SafeNet ProtectV

API Guide

gemalto
security to be free

Document Information

Document Information

Product Version	4.X
Document Number	007-013917-001
Release Date	01 December 2017

Revision History

Revision	Date	Reason
A	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 API 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 API Guide* provides description of RESTful APIs included in SafeNet ProtectV.

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 API Guide* contains the chapter "RESTful APIs" on page 9. This chapter describes how to set up client instances for the REST server. It also describes how to use the RESTful APIs included in SafeNet ProtectV to perform certain tasks from command line. These tasks can also be performed on the SafeNet ProtectV Manager Interface.

The *SafeNet ProtectV API Guide* contains the following chapters:

1. "RESTful APIs" on page 9
2. "Token APIs" on page 11
3. "Cloning APIs" on page 16
4. "Image and Instance APIs" on page 18
5. "Cryptographic APIs" on page 29

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 ]`
`[<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.

`{ 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
RESTful APIs

This chapter describes how to set up client instances for the REST server. It also describes how to use the RESTful APIs included in SafeNet ProtectV to perform certain tasks from command line. These tasks can also be performed on the SafeNet ProtectV Manager Interface.

Examples in this chapter show how to use the RESTful APIs using the Curl tool. You may use other tools or programs as per your requirements.

Setting up Clients for REST Server

Before using RESTful APIs, set up client instances for the REST server.

To do so:

1. Log on to your client instance.
2. Add an entry for ProtectV Manager in the list of hosts. For example, on a Linux client, add `<ProtectV Manager IP> pvmrest` in the `/etc/hosts` file.
3. Get the certificate of ProtectV Manager's REST server. This certificate is used for authentication when REST APIs are called.

   Run: `openssl s_client -showcerts -servername pvmrest -connect pvmrest:443`

   This command will display the certificate of ProtectV Manager's REST server.

   > **Note:** RESTful APIs included in SafeNet ProtectV do not support customer certificates. They use dynamically generated Gemalto certificates only.

4. Copy the certificate text. Copy starting from the header (`-----BEGIN CERTIFICATE-----`) to the footer (`-----END CERTIFICATE-----`).
5. Save the certificate text in a file, `<certificate>.crt`. Examples in this document use `server.crt`. This certificate will be required for calling RESTful APIs, as described in "Cloning APIs" on page 16.

API Response Codes

RESTful APIs included in SafeNet ProtectV are based on HTTP protocol. They return standard HTTP response status codes. The response codes returned by APIs included in SafeNet ProtectV are:

Response Code	Description
2xx	Success
4xx	Client errors

Response Code	Description
5xx	Server errors

Refer to "HTTP status codes" for details.

APIs in SafeNet ProtectV

The APIs included in SafeNet ProtectV can be categorized as:

- "Token APIs" on page 11
- "Image and Instance APIs" on page 18
- "Cryptographic APIs" on page 29
- "Cloning APIs" on page 16

2
Token APIs

The following table lists the RESTful APIs related to authentication and enrollment tokens:

Use this API…	To do this...
"getAuthToken"	Generate authentication token
"getClientEnrollmentToken"	Request for client enrollment token
"listClientEnrollmentTokens"	View the existing client enrollment tokens
"getClientEnrollmentTokenCount"	View the number of client enrollment tokens
"revokeClientEnrollmentToken"	Revoke client enrollment token

These APIs are described in subsequent sections.

getAuthToken

Use this API to generate an authentication token.

Syntax

```
curl --cacert <certificate>.crt -X GET 'https://pvmrest/getAuthToken' -D - -H 'Host:pvmrest'
-d '{"connection": "local_account",  "username": "USERNAME", "password": "PASSWORD"}'
```

Here,

- `USERNAME` – User name of the ProtectV Manager administrator.
- `PASSWORD` – Password of the ProtectV administrator.

Example

```
# curl --cacert server.crt -X GET 'https://pvmrest/getAuthToken' -D - -H 'Host:pvmrest' -d '
{"connection": "local_account", "username": "admin", "password": "adminpassword"}'
HTTP/1.1 201 Created
Server: nginx
Date: Thu, 22 Jun 2017 10:12:12 GMT
Content-Type: application/json
Content-Length: 356
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
        "token":
```

```
"eyJh-
bGciOiJIUzI1NiIsInR5cCI6Ik-
pXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJpc3MiOiJwdm0ifQ.8I3kK3PqWliSKL8
TmgMK-oYzU7U7Oe7GaUwtac__OfM",
        "msg": "Authentication token created. You can use it for further requests. This token
expires in 30 minutes. So, use it before it expires. If expired, you will have to create a
new token."
}
```

In the output above, `eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJpc3MiOiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM` is the generated authentication token. This token is used for authenticating requests such as creating or revoking a client enrollment token and turning on or off Autoscaling, as described in subsequent sections.

> **Note:** Authentication token expires in **30 minutes**; use it before it expires. If expired, you need to create a new token when needed.

getClientEnrollmentToken

Use this API to request for a client enrollment token.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X GET 'https://pvm-
rest/getClientEnrollmentToken' -D - -H 'Host:pvmrest'
```

Here,

- `AUTHTOKEN` – Authentication token generated using "getAuthToken" on the previous page.

Example

```
# curl --cacert server.crt -H "Authorization: Bearer
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJp
c3MiOiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X GET
'https://pvmrest/getClientEnrollmentToken' -D - -H 'Host:pvmrest'
HTTP/1.1 201 Created
Server: nginx
Date: Mon, 01 May 2017 10:07:20 GMT
Content-Type: application/json
Content-Length: 94
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
                "token": "nj4A00b6uQkAplNBhLkvkfXKJhb5gnB2",
                "msg": "Client enrollment token created."
}
```

In the output above, `nj4A00b6uQkAplNBhLkvkfXKJhb5gnB2` is the generated client enrollment token. This token is needed when revoking a client enrollment token, as described in "revokeClientEnrollmentToken" on the next page.

listClientEnrollmentTokens

Use this API to view existing client enrollment tokens.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X GET 'https://pvm-rest/listClientEnrollmentTokens' -D - -H 'Host:pvmrest' -d '{"skip":0, "limit":5}'
```

Here,

- `AUTHTOKEN` – Authentication token generated using "getAuthToken" on page 11.
- `'{"skip":0, "limit":5}'` – Range of records to display. Here, `{"skip":0, "limit":5}'` specifies that first five records (1 to 5) will be displayed.

