SafeNet ProtectV

Log Monitoring Guide

gemalto
security to be free

Document Information

Document Information

Product Version	4.X
Document Number	007-013951-001
Release Date	01 December 2017

Revision History

Revision	Date	Reason
B	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 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 ProtectVLog Monitoring Guide* describes audit and services logs generated on the SafeNet ProtectV Manager Console and ProtectV Client instances. The guide also explains logs of CLI login events occurring on ProtectV Manager.

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".

What's New?

SafeNet ProtectV offers improved logging in this release. Logs of CLI login events are redirected to a configured Syslog server. These logs include information such as when events occurred, IP address of host machines, and event success or failure messages.

Moreover, this release includes reformatted audit logs for better readability.

Organization

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**.)

Convention	Description
	• 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
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 also provides an option to redirect audit and services logs to a dedicated Syslog server. When ProtectV Manager is configured for the Syslog server, logs of CLI login events automatically start redirecting to the Syslog server. These events include login attempts to ProtectV Manager using `SSH`.

Refer to the "Redirecting Logs to Syslog Server" section in the *SafeNet ProtectV User's Guide* for details.

This section covers the following information:

Audit Events

This section provides format of audit event logs and lists significant audit events logged by SafeNet ProtectV Manager.

Log Format

Audit events are logged in the following format:

```
<TIMESTAMP> <PVMIP> gordium <PVM-TIMESTAMP> category=<CATEGORY>, status=<STATUS>,
msg=<MESSAGE>, subject=<SUBJECT>, client-name=<CLIENT-NAME>
```

Here,

- `<TIMESTAMP>`: Date and time when the log is redirected to the Syslog server. This column appears on logs stored on the Syslog server.
- `<PVMIP>`: IP address of the ProtectV Manager instance where logs are generated. This column appears on logs stored on the Syslog server.
- `<PVM-TIMESTAMP>`: Date and time when the log is generated on the ProtectV Manager instance.
- `<CATEGORY>`: Category of the log entry is `Audit`.
- `<STATUS>`: Status of the event, `success`or `failure`.
- `<MESSAGE>`: Event message.
- `<SUBJECT>`: Title of the event.
- `<CLIENT-NAME>`: Host name of the client if the audit event is related to a client. `<None>` is displayed in logs if the log entry is not related to a client.

Sample logs are:

```
Oct 12 07:35:49 54.89.128.83 gordium 2017-10-12 07:35:48 category=<Audit>
status=<success> msg=<Client instance update success> subject=<Instance> client-
name=<ip-172-30-1-40>

Oct 12 07:28:15 54.89.128.83 gordium 2017-10-12 07:28:14 category=<Audit>
status=<success> msg=<Agent create success> subject=<Agent> client-name=<none>

Oct 12 07:28:15 54.89.128.83 gordium 2017-10-12 07:28:13 category=<Audit>
status=<success> msg=<Gateway token create> subject=<AgentEnrollmentToken>
client-name=<none>

Oct 12 07:28:15 54.89.128.83 gordium 2017-10-12 07:28:14 category=<Audit>
status=<success> msg=<Agent create success> subject=<Agent> client-name=<none>
```

Errors

The following table lists significant error events logged by SafeNet ProtectV Manager.

Event	Description	Remedy
`Agent create error`	ProtectV Gateway could not be enrolled with ProtectV Manager. It is applicable only if ProtectV Gateway is instantiated external to ProtectV Manager and occurs if the gateway enrollment token is invalid.	Use valid gateway enrollment token.
`Agent delete error`	Specified ProtectV Gateway for deletion is not valid. This is an internal error and does not occur if the gateway is deleted from the ProtectV Manager UI.	
`Client enroll error`	ProtectV Client could not be registered due to invalid image token.	Specify valid image enrollment token in the registration file.
`Client instance access denied`	A unauthentic instance tried to fetch client metadata.	Alert
`Client instance update error`	ProtectV Manager failed to update the client metadata when requested by a clone of the ProtectV Client. Likely reason is the failure of the database service.	Restart ProtectV Manager services by running the `pvmctl` command. Also, check disk space by running the `df` command. If disk is full, create a new ProtectV Manager instance, restoring database from this ProtectV Manager.
`Client update error`	ProtectV Manager failed to update the client metadata when requested by a ProtectV Client. Likely reason is the failure of the database service.	
`Error creating ACL`	ProtectV Manager failed to create ACL mapping key-ID to allowed client mapping. Likely reason is the failure of the database	

