Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

Configuration Guide for Gemalto SafeNet ProtectDB File SmartConnector

Document Release Date: February 2022
Software Release Date: February, 2022

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Configuration Guide for Gemalto SafeNet ProtectDB File SmartConnector

Configuration Guide for Gemalto SafeNet ProtectDB File SmartConnector

This guide provides information to install the SmartConnector for Gemalto SafeNet ProtectDB File and to configure the device for log file event collection.

Product Overview

SafeNet ProtectDB allows large amounts of sensitive data to be moved in and out of data stores by encrypting and decrypting specific fields in databases. The solution provides column-level encryption of structured, sensitive data, such as credit card numbers, social security numbers, national ID numbers, passwords, account numbers and balances, and email addresses.

Configuration

Event alerts inform you when certain events such as detection of a virus, software update, or disk space approaching capacity occur. You must define the events for which alerts are to be created in the ProtectDB console. Select **Administration** > **Alerts** > **Events**, in the ProtectDB console to define events. For more information, see the Gemalto SecureNet ProtectDB documentation.

Installing the SmartConnector

The following sections provide instructions to install and configure the SmartConnector.

Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

Preparing to Install the SmartConnector

(missing or bad snippet)(missing or bad snippet)

Installing and Configuring the SmartConnector

(missing or bad snippet)

1. Select **Gemalto SafeNet ProtectDB File** from the Type drop-down, then click **Next**.
2. Specify the following information:

Parameter	Description
Log File Name	Absolute path to the folder to which ProtectDB log files are written.
Version	Select the ProtectDB version from the drop-down list.

(missing or bad snippet)

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

ProtectDB v6 Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Additional data	copiedRecipient
Additional data	exploit
Additional data	list
Additional data	tag
Application Protocol	ProtocolType (HTTP, HTTPS, FTP, SMTP, POP3)
ArcSight Severity	Medium when Device Severity = Error; Low when Device Severity = Msg
Destination Address	DestIP
Destination User Name	MailRecipient
Device Custom Number 1	disk size in bytes
Device Custom String 1	FileName (Filter Name | Mail Message)
Device Custom String 2	FileType (Filter Type)
Device Custom String 3	Extended result
Device Custom String 4	Profile
Device Custom String 5	URL Category
Device Custom String 6	virus name
Device Event Class ID	Event
Device Product	'SafeNet ProtectDB'
Device Receipt Time	Date
Device Severity	Severity ('Msg' or 'Error')
Device Vendor	'Gemalto'
File Size	FileSize

ArcSight ESM Field	Device-Specific Field
File Type	FileType
Message	Event
Name	Event
Request Method	Method
Request URL	FileName
Source Address	SourceIP
Source Host Name	Source host name
Source Port	Source port
Source User Name	MailSender

ProtectDB v5 Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Application Protocol	ProtocolType
ArcSight Severity	Medium when Device Severity = Error; Low when Device Severity = Msg
Destination Address	DestIP
Destination User Name	MailRecipient
Device Custom Number 1	Message number
Device Custom String 1	FileName (Filter Name)
Device Custom String 2	FileType (Filter Type)
Device Custom String 3	Mail Sender
Device Custom String 4	Mail Recipient
Device Custom String 5	URLCategory
Device Custom String 6	Application filter name
Device Event Class ID	Event
Device Product	'SafeNet ProtectDB'
Device Receipt Time	Date
Device Severity	Severity
Device Vendor	'Gemalto'
File Name	FileName

ArcSight ESM Field	Device-Specific Field
File Size	FileSize
File Type	FileType
Message	Format or Pipeline
Name	Event
Request Method	Method
Request URL	FileName
Source Address	SourceIP
Source Host Name	Source host
Source Port	Source port
Source User Name	MailSender

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuration Guide for Gemalto SafeNet ProtectDB File SmartConnector (SmartConnectors 8.3.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!