Example

```
# curl --cacert server.crt -H "Authorization: Bearer
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJpc3MiOiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X GET
'https://pvmrest/listClientEnrollmentTokens' -D - -H 'Host:pvmrest' -d '{"skip":0, "limit":5}
'
HTTP/1.1 201 Created
Server: nginx
Date: Thu, 22 Jun 2017 10:14:36 GMT
Content-Type: application/json
Content-Length: 231
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
        "tokens": {
                "limit": 5,
                "resources": [
                        {
                                "secret": "Q1iA2XD7lwvFoo68HlSCMv7Ob3eqnpBM"
                        },
                        {
                                "secret": "3L4cznUPJe1t8OIKXsbyGRs3y9i90Vda"
                        }
                ],
                "skip": 0,
                "total": 2
        },
        "msg": "Available Tokens."
}
```

The sample output above shows the list of existing client enrollment tokens (secrets).

getClientEnrollmentTokenCount

Use this API to view the number of generated client enrollment tokens.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X GET 'https://pvm-rest/getClientEnrollmentTokenCount' -D - -H 'Host:pvmrest'
```

Here,

- `AUTHTOKEN` – Authentication token generated using "getAuthToken" on page 11.

Example

```
# curl --cacert server.crt -H "Authorization: Bearer
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJp
c3MiOiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X GET
'https://pvmrest/getClientEnrollmentTokenCount' -D - -H 'Host:pvmrest'
HTTP/1.1 201 Created
Server: nginx
Date: Thu, 06 Jul 2017 05:58:13 GMT
Content-Type: application/json
Content-Length: 66
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
                "msg": "Total client enrollment token count.",
                "count": "1"
}
```

The sample output above shows the number of generated client enrollment tokens.

revokeClientEnrollmentToken

Use this API to revoke a client enrollment token.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X POST 'https://pvm-rest/revokeClientEnrollmentToken/CLIENTENROLLMENTTOKEN' -D - -H 'Host:pvmrest'
```

Here,

- `AUTHTOKEN` – Authentication token generated using "getAuthToken" on page 11.
- `CLIENTENROLLMENTTOKEN` – Client enrollment token generated using "getClientEnrollmentToken" on page 12.

Example

```
# curl --cacert server.crt -H "Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJpc3Mi
OiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X POST
'https://pvmrest/revokeClientEnrollmentToken/nj4A00b6uQkAplNBhLkvkfXKJhb5gnB2' -D - -H
'Host:pvmrest'
HTTP/1.1 201 Created
Server: nginx
Date: Thu, 22 Jun 2017 10:25:24 GMT
Content-Type: application/json
Content-Length: 94
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
                "msg": "Client enrollment token revoked."
}
```

The sample output shows that the client enrollment token, `nj4A00b6uQkAplNBhLkvkfXKJhb5gnB2`, is revoked. Whenever needed, create a new client enrollment token, as described in "getClientEnrollmentToken" on page 12.

3
Cloning APIs

The following table lists the RESTful APIs related to cloning SafeNet ProtectV Client instances:

Use this API…	To do this...
"autoScaleOn"	Turn on autoscaling for a client instance
"autoScaleOff"	Turn off autoscaling for a client instance

These APIs are described in subsequent sections.

autoScaleOn

Use this API to turn on Autoscaling for a client image.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X POST 'https://pvm-rest/autoScaleOn/IMAGEIP' -D - -H 'Host:pvmrest'
```

Here,

- `AUTHTOKEN` – Authentication token generated using "getAuthToken" on page 11.
- `IMAGEIP` – IP address of the instance having Instance Name the same as the Image Name on the SafeNet ProtectV Manager Console. This is the IP address of the *first* instance based on the specified SafeNet ProtectV Client image.

Example

```
# curl --cacert server.crt -H "Authorization: Bearer eyJh-
bGciOiJIUzI1NiIsInR5cCI6Ik-
pXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJpc3MiOiJwdm0ifQ.8I3kK3PqWliSKL8
TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X POST 'https://pvmrest/autoScaleOn/34.207.214.231' -D - -H
'Host:pvmrest'
HTTP/1.1 201 Created
Server: nginx
Date: Thu, 22 Jun 2017 10:26:20 GMT
Content-Type: application/json
Content-Length: 69
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
```

```
                "msg": "Autoscaling turned ON for client image."
}
```

The sample output shows that Autoscaling is turned on for the client image. To turn it off, see "autoScaleOff" below.

autoScaleOff

Use this API to turn off Autoscaling for a client image.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X POST 'https://pvm-
rest/autoScaleOff/IMAGEIP' -D - -H 'Host:pvmrest'
```

Here,

- `AUTHTOKEN` – Authentication token generated using "getAuthToken" on page 11.
- `IMAGEIP` – IP address of the instance having Instance Name the same as the Image Name on the SafeNet ProtectV Manager Console. This is the IP address of the *first* instance based on the specified SafeNet ProtectV Client image.

Example

```
# curl --cacert server.crt -H "Authorization: Bearer
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJp
c3MiOiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X POST
'https://pvmrest/autoScaleOff/34.207.214.231' -D - -H 'Host:pvmrest'
HTTP/1.1 201 Created
Server: nginx
Date: Thu, 22 Jun 2017 10:27:02 GMT
Content-Type: application/json
Content-Length: 70
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
                "msg": "Autoscaling turned OFF for client image."
}
```

The sample output shows that Autoscaling is turned off for the client image. To again turn it on, see "autoScaleOn" on the previous page.