Event	Description	Remedy
	service.	
Gateway token create error	ProtectV Manager failed to create the gateway enrollment token.	
Key create error	ProtectV Manager failed to create key specific meta-structure. The client is not allowed to create key (not enrolled).	
KeySecure key create error	ProtectV Manager failed to create key on SafeNet KeySecure. KeySecure may be unreachable.	Ensure that KeySecure is up and running. If running, check activity and audit logs.
Key not found	Requested key is not found on SafeNet KeySecure. It can occur if the KeySecure administrator deleted keys from KeySecure.	Check the KeySecure audit and activity logs for any key deletion.
Key update error	ProtectV Manager failed to update the key metadata. The specified key is missing.	Check the KeySecure audit and activity logs for any key deletion.

Success/Information

The following table lists significant success and informational events logged by SafeNet ProtectV Manager.

Event	Description
`Agent create success`	ProtectV Gateway created successfully.
`Agent delete success`	ProtectV Gateway revoked. It can no longer be used by clients.
`Client create success`	ProtectV Client enrolled successfully.
`Client delete`	ProtectV Client removed from ProtectV Manager records. It will no longer be able to fetch keys from ProtectV Manager.
`Client instance update success`	A clone of client updated its metadata regarding partitions, access time, and so on.
`Client update`	A ProtectV Client updated its metadata regarding partitions, access time, and so on.
`Gateway token create`	A gateway enrollment token was created on ProtectV Manager, which can be used to enroll a new gateway. A gateway token is one-time usable only.
`Gateway token delete`	Remove an unused gateway enrollment token.
`Image enrollment token create`	An image enrollment token can be used to enroll a ProtectV Client. Once enrolled, ProtectV Client does not use the token.
`Image enrollment token delete`	Remove an image enrollment token.
`Key accessed`	ProtectV Manager provided requested key to ProtectV Client.
`Key ACL create`	Successful creation of a Key ACL allowing a client access to the key.
`Key ACL update`	A Key ACL was updated to allow clones of an instance to fetch key.
`Key created successfully`	A new key was created.
`Key update`	Key metadata was updated (for example, when key was accessed.)

CLI Login Events

This section provides format of CLI login event logs. The section also lists significant CLI login events redirected to the Syslog server.

Log Format

CLI login logs are displayed in the following format:

```
<TIMESTAMP> <HOSTIP> sshd[SSHID]: <MESSAGE>
```

Here,

- `<TIMESTAMP>`: Date and time when the log is generated.
- `<HOSTIP>`: IP address of the host machine where SSH is performed.
- `[SSHID]`: Random ID of the SSH session.
- `<MESSAGE>`: Event message.

Sample logs are:

```
Oct 12 08:19:40 54.89.128.83 sshd[30098]: pam_unix(sshd:session): session opened
for user pvadmin by (uid=0)

Oct 12 08:29:57 54.89.128.83 sshd[30192]: Accepted publickey for pvadmin from
42.99.164.65 port 26090 ssh2: RSA b1:98:b0:a9:7b:ee:8b:0f:9e:5b:c1:8c:0a:17:8e:75

Oct 12 08:29:57 54.89.128.83 sshd[30192]: pam_unix(sshd:session): session opened
for user pvadmin by (uid=0)

Oct 12 08:30:46 54.89.128.83 sshd[21455]: pam_unix(sshd:session): session closed
for user pvadmin

Oct 12 08:31:47 54.89.128.83 sshd[21580]: pam_unix(sshd:session): session closed
for user pvadmin

Oct 12 08:31:47 54.89.128.83 sshd[21603]: Received disconnect from 127.0.0.1: 11:
disconnected by user
```

Errors

The following table lists errors that are logged when attempts to log on to ProtectV Manager are unsuccessful.

