Fortanix®

User Guide

DATA SECURITY MANAGER – INTEGRATION WITH EXTERNAL LOGGING SYSTEMS

VERSION 3.0

Fortanix Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | United States of America | ☎ +1 (650) 943-2484 |
✉ info@fortanix.com | 🌐 www.fortanix.com

TABLE OF CONTENTS

1.0 INTRODUCTION

This article describes how to integrate **Fortanix Data Security Manager (DSM)** with **External logging systems**. Fortanix DSM automatically maintains an internal audit log of system operations. You can configure Fortanix DSM to send these audit log entries to an external logging system. In this article you will learn how to send Fortanix DSM audit logs to the following external logging systems:

- Splunk
- Google Cloud's operations suite
- Syslog Server

1.1 NEED FOR EXTERNAL LOGGING

Typical enterprises have a requirement to collect and maintain logs of all systems including Fortanix DSM in a single place. Enterprises write rules with external logging systems such as Splunk, Google Cloud's operations suite, and Syslog to generate actions such as alerts, emails, and so on to match on a log or event. Fortanix DSM supports pushing logs/system events to Splunk, Google Cloud's operations suite, and Syslog for external logging.

2.0 DEFINITIONS

- **Fortanix Data Security Manager**

  Fortanix DSM is the cloud solution secured with Intel® SGX. With Fortanix DSM, you can securely generate, store, and use cryptographic keys and certificates, as well as secrets, such as passwords, API keys, tokens, or any blob of data.

- **Accounts**

  A Fortanix DSM account is the top-level container for security objects managed by the Fortanix DSM. An account is generally associated with an organization, rather than an individual. Security objects, groups, and applications belong to exactly one account. Different accounts are fully isolated from each other. *See support for more information.*

- **Fortanix Data Security Manager Security Objects**

  A security object is any datum stored in Fortanix DSM (for example a key, a certificate, a password, or other security objects). Each security object is assigned to exactly one group. Users and applications assigned to the group have permission to see the security object and to perform operations on it. *See support for more information.*

3.0 FORTANIX DATA SECURITY MANAGER LOGGING

NOTE: Only an Account Administrator can set up integration with external logging systems.

3.1 FORTANIX DATA SECURITY MANAGER AUDIT LOG

The Fortanix DSM external event logging is configured on a per account basis. Logs/events of an account is not visible to another account within an enterprise. Fortanix DSM automatically maintains an internal audit log of system operations. To view the audit log:

1. Click the **Audit Log** tab in the Fortanix DSM UI.

   For convenience, when viewing the details of a security object and other Fortanix DSM objects, the most recent audit log entries applicable to the object are shown in the right-hand pane in the detailed view of a security object.

3.2 SET RETENTION PERIOD FOR AUDIT LOG

By default, audit log entries older than 3 months are automatically deleted. The following steps describe how to set the retention period of audit logs for each account:

1. In the Fortanix DSM UI, click the **LOG MANAGEMENT** tab on the **Account Settings** page.
2. Click **EDIT** to set retention period for audit logs.
3. To permanently retain the audit logs, select the **Keep the logs forever** option or set it to a future date.
4. Click **SAVE** to save the changes.

NOTE:

- This setting can only be enabled if you have an Account Quorum policy configured with the **Log Management** option selected, since changes to the log management settings require account quorum approval.
- Audit logs that have already been forwarded to external log management integrations such as Syslog, Splunk, and so on will not be impacted because of this setting. This is applicable for all accounts including System administration audit logs.
- The retention period for audit logs can also be set from the **System Administration Settings** -> **Log management** page.

3.3 LOG INVALID API REQUESTS

Sometimes applications encounter invalid API requests that lead to 4XX errors, such as 400 (bad request) type error. To debug an application against 4XX errors, the Fortanix DSM enables audit logging for such errors using the Log Management feature. To enable this:

1. In the Fortanix DSM UI, go to **LOG MANAGEMENT** option in the **Account settings** page.
2. Enable the toggle for **Logging invalid API requests**.
3. To see the 4XX logs, click the **Audit Log** tab in the Fortanix DSM UI.

3.4 HIGH VOLUME SECURITY OBJECTS

In scenarios where a security object is used for cryptographic operations with very high usage, audit logging related to these operations can be explicitly disabled for the security object. This is the only scenario where audit logs can be disabled for an object.

NOTE: Audit logs related to only cryptographic operations are disabled. Logs related to key management operations on the security object are still enabled.