4
Image and Instance APIs

The following table lists the APIs related to SafeNet ProtectV images and client instances:

Use this API…	To do this...
"listImages"	View the registered SafeNet ProtectV Client images
"getImageCount"	View the number of registered SafeNet ProtectV Client images
"getInstanceDetails"	View the details of a client instance with the specified IP address
"listInstances"	View the details of all client instances
"getInstancesCount"	View the total number of instances on the SafeNet ProtectV Manager Console
"listImageInstances"	View the instances based on a client image with specified IP address
"getImageInstancesCount"	View the number of instances based on an image
"deleteImage"	Delete a SafeNet ProtectV Client image

These APIs are described in subsequent sections.

listImages

Use this API to view the registered SafeNet ProtectV Client images.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X GET 'https://pvm-rest/listImages' -D - -H 'Host:pvmrest' -d '{"skip":0, "limit":5}'
```

Here,

- `AUTHTOKEN` – Authentication token generated using "getAuthToken" on page 11.
- `'{"skip":0, "limit":5}'` – Range of records to display. Here, `{"skip":0, "limit":5}'` specifies that first five records (1 to 5) will be displayed.

Example

```
# curl --cacert server.crt -H "Authorization: Bearer
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJp
c3MiOiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X GET
'https://pvmrest/listImages' -D - -H 'Host:pvmrest' -d '{"skip":0, "limit":5}'
HTTP/1.1 201 Created
```

```
Server: nginx
Date: Thu, 22 Jun 2017 10:13:47 GMT
Content-Type: application/json
Content-Length: 544
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
        "images": {
                "limit": 5,
                "resources": [
                        {
                                "alarmed": false,
                                "cloudId": {
                                        "BiosUuid":
"Pqgu5n8bLjmjB2kB2QKxiOPagPmgANxNTcUgDoMd"
                                },
                                "cloudLocked": true,
                                "createdAt": "2017-06-22T09:43:57.262375Z",
                                "id": "eafceba7-893c-439a-aac0-802662ec68c6",
                                "instanceCount": 1,
                                "ip": "34.207.214.231",
                                "name": "ip-172-30-1-41",
                                "tags": [
                                        "a27426d4-ee5a-463a-b9c4-7e7e8ff1ce9e"
                                ],
                                "updatedAt": "2017-06-22T09:43:57.383737Z"
                        }
                ],
                "skip": 0,
                "total": 1
        },
        "msg": "Available Images."
}
```

The sample output above shows the registered SafeNet ProtectV Client images.

getImageCount

Use this API to view the number of registered SafeNet ProtectV Client images.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X GET 'https://pvm-
rest/getImageCount' -D - -H 'Host:pvmrest'
```

Here,

- `AUTHTOKEN` – Authentication token generated using "getAuthToken" on page 11.

Example

```
# curl --cacert server.crt -H "Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJpc3Mi
OiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X GET
'https://pvmrest/getImageCount' -D - -H 'Host:pvmrest'
HTTP/1.1 201 Created
Server: nginx
Date: Thu, 06 Jul 2017 05:58:37 GMT
Content-Type: application/json
Content-Length: 48
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
                "msg": "Total number of the registered client images.",
                "count": "1"
}
```

The sample output above shows that one SafeNet ProtectV Client image is registered on the SafeNet ProtectV Manager Console.

getInstanceDetails

Use this API to view the details of a client instance with specified IP address.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X GET 'https://pvm-
rest/getInstanceDetails/INSTANCEIP' -D - -H 'Host:pvmrest'
```

Here,

- `AUTHTOKEN` – Authentication token generated using "getAuthToken" on page 11.
- `INSTANCEIP` – IP address of the client instance.

Example

```
# curl --cacert server.crt -H "Authorization: Bearer
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJp
c3MiOiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X GET
'https://pvmrest/getInstanceDetails/34.207.214.231' -D - -H 'Host:pvmrest'
HTTP/1.1 201 Created
Server: nginx
Date: Thu, 22 Jun 2017 10:59:44 GMT
Content-Type: application/json
Content-Length: 1420
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
        "msg": "Instance Details.",
        "instance": {
                "alarmed": false,
                "applicationMetadata": {
```

```
                        "partitions": {
                                "48341277-cc4b-40b2-ab46-f3399367a5f1": {
                                        "decrypt": "false",
                                        "diskName": "xvdi",
                                        "friendlyName": "swap",
                                        "size": 1.073741824e+09,
                                        "status": "unprotected",
                                        "systemName": "xvdi"
                                },
                                "4ee8df0e-92ab-4aef-b276-b8ed167ed219": {
                                        "decrypt": "false",
                                        "diskName": "xvdh",
                                        "friendlyName": "/data",
                                        "size": 1.073741824e+09,
                                        "status": "unprotected",
                                        "systemName": "xvdh"
                                },
                                "aa697099-062b-4b53-976e-f2ac573effd9": {
                                        "decrypt": "false",
                                        "diskName": "xvda1",
                                        "friendlyName": "/",
                                        "size": 8.589934592e+09,
                                        "status": "unprotected",
                                        "systemName": "xvda1"
                                }
                        },
                        "platform": {
                                "clientVer": "4.2.0.DEV",
                                "linuxDistribution": [
                                        "Ubuntu",
                                        "14.04",
                                        "trusty"
                                ],
                                "system": "Linux",
                                "version": "#46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014"
                        },
                        "preboot": false
                },
                "authorized": true,
                "client": "ea81f2b7-4c77-4fe7-aad4-5149808047ac",
                "cloudId": {
                        "BiosUuid": "Pqgu5n8bLjmjB2kB2QKxiOPagPmgANxNTcUgDoMd"
                },
                "createdAt": "2017-06-22T10:58:34.907699Z",
                "id": "876e1466-335e-4cd2-9101-4de7d9ca731b",
                "ip": "34.207.214.231",
                "lastConnected": "2017-06-22T10:58:35.338691Z",
                "name": "ip-172-30-1-41",
                "updatedAt": "2017-06-22T10:58:35.352308Z"
        }
}
```


The sample output above shows details of the specified client instance.

getInstancesCount

Use this API to view the total number of instances on the SafeNet ProtectV Manager Console.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X GET 'https://pvm-rest/getInstancesCount' -D - -H 'Host:pvmrest'
```

Here,

- `AUTHTOKEN` – Authentication token generated using "getAuthToken" on page 11.

