV Manager instances to ensure their high availability. If one goes down, another starts providing services.
- Rerun the `pvmctl gwstart` command every time the IP address of SafeNet ProtectV Manager changes.
- 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 “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)”.
- It is recommended to turn Autoscale on for an image before creating its clones. If Autoscale is turned on after new clones are already created, keys will not be granted to them.
- When specifying passwords from the command line, include them in double-quotes, `""`. For example, `"--prikeypass="PRIKEYPASS"`.

## Minimum System Requirements

Refer to the “System Requirements” section in the *SafeNet ProtectV User’s Guide*.

# Resolved and Known Issues

## Issue Severity and Classification

The following table serves as a key to the severity and classification of the issues listed in the **Resolved Issues** table and the **Known Issues** table, which can be found in the sections that follow.

| Severity | Classification | Definition |
|---|---|---|
| C | Critical | No reasonable workaround exists |
| H | High | Reasonable workaround exists |
| M | Medium | Medium-level priority problems |
| L | Low | Low-level priority problems |

## Resolved Issues

| Severity | Issue | Synopsis |
|---|---|---|
| H | PVT-1884 | **Summary:** Fix vulnerability related to the ProtectV Manager Database (PVMDB) port.<br>This issue has been fixed. |
| M | PVT-1958 | **Summary:** Add support to import custom CSR and private key for client certificate authentication with SafeNet KeySecure.<br>This issue has been fixed. |

| Severity | Issue | Synopsis |
|---|---|---|
| M | PVT-1872 | **Summary:** When a ProtectV Manager instance with static network configuration and encrypted disk is rebooted, attempts to start the SafeNet ProtectV service return error.<br>This issue has been fixed. |
| M | PVT-1594 | **Summary:** Users are not logged out when the Web browser tab containing the SafeNet ProtectV Manager Console or the browser is closed.<br>This issue has been fixed. |

## Known Issues

| Severity | Issue | Synopsis |
|---|---|---|
| M | PVT-1405 | **Summary:** ProtectV Manager cannot be deployed on VMware vSphere/ESXi v5.0 or lower versions.<br>**Workaround:** ProtectV Manager supports VMware vSphere/ESXi v5.1 and higher versions. To deploy ProtectV Manager on VMware 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. |
| M | PVT-1276 | **Summary:** Non-admin users can revoke gateways on the SafeNet ProtectV Manager Console. |
| M | PVT-1271 | **Summary:** The `pvmctl createcsr` command uses hardcoded attributes.<br>**Workaround:** To handle this issue:<br>1. Generate a CSR using OpenSSL on a different machine.<br>2. Copy the private key and signed certificate to the ProtectV Manager instance. |
| L | PVT-1575 | **Summary:** [Intermittent] Attempt to clear the cluster state of a deregistered node returns, "`deregister not called for this pvm`."<br>**Workaround:** Retry to clear the cluster state of the deregistered node. |

# Compatibility and Upgrade Information

## Interoperability

### Operating Systems

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 File Systems

**Linux**

- SafeNet ProtectV supports btrfs, ext2, ext3, ext4, and XFS file systems.

**NOTE:** As XFS is not the default file system on Red Hat Enterprise Linux 6.x and Ubuntu 14.04 platforms, SafeNet ProtectV does not support XFS file system on these platforms.

**Windows**

- SafeNet ProtectV supports NTFS on encrypted disk.

### Supported SafeNet KeySecure Versions

SafeNet ProtectV supports both virtual and physical SafeNet KeySecure servers. SafeNet ProtectV supports SafeNet KeySecure OS v8.1.0 and higher versions.

**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.

## Upgrade Instructions

- Upgrading from SafeNet ProtectV 3.3.0 and Higher
- Migration from SafeNet ProtectV 2.x

### Upgrading from SafeNet ProtectV 3.3.0 and Higher

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

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

To upgrade the ProtectV Manager instance:

1. Back up your ProtectV Manager database manually. Refer to "Backing up the SafeNet ProtectV Manager Database Manually" in the *SafeNet ProtectV 4.x User's Guide* for details.
2. Launch a new ProtectV Manager instance. Use the latest ProtectV Manager AMI from Gemalto. Refer to "Launching SafeNet ProtectV Manager Instance" in the *SafeNet ProtectV 4.x User's Guide* 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" in the *SafeNet ProtectV 4.x User's Guide* for details.
5. Configure the new ProtectV Manager instance with SafeNet KeySecure. Make sure that SafeNet KeySecure server and user are the same with which the old ProtectV Manager was configured. Refer to "Configuring SafeNet ProtectV Manager with SafeNet KeySecure" in the *SafeNet ProtectV 4.x User's Guide* for details.
6. Start the ProtectV Manager service on the new ProtectV Manager instance. Make sure 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" in the *SafeNet ProtectV 4.x User's Guide* 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 SafeNet ProtectV Manager instance in the registration file. Refer to "Updating the Registration File" section in the *SafeNet ProtectV 4.x User’s Guide* 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" in the *SafeNet ProtectV 4.x User’s Guide* for details.

## 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 can be upgraded to use the latest SafeNet ProtectV version.

To migrate from SafeNet ProtectV 2.x:

1. Set up SafeNet ProtectV components. Refer to the *SafeNet ProtectV 4.x User’s Guide* for details.
2. Upgrade SafeNet ProtectV Clients on client instances. Refer to "Upgrading SafeNet ProtectV Clients" in the *SafeNet ProtectV 4.x User’s Guide* for details.
3. Reboot the client instances.

# Limitations

- SafeNet ProtectV does not support rekey for Windows system partitions, for example, C:\ drive.
- [AWS] SafeNet ProtectV Manager, external SafeNet ProtectV Gateway, and client instances need not be in the same VPC. However, they must be able to communicate successfully.
- [AWS] SafeNet ProtectV Manager and external SafeNet ProtectV Gateway 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 Gateway.

  Refer to http://docs.aws.amazon.com/general/latest/gr/rande.html#ec2_region for details.

# Product Documentation

The following product documentation is associated with this release:

- *SafeNet ProtectV User’s Guide* (PN: 007-013689-001, Rev E)
- *SafeNet ProtectV API Guide* (PN: 007-013917-001, Rev A)
- *SafeNet ProtectV Log Monitoring Guide* (PN: 007-013951-001, Rev A)
- *SafeNet ProtectV Clients Customer Release Notes* (PN: 007-013691-001, Rev E)

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.

# 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<br>4690 Millennium Drive<br>Belcamp, Maryland  21017, USA | |
| **Phone** | US | 1-800-545-6608 |
| | International | 1-410-931-7520 |
| **Technical Support Customer Portal** | https://supportportal.gemalto.com<br>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. | |