To disable the audit log on an existing security object:

1. Go to the detailed view of the object and click the toggle for audit logging to **disabled** mode.
2. If the group has a quorum policy set, then you will see "HIGHVOLUME" in the "**key operations permitted**" section of the "**Quorum approval request**" dialog box. The presence of HIGHVOLUME operation indicates that the audit log is requested to be disabled.

   To disable the audit log for a security object during object creation:

   a. Scroll to the bottom of the Security Object Create/Import page.

   b. Clear **Keep detailed log for the object** option.

3.5 LOG MANAGEMENT

Currently, Fortanix DSM supports the following logging systems:

- Splunk
- Google Cloud's operations suite
- Syslog

NOTE:

- Only an **Account Administrator** in Fortanix DSM can add the log management integrations with **Splunk**, **Google Cloud's operations suite**, and **Syslog**.

To integrate with the above logging systems, click the **Settings** tab in the Fortanix DSM UI left pane, and then click the **LOG MANAGEMENT** tab. It will give you three options for integration: Splunk, Google Cloud's operations suite, and Syslog. It is possible to have more than one integration active at the same time. Logs will be pushed from Fortanix DSM to all logging facilities that are configured.

3.6 SENDING AUDIT LOGS TO SPLUNK

You can configure Fortanix DSM to send audit log entries to a Splunk server using the HTTP Event Collector (HEC).

To configure logging events to Splunk,

1. Click the **Settings** icon in the Fortanix DSM UI.
2. Click the **LOG MANAGEMENT** tab from the left panel.
3. In the **Custom Log Management Integrations** section, click the **Add Integration** button for Splunk.
4. Configuring a Splunk integration requires the following information:
    a. Enter the IP Address or the hostname of your Splunk server.
        i. Select **Enable HTTPS** to communicate with the Splunk server over HTTPS (recommended) and also select the **Enable SSL checkbox** in the Splunk Global Settings. *Refer to the Appendix for the screenshot.*

        NOTE: If you are using an HTTP connection, then clear the **Enable HTTPS** checkbox in the Fortanix DSM **Log Management** screen and also clear the **Enable SSL** checkbox in the Splunk Global Settings. *Refer to the Appendix for the screenshot.*

        Depending on the type of TLS certificate the Splunk server is using:

        ii. Select **Global Root CAs** if you are using a certificate that is signed by a well-known public CA.

        iii. Select **Custom CA Certificate**, if you as an enterprise want to self-sign the certificate using your own internal CA. To do this, upload the CA certificate using the **UPLOAD A FILE** button. When Fortanix DSM as a client connects to the Splunk server and is

presented the server's certificate, it will be able to validate it using the enrolled custom CA Certificate. To generate the CA certificate, run the following command:

```
openssl s_client -connect <endoint/ipaddress>:port -showcerts
```

Where,

- `Ipaddress`: is the IP address of the Splunk server.
- `port`: is the value of the **Management port**, under **Server settings->General settings** in the Splunk Server. *Refer to the Appendix for the screenshot.*

iv. In case the Custom CA Certificate has a Common Name (CN) that does not match with the server in which Splunk is deployed, clear the **Validate Hostname** checkbox which prompts Fortanix DSM to ignore the hostname of the Splunk deployment instance. Only the certificate chain will be validated in this case.

b. The default **Port** number is **`80`**. If you are running on a different port, add the applicable port number. If you enable HTTPS in "*Step a*" above, then the default port number is **`443`**.

c. Add the name of the Splunk index in the **Index** field to submit events. The index value should be the same as the index in Splunk. *Refer to the Appendix for the screenshot*. When you push the logs to Splunk, you need to push it to a specific index. This value is sent to the Splunk server and can be set to whatever you like. This will allow distinguishing logs from different sources. For example, the logs from Fortanix DSM can be pushed to the Index source name **`SDKMS`**.

d. Enter a valid **Authentication token** to authenticate to the HTTP Event Collector of your Splunk instance. The Authentication token will authenticate Fortanix DSM as a client to Splunk and allows it to push the events to Splunk. See the Splunk documentation for detail about generating HEC authentication tokens.

NOTE: For security reasons, the authentication token is not displayed in the interface when editing an existing configuration.

5. Click **ADD INTEGRATION** to save the Splunk integration.

3.7 SENDING AUDIT LOGS TO GOOGLE CLOUD'S OPERATIONS SUITE

You can configure Fortanix DSM to send audit log entries to Google Cloud's operations