Example

```
# curl --cacert server.crt -H "Authorization: Bearer
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJp
c3MiOiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X GET
'https://pvmrest/getInstancesCount' -D - -H 'Host:pvmrest'
HTTP/1.1 201 Created
Server: nginx
Date: Thu, 06 Jul 2017 05:58:57 GMT
Content-Type: application/json
Content-Length: 51
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
                "msg": "Total number of instances on the management console.",
                "count": "2"
}
```

The sample output above shows that two instances are registered on the SafeNet ProtectV Manager Console.

listInstances

Use this API to view details of all client instances.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X GET 'https://pvm-rest/listInstances' -D - -H 'Host:pvmrest' -d '{"skip":0, "limit":5}'
```

Here,

- `AUTHTOKEN` – Authentication token generated using "getAuthToken" on page 11.
- `'{"skip":0, "limit":5}'` – Range of records to display. Here, `{"skip":0, "limit":5}'` specifies that first five records (1 to 5) will be displayed.

Example

```
# curl --cacert server.crt -H "Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJpc3Mi
OiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X GET
'https://pvmrest/listInstances' -D - -H 'Host:pvmrest' -d '{"skip":0, "limit":5}'
HTTP/1.1 201 Created
Server: nginx
Date: Thu, 22 Jun 2017 10:13:08 GMT
Content-Type: application/json
Transfer-Encoding: chunked
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
        "msg": "Available Instances.",
        "instance": {
                "limit": 5,
                "resources": [
                        {
                                "alarmed": false,
                                "applicationMetadata": {
                                        "partitions": {
                                                "48341277-cc4b-40b2-ab46-f3399367a5f1": {
                                                        "decrypt": "false",
                                                        "diskName": "xvdi",
                                                        "friendlyName": "swap",
                                                        "size": 1.073741824e+09,
                                                        "status": "unprotected",
                                                        "systemName": "xvdi"
                                                },
                                                "4ee8df0e-92ab-4aef-b276-b8ed167ed219": {
                                                        "decrypt": "false",
                                                        "diskName": "xvdh",
                                                        "friendlyName": "/data",
                                                        "size": 1.073741824e+09,
                                                        "status": "unprotected",
                                                        "systemName": "xvdh"
                                                },
                                                "aa697099-062b-4b53-976e-f2ac573effd9": {
                                                        "decrypt": "false",
                                                        "diskName": "xvda1",
                                                        "friendlyName": "/",
                                                        "size": 8.589934592e+09,
                                                        "status": "unprotected",
                                                        "systemName": "xvda1"
                                                }
                                        },
                                        "platform": {
                                                "clientVer": "4.3.0",
                                                "linuxDistribution": [
                                                        "Ubuntu",
                                                        "14.04",
                                                        "trusty"
                                                ],
                                                "system": "Linux",
```

```
                                        "version": "#46-Ubuntu SMP Thu Apr 10
19:11:08 UTC 2014"
                                },
                                "preboot": false
                        },
                        "authorized": true,
                        "client": "eafceba7-893c-439a-aac0-802662ec68c6",
                        "cloudId": {
                                "BiosUuid":
"Pqgu5n8bLjmjB2kB2QKxiOPagPmgANxNTcUgDoMd"
                        },
                        "createdAt": "2017-06-22T09:43:57.263595Z",
                        "id": "6f29d565-9d92-4cf1-8979-f523aa807a8a",
                        "ip": "34.207.214.231",
                        "lastConnected": "2017-06-22T09:43:57.614231Z",
                        "name": "ip-172-30-1-41",
                        "updatedAt": "2017-06-22T09:43:57.619816Z"
                },
                {
                        "alarmed": false,
                        "applicationMetadata": {
                                "partitions": {
                                        "48341277-cc4b-40b2-ab46-f3399367a5f1": {
                                                "decrypt": "false",
                                                "diskName": "xvdi",
                                                "friendlyName": "swap",
                                                "size": 1.073741824e+09,
                                                "status": "unprotected",
                                                "systemName": "xvdi"
                                        },
                                        "4ee8df0e-92ab-4aef-b276-b8ed167ed219": {
                                                "decrypt": "false",
                                                "diskName": "xvdh",
                                                "friendlyName": "/data",
                                                "size": 1.073741824e+09,
                                                "status": "unprotected",
                                                "systemName": "xvdh"
                                        },
                                        "aa697099-062b-4b53-976e-f2ac573effd9": {
                                                "decrypt": "false",
                                                "diskName": "xvda1",
                                                "friendlyName": "/",
                                                "size": 8.589934592e+09,
                                                "status": "unprotected",
                                                "systemName": "xvda1"
                                        }
                                },
                                "platform": {
                                        "clientVer": "4.3.0",
                                        "linuxDistribution": [
                                                "Ubuntu",
                                                "14.04",
                                                "trusty"
                                        ],
                                        "system": "Linux",
                                        "version": "#46-Ubuntu SMP Thu Apr 10
19:11:08 UTC 2014"
```

```
                                        },
                                        "preboot": false
                                },
                                "authorized": true,
                                "client": "e5d6dba6-e63f-476e-8d70-60e76181152f",
                                "cloudId": {
                                        "BiosUuid":
"Pqgu5n8bLjmjB2kB2QKxiOPagPmgANxNTcUgDoMd"
                                },
                                "createdAt": "2017-06-21T11:37:43.358817Z",
                                "id": "648fbe43-2cc1-467a-86b8-2dbf690d3d6e",
                                "ip": "34.207.214.231",
                                "lastConnected": "2017-06-22T04:09:33.474459Z",
                                "name": "ip-172-30-1-41",
                                "updatedAt": "2017-06-22T04:09:33.489141Z"
                        }
                ],
                "skip": 0,
                "total": 2
        }
}
```


The sample output above shows details of all client instances.

listImageInstances

Use this API to view all instances based on a SafeNet ProtectV Client image with specified IP address.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X GET 'https://pvm-
rest/listImageInstances/IMAGEIP' -D - -H 'Host:pvmrest' -d '{"skip":0, "limit":5}'
```

Here,

- `AUTHTOKEN` – Authentication token generated using "getAuthToken" on page 11.
- `IMAGEIP` – IP address of the instance having Instance Name the same as the Image Name on the SafeNet ProtectV Manager Console. This is the IP address of the *first* instance based on the specified SafeNet ProtectV Client image.
- `'{"skip":0, "limit":5}'` – Range of records to display. Here, `{"skip":0, "limit":5}'` specifies that first five records (1 to 5) will be displayed.