Event	Description	Remedy
`pam_unix(sshd:auth): authentication failure; logname= uid=<uid> euid=<euid> tty=ssh ruser= rhost=<host machine IP> user=<user>`	Authentication has failed for the user.	Retry login attempt with valid credentials.
`Failed password for <user> from <host machine IP> port <port> ssh2`	Password of the user is incorrect.	Retry login attempt with correct password.
`Disconnecting: Too many authentication failures for <user> [preauth]`	Session will be closed due to multiple login attempts without success.	Contact your ProtectV Administrator. Retry login attempt with valid credentials.
`error: maximum authentication attempts exceeded for <user> from <host machine IP> port <port> ssh2 [preauth]`	User has exceeded the maximum allowed login attempts without success.	Contact your ProtectV Administrator. Retry after some time.
`error: Received disconnect from <host machine IP>: 14: No supported`	Possible reason is: • Incorrect user	Retry login attempt with correct user/key.

Event	Description	Remedy
`authentication methods available [preauth]`	• Incorrect key • No key specified when expected	

Success/Information

The following table lists success and informational messages that are logged when attempts to log on to ProtectV Manager are successful.

Event	Description
`Accepted password for <user> from <host machine IP> port <port> ssh2`	Password for the user trying to log on to ProtectV Manager is accepted. The message also shows the IP address (with port number) of the host machine from where the login attempt is made to send/receive requests.
`Accepted publickey for <user> from <host machine IP> port <port> ssh2: RSA <algorithm>`	Public key for the user trying to log on to ProtectV Manager is accepted. The message also shows the IP address (with port number) of the host machine from where the login attempt is made to send/receive requests.
`pam_unix(sshd:session): session opened for user <user> by (uid=<uid>)`	Session is opened for the user.
`pam_unix(sshd:session): session closed for user <user>`	Session is closed for the logged in user.

2
SafeNet ProtectV Client Logs

Introduction

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.

Errors

The following table lists error messages gathered in logs generated on SafeNet ProtectV Client:

Message	Description	Remedy
`Error - No PV Version file found`	ProtectV Client did not install correctly.	Reinstall ProtectV Client
`ERROR - system disk too small!`	System disk is less than 2 MB.	
`Failed root certificate request`	ProtectV Client could not fetch certificate of ProtectV Manager.	Check connectivity between ProtectV Manager and ProtectV Client. Ensure that ProtectV Manager is up and running.

`Failed gateway connection`
`Failed gateway certificate status check`
`Failed process gateway certificate request`
	ProtectV Client could not ensure that gateway certificate is valid.	Check if ProtectV Manager and gateway are up and running and gateway certificate is not revoked at ProtectV Manager.

Message	Description	Remedy
Gateway certificate not good		
Key not found for system partitions, retrying Key not found, retrying Too many failed attempts for get keys.	ProtectV Client could not get key for system partition.	Check ProtectV Manager logs for additional debugging.
Unable to protect system partiton	ProtectV Client cannot encrypt system partition due to absence of work disk.	Attach a raw disk of size greater than or equal to system partition, and reboot the client instance.

Success/Information

The following table lists success and informational messages gathered in logs generated on SafeNet ProtectV Client:

Message	Description
Retrieving current key for	ProtectV Client fetches key for a partition.
Creating a new key for	ProtectV Client requests key creation for a partition.
Retrieving new key for	ProtectV Client fetches new key in case of rekey.
Key refused for	ProtectV Manager refused key for a partition.
Rekeying immediately	Rekeying a partition.
Work disk for system disk is present	Temporary disk for making copy of system partition is attached.
Work disk for system disk not present	Temporary disk for making copy of system partition is not attached.
Found encrypted partition	A partition is found to be encrypted.
Processing system partitions	Encrypting/unlocking system partition.
Processing non-system partitions	Encrypting/unlocking data partitions.
Decrypting partition	Decrypting a partition (if configured on ProtectV Manager)
Copy Data part Copy System/Boot parts Copy System Only Copy XFS Only	Making a copy of partitions if these cannot be encrypted in-place.

Message	Description

`Restore Boot part`
`Restore Data part`
`Restore System part`
`Restore XFS part`
	Restoring partitions from temporary copies after repartitioning and encrypting.