Example


```
# curl --cacert server.crt -H "Authorization: Bearer
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJp
c3MiOiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X GET
'https://pvmrest/listImageInstances/34.207.214.231' -D - -H 'Host:pvmrest' -d '{"skip":0,
"limit":5}'
HTTP/1.1 201 Created
Server: nginx
Date: Thu, 22 Jun 2017 10:16:15 GMT
```

```
Content-Type: application/json
Content-Length: 1652
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
        "images": {
                "limit": 5,
                "messages": [
                        "Searching on field tag is not supported."
                ],
                "resources": [
                        {
                                "alarmed": false,
                                "applicationMetadata": {
                                        "partitions": {
                                                "48341277-cc4b-40b2-ab46-f3399367a5f1": {
                                                        "decrypt": "false",
                                                        "diskName": "xvdi",
                                                        "friendlyName": "swap",
                                                        "size": 1.073741824e+09,
                                                        "status": "unprotected",
                                                        "systemName": "xvdi"
                                                },
                                                "4ee8df0e-92ab-4aef-b276-b8ed167ed219": {
                                                        "decrypt": "false",
                                                        "diskName": "xvdh",
                                                        "friendlyName": "/data",
                                                        "size": 1.073741824e+09,
                                                        "status": "unprotected",
                                                        "systemName": "xvdh"
                                                },
                                                "aa697099-062b-4b53-976e-f2ac573effd9": {
                                                        "decrypt": "false",
                                                        "diskName": "xvda1",
                                                        "friendlyName": "/",
                                                        "size": 8.589934592e+09,
                                                        "status": "unprotected",
                                                        "systemName": "xvda1"
                                                }
                                        },
                                        "platform": {
                                                "clientVer": "4.2.0.DEV",
                                                "linuxDistribution": [
                                                        "Ubuntu",
                                                        "14.04",
                                                        "trusty"
                                                ],
                                                "system": "Linux",
                                                "version": "#46-Ubuntu SMP Thu Apr 10
19:11:08 UTC 2014"
                                        },
                                        "preboot": false
                                },
                                "authorized": true,
                                "client": "eafceba7-893c-439a-aac0-802662ec68c6",
                                "cloudId": {
```

```
                                        "BiosUuid":
"Pqgu5n8bLjmjB2kB2QKxiOPagPmgANxNTcUgDoMd"
                                    },
                                    "createdAt": "2017-06-22T09:43:57.263595Z",
                                   "id": "6f29d565-9d92-4cf1-8979-f523aa807a8a",
                                    "ip": "34.207.214.231",
                                    "lastConnected": "2017-06-22T09:43:57.614231Z",
                                    "name": "ip-172-30-1-41",
                                    "updatedAt": "2017-06-22T09:43:57.619816Z"
                            }
                ],
                "skip": 0,
                "total": 1
        },
        "msg": "Available Instances."
}
```


The sample output above shows the list of all instances based on the specified SafeNet ProtectV Client image.

getImageInstancesCount

Use this API to view the number of instances based on a SafeNet ProtectV Client image.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X GET 'https://pvm-
rest/getImageInstancesCount/IMAGEIP' -D - -H 'Host:pvmrest'
```

Here,

- `AUTHTOKEN` – Authentication token generated using "getAuthToken" on page 11.
- `IMAGEIP` – IP address of the instance having Instance Name the same as the Image Name on the SafeNet ProtectV Manager Console. This is the IP address of the *first* instance based on the specified SafeNet ProtectV Client image.

Example


```
# curl --cacert server.crt -H "Authorization: Bearer
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJp
c3MiOiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X GET
'https://pvmrest/getImageInstancesCount/52.91.56.178' -D - -H 'Host:pvmrest'
HTTP/1.1 201 Created
Server: nginx
Date: Thu, 06 Jul 2017 05:59:33 GMT
Content-Type: application/json
Content-Length: 58
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
                "msg": "Total number of instances based on a client image.",
                "count": "2"
}
```

The sample output above shows that *two* instances are based on the specified SafeNet ProtectV Client image.

deleteImage

Use this API to delete a SafeNet ProtectV Client image.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X DELETE 'https://pvm-rest/deleteImage/IMAGEIP' -D - -H 'Host:pvmrest' -d '{"confirm":"Yes"}'
```

Here,

- `AUTHTOKEN` – Authentication token generated using "getAuthToken" on page 11.
- `IMAGEIP` – IP address of the instance having Instance Name the same as the Image Name on the SafeNet ProtectV Manager Console. This is the IP address of the *first* instance based on the specified SafeNet ProtectV Client image.
- `'{"confirm":"Yes"}'` – Option to run the command without asking for confirmation to delete the image. If this option is not specified, the image will not be deleted.

Example

```
# curl --cacert server.crt -H "Authorization: Bearer
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJp
c3MiOiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X DELETE
'https://pvmrest/deleteImage/34.207.214.231' -D - -H 'Host:pvmrest' -d '{"confirm":"Yes"}'
HTTP/1.1 201 Created
Server: nginx
Date: Thu, 22 Jun 2017 10:53:41 GMT
Content-Type: application/json
Content-Length: 41
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
        "msg": "Image deleted successfully."
}
```

The sample output above shows that the SafeNet ProtectV Client image is deleted successfully.

5
Cryptographic APIs

The following table lists the cryptographic APIs available in SafeNet ProtectV:

Use this API...	To do this...
"decryptInstance"	Decrypt all partitions of a protected client instance
"encryptInstance"	Encrypt all partitions of a decrypted client instance
"encryptPartition"	Encrypt a partition of a client instance
"decryptPartition"	Decrypt a partition of a client instance
"setRekeyPolicy"	Enable 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

These APIs are described in subsequent sections.

decryptInstance

Use this API to decrypt all partitions of a client instance.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X POST 'https://pvm-rest/decryptInstance/INSTANCEIP' -D - -H 'Host:pvmrest'
```

Here,

- `AUTHTOKEN` – Authentication token generated using "getAuthToken" on page 11.
- `INSTANCEIP` – IP address of the client instance on the SafeNet ProtectV Manager Console.

Example

```
# curl --cacert server.crt -H "Authorization: Bearer eyJh-
bGciOiJIUzI1NiIsInR5cCI6Ik-
pXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJpc3MiOiJwdm0ifQ.8I3kK3PqWliSKL8
TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X POST 'https://pvmrest/decryptInstance/34.207.214.231' -D - -
```

```
H 'Host:pvmrest'
HTTP/1.1 201 Created
Server: nginx
Date: Thu, 22 Jun 2017 10:23:06 GMT
Content-Type: application/json
Content-Length: 61
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
        "msg": "Decryption will happen on next client reboot."
}
```

The sample output shows that the client instance is ready for decryption. All partitions of the client instance will be decrypted during the next reboot. To again encrypt the instance, see "encryptInstance" below.

> **Note:** Windows client instances do not require reboot for decryption.

encryptInstance

Use this API to encrypt all partitions of a client instance.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X POST 'https://pvm-
rest/encryptInstance/INSTANCEIP' -D - -H 'Host:pvmrest'
```

Here,

- `AUTHTOKEN` – Authentication token generated using "getAuthToken" on page 11.
- `INSTANCEIP` – IP address of the client instance on the SafeNet ProtectV Manager Console.

Example

```
# curl --cacert server.crt -H "Authorization: Bearer eyJh-
bGciOiJIUzI1NiIsInR5cCI6Ik-
pXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJpc3MiOiJwdm0ifQ.8I3kK3PqWliSKL8
TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X POST 'https://pvmrest/encryptInstance/172.30.1.60' -D - -H
'Host:pvmrest'

HTTP/1.1 201 Created
Server: nginx
Date: Mon, 24 Apr 2017 10:18:49 GMT
Content-Type: application/json
Content-Length: 69
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
                "msg": "Encryption will happen on next client reboot."
}
```

The sample output shows that the client instance is ready for encryption. All partitions of the client instance will be encrypted during the next reboot. To decrypt the instance, see "decryptInstance" on page 29.

Note: Windows client instances do not require reboot for encryption.

encryptPartition

Use this API to encrypt a partition of a client instance.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X PATCH 'https://pvm-rest/encryptPartition/INSTANCEIP/SYSTEMNAME' -D - -H 'Host:pvmrest'
```

Here,

- `AUTHTOKEN` – Authentication token generated using "getAuthToken" on page 11.
- `INSTANCEIP` – IP address of the client instance on the SafeNet ProtectV Manager Console.
- `SYSTEMNAME` – Name of the partition.

Note: You can find the names of a client instance's partitions on the SafeNet ProtectV Manager Console. Alternatively, use "getInstanceDetails" to view the partitions of a client instance. Check for the values of `"systemName"` entries; for example, `"systemName": "sdc"`. There will be multiple entries of `"systemName"`, one per partition.

Example (Linux)

```
# curl --cacert server.crt -H "Authorization: Bearer
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJpc3MiOiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X PATCH
'https://pvmrest/encryptPartition/10.164.12.197/sdc' -D - -H 'Host:pvmrest'
HTTP/1.1 201 Created
Server: nginx
Date: Mon, 14 Aug 2017 09:51:12 GMT
Content-Type: application/json
Content-Length: 61
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
        "msg": "Encryption turned on for specified partition."
}
```

The sample output above shows that the partition is ready for encryption. The partition will be encrypted during the next reboot. To decrypt the partition, see "decryptPartition" on the next page.

Example (Windows)

```
# curl --cacert server.crt -H "Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJpc3Mi
OiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X PATCH
'https://pvmrest/encryptPartition/10.164.12.197/Volume\{b88e1404-0000-0000-0000-
100000000000\}' -D - -H 'Host:pvmrest'
```

Note: Windows client instances do not require reboot for encryption.

decryptPartition

Use this API to decrypt a partition of a client instance.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X PATCH 'https://pvm-
rest/decryptPartition/INSTANCEIP/SYSTEMNAME' -D - -H 'Host:pvmrest'
```

Here,

- `AUTHTOKEN` – Authentication token generated using "getAuthToken" on page 11.
- `INSTANCEIP` – IP address of the client instance on the SafeNet ProtectV Manager Console.
- `SYSTEMNAME` – Name of the partition.

Note: Find the names of a client instance's partitions on the SafeNet ProtectV Manager Console. Alternatively, use "getInstanceDetails" to view the partitions of a client instance. Check for the values of `"systemName"` entries; for example, `"systemName": "sdc"`. There will be multiple entries of `"systemName"`, one per partition.

Example (Linux)

```
# curl --cacert server.crt -H "Authorization: Bearer
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJp
c3MiOiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X PATCH
'https://pvmrest/decryptPartition/10.164.12.197/sdc' -D - -H 'Host:pvmrest'
HTTP/1.1 201 Created
Server: nginx
Date: Mon, 14 Aug 2017 09:51:16 GMT
Content-Type: application/json
Content-Length: 62
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
        "msg": "Encryption turned off for specified partition."
}
```

The sample output above shows that the partition is ready for decryption. The partition will be decrypted during the next reboot. To again encrypt the partition, see "encryptPartition" on the previous page.

Example (Windows)

```
# curl --cacert server.crt -H "Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJpc3Mi
OiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X PATCH
'https://pvmrest/decryptPartition/10.164.12.197/Volume\{b88e1404-0000-0000-0000-
100000000000\}' -D - -H 'Host:pvmrest'
```

Note: Windows client instances do not require reboot for decryption.

setRekeyPolicy

Use this API to enable/disable and configure the rekey feature.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X POST 'https://pvm-
rest/setRekeyPolicy' -D - -H 'Host:pvmrest' -d '{"rekeyInterval":"N"}'
```

Here,

- `AUTHTOKEN` – Authentication token generated using "getAuthToken" on page 11.
- `'{"rekeyInterval":"N"}'` – Rekey interval in days. Here, `"N"` is a *positive* integer that specifies the days after which existing encryption keys will be changed automatically. The default value of `"N"` is `180`.

Note: To disable the rekey feature, set `'{"rekeyInterval":"0"}'`.

Example

```
# curl --cacert server.crt -H "Authorization: Bearer
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJp
c3MiOiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X POST
'https://pvmrest/setRekeyPolicy' -D - -H 'Host:pvmrest' -d '{"rekeyInterval":"10"}'
HTTP/1.1 201 Created
Server: nginx
Date: Mon, 04 Sep 2017 16:06:23 GMT
Content-Type: application/json
Content-Length: 65
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
                "msg": "Rekey interval set to:",
                "rekeyInterval": "10 Days"
}
```

The sample output above shows that the rekey interval is set to 10 days. Encryption keys will be changed automatically after 10 days. To view the existing rekey interval in future, refer to "getRekeyPolicy" below.

getRekeyPolicy

Use this API to view the existing rekey configuration.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X GET 'https://pvm-rest/getRekeyPolicy' -D - -H 'Host:pvmrest'
```

Here,

- `AUTHTOKEN` – Authentication token generated using "getAuthToken" on page 11.

Example

```
# curl --cacert server.crt -H "Authorization: Bearer
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJp
c3MiOiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X GET
'https://pvmrest/getRekeyPolicy' -D - -H 'Host:pvmrest'
HTTP/1.1 201 Created
Server: nginx
Date: Mon, 04 Sep 2017 16:07:04 GMT
Content-Type: application/json
Content-Length: 61
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
                "msg": "Existing rRekey interval is:",
                "rekeyInterval": "10 Days"
}
```

The sample output above shows that the existing rekey interval is set to 10 days. Encryption keys will be changed automatically after 10 days. To change the rekey interval, refer to "setRekeyPolicy" on the previous page.

allowPartitionKey

Use this API to allow keys for a partition to reassign it to a client instance.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X PATCH 'https://pvm-rest/allowPartitionKey/INSTANCEIP/SYSTEMNAME' -D - -H 'Host:pvmrest'
```

Here,

- `AUTHTOKEN` – Authentication token generated using "getAuthToken" on page 11.
- `INSTANCEIP` – IP address of the client instance on the SafeNet ProtectV Manager Console.

- SYSTEMNAME – Name of the partition.

> **Note:** Find the names of a client instance's partitions on the SafeNet ProtectV Manager Console. Alternatively, use "getInstanceDetails" to view the partitions of a client instance. Check for the values of "systemName" entries; for example, "systemName": "sdc". There will be multiple entries of "systemName", one per partition.

Example (Linux)

```
# curl --cacert server.crt -H "Authorization: Bearer
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJp
c3MiOiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X PATCH
'https://pvrest/allowPartitionKey/10.164.12.197/sdc' -D - -H 'Host:pvmrest'
HTTP/1.1 201 Created
Server: nginx
Date: Mon, 14 Aug 2017 09:50:47 GMT
Content-Type: application/json
Content-Length: 48
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
        "msg": "Partition assigned successfully."
}
```

The sample output above shows that the partition is allowed reassignment to the client instance.

Example (Windows)

```
# curl --cacert server.crt -H "Authorization: Bearer eyJh-
bGciOiJIUzI1NiIsInR5cCI6Ik-
pXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJpc3MiOiJwdm0ifQ.8I3kK3PqWliSKL8
TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X PATCH
'https://pvrest/allowPartitionKey/10.164.12.197/Volume\{b88e1404-0000-0000-0000-
100000000000\}' -D - -H 'Host:pvmrest'
```

refusePartitionKey

Use this API to refuse keys for a partition to prevent it from reassigning to a client instance.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X PATCH 'https://pvm-
rest/refusePartitionKey/INSTANCEIP/SYSTEMNAME' -D - -H 'Host:pvmrest'
```

Here,

- AUTHTOKEN – Authentication token generated using "getAuthToken" on page 11.
- INSTANCEIP – IP address of the client instance on the SafeNet ProtectV Manager Console.

- SYSTEMNAME – Name of the partition.

> **Note:** Find the names of a client instance's partitions on the SafeNet ProtectV Manager Console. Alternatively, use "getInstanceDetails" to view the partitions of a client instance. Check for the values of "systemName" entries; for example, "systemName": "sdc". There will be multiple entries of "systemName", one per partition.

Example (Linux)

```
# curl --cacert server.crt -H "Authorization: Bearer
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJp
c3MiOiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X PATCH
'https://pvmrest/refusePartitionKey/10.164.12.197/sdc' -D - -H 'Host:pvmrest'
HTTP/1.1 201 Created
Server: nginx
Date: Mon, 14 Aug 2017 09:50:55 GMT
Content-Type: application/json
Content-Length: 50
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
        "msg": "Partition unassigned successfully."
}
```

The sample output above shows that the partition is prevented from reassigning to the client instance.

Example (Windows)

```
# curl --cacert server.crt -H "Authorization: Bearer
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJp
c3MiOiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X PATCH
'https://pvmrest/refusePartitionKey/10.164.12.197/Volume\{b88e1404-0000-0000-0000-
100000000000\}' -D - -H 'Host:pvmrest'
```

getPartitionKeyStatus

Use this API to check whether keys are allowed or denied for a partition of a client instance.

Syntax

```
curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X GET 'https://pvm-
rest/getPartitionKeyStatus/INSTANCEIP/SYSTEMNAME' -D - -H 'Host:pvmrest'
```

Here,

- AUTHTOKEN – Authentication token generated using "getAuthToken" on page 11.
- INSTANCEIP – IP address of the client instance on the SafeNet ProtectV Manager Console.
- SYSTEMNAME – Name of the partition.

Note: Find the names of a client instance's partitions on the SafeNet ProtectV Manager Console. Alternatively, use "getInstanceDetails" to view the partitions of a client instance. Check for the values of `"systemName"` entries; for example, `"systemName": "sdc"`. There will be multiple entries of `"systemName"`, one per partition.

Example (Linux)

```
# curl --cacert server.crt -H "Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJpc3Mi
OiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X GET
'https://pvmrest/getPartitionKeyStatus/10.164.12.197/sdc' -D - -H 'Host:pvmrest'
HTTP/1.1 201 Created
Server: nginx
Date: Mon, 14 Aug 2017 09:51:31 GMT
Content-Type: application/json
Content-Length: 66
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
        "msg": "Current permission for partition",
        "permit": false
}
```

The sample output above shows that keys are denied for the partition of the client instance.

Example (Windows)

```
# curl --cacert server.crt -H "Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJpc3Mi
OiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-oYzU7U7Oe7GaUwtac__OfM" -X GET
'https://pvmrest/getPartitionKeyStatus/10.164.12.197/Volume\{b88e1404-0000-0000-0000-
100000000000\}' -D - -H 'Host:pvmrest'
```

APPENDIX A
Compliance Report

This appendix provides instructions to generate a compliance report on client instances registered with SafeNet ProtectV Manager.

Generating the Compliance Report

To generate a compliance report:

1. Generate an authentication token. This token is used to establish communication with the REST server.

   Run `curl --cacert <certificate>.crt -X GET 'https://pvmrest/getAuthToken' -D - -H 'Host:pvmrest' -d '{"connection": "local_account", "username": "USERNAME", "password": "PASSWORD"}'`

   Refer to "getAuthToken" on page 11 for details.

2. View details of all instances.

   Run `curl --cacert <certificate>.crt -H "Authorization: Bearer AUTHTOKEN" -X GET 'https://pvmrest/listInstances' -D - -H 'Host:pvmrest' -d '{"skip":0, "limit":5}'`

Refer to "listInstances" on page 22 for details. The output of the `listInstances` API shows details of all partitions of all instances.

For example:

```
# curl --cacert server.crt -H "Authorization: Bearer eyJh-
bGciOiJIUzI1NiIsInR5cCI6Ik-
pXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZXhwIjoxNDk4MTI4MTMyLCJpc3MiOiJwdm0ifQ.8I3kK3PqWliSKL8TmgMK-
oYzU7U7Oe7GaUwtac__OfM" -X GET 'https://pvmrest/listInstances' -D - -H 'Host:pvmrest' -d '
{"skip":0, "limit":5}'
HTTP/1.1 201 Created
Server: nginx
Date: Thu, 22 Jun 2017 10:13:08 GMT
Content-Type: application/json
Transfer-Encoding: chunked
Connection: keep-alive
X-Frame-Options: SAMEORIGIN

{
        "msg": "Available Instances.",
        "instance": {
                "limit": 5,
                "resources": [
                                                Instance 1
                        {
                                "alarmed": false,
                                "applicationMetadata": {
                                        "partitions": {
```

```
                                        "4ee8df0e-92ab-4aef-b276-b8ed167ed219": {
                                                "decrypt": "false",
                                                "diskName": "xvdh",
                                                "friendlyName": "/data",
                                                "size": 1.073741824e+09,
                                                "status": "protected",
                                                "systemName": "xvdh"
                                        },
                                        "aa697099-062b-4b53-976e-f2ac573effd9": {
                                                "decrypt": "false",
                                                "diskName": "xvda1",
                                                "friendlyName": "/",
                                                "size": 8.589934592e+09,
                                                "status": "unprotected",
                                                "systemName": "xvda1"
                                        }
                                },
                                "platform": {
                                        "clientVer": "4.2.0.DEV",
                                        "linuxDistribution": [
                                                "Ubuntu",
                                                "14.04",
                                                "trusty"
                                        ],
                                        "system": "Linux",
                                        "version": "#46-Ubuntu SMP Thu Apr 10
19:11:08 UTC 2014"
                                },
                                "preboot": false
                        },
                        "authorized": true,
                        "client": "eafceba7-893c-439a-aac0-802662ec68c6",
                        "cloudId": {
                                "BiosUuid": "Pqgu5n8bLjmjB2kB2QKx-
iOPagPmgANxNTcUgDoMd"
                        },
                        "createdAt": "2017-06-22T09:43:57.263595Z",
                        "id": "6f29d565-9d92-4cf1-8979-f523aa807a8a",
                        "ip": "34.207.214.231",
                        "lastConnected": "2017-06-22T09:43:57.614231Z",
                        "name": "ip-172-30-1-41",
                        "updatedAt": "2017-06-22T09:43:57.619816Z"
                },
```


Instance 2


```
                {
                        "alarmed": false,
                        "applicationMetadata": {
                                "partitions": {
                                        "4ee8df0e-92ab-4aef-b276-b8ed167ed219": {
                                                "decrypt": "false",
                                                "diskName": "xvdh",
                                                "friendlyName": "/data",
                                                "size": 1.073741824e+09,
                                                "status": "unprotected",
                                                "systemName": "xvdh"
                                        },
                                        "aa697099-062b-4b53-976e-f2ac573effd9": {
```

```
                                                "decrypt": "false",
                                                "diskName": "xvda1",
                                                "friendlyName": "/",
                                                "size": 8.589934592e+09,
                                                "status": "protected",
                                                "systemName": "xvda1"
                                        }
                                },
                                "platform": {
                                        "clientVer": "4.3.0",
                                        "linuxDistribution": [
                                                "Ubuntu",
                                                "14.04",
                                                "trusty"
                                        ],
                                        "system": "Linux",
                                        "version": "#46-Ubuntu SMP Thu Apr 10
19:11:08 UTC 2014"
                                },
                                "preboot": false
                        },
                        "authorized": true,
                        "client": "e5d6dba6-e63f-476e-8d70-60e76181152f",
                        "cloudId": {
                                "BiosUuid": "Pqgu5n8bLjmjB2kB2QKx-
iOPagPmgANxNTcUgDoMd"
                        },
                        "createdAt": "2017-06-21T11:37:43.358817Z",
                        "id": "648fbe43-2cc1-467a-86b8-2dbf690d3d6e",
                        "ip": "34.207.214.231",
                        "lastConnected": "2017-06-22T04:09:33.474459Z",
                        "name": "ip-172-30-1-41",
                        "updatedAt": "2017-06-22T04:09:33.489141Z"
                }
        ],
        "skip": 0,
        "total": 2
    }
}
```


The sample output above shows details of partitions of *two* (indicated by **`"total": 2`**) client instances (labelled **Instance 1** and **Instance 2**.) The actual number of client instances and partitions on them may vary.

This document shows details of two partitions of two client instances only. Look for details under the **`"applicationMetadata"`** tag in the API output. Each tag shows important details of a client instance under `"partitions"`, `"platform"`, and `"preboot"`.

- `"partitions"` – Shows the following details about partitions of a client instance:
  - `decrypt` – Whether marked for decryption; `"true"` for partitions marked for encryption, `"false"` for partitions marked for decryption.
  - `diskName` – Name of the partition.
  - `friendlyName` – Friendly name of the partition.
  - `size` – Size of the partition.

  - `status` – Encryption status of the partition; `"protected"` for encrypted partitions, `"unprotected"` for unencrypted partitions.
  - `systemName` – System name of the partition.
- `"platform"` – Shows the version of the SafeNet ProtectV Client and operating system running on a client instance.
- `"preboot"` – Shows whether the client instance is in preboot state. By default, it is set to `false`; in preboot state, it is set to `true`.

Apart from information under the **`"applicationMetadata"`** tag, the API provides details such as the IP address of the client instance, name of the client instance, and when the client was last connected and update.

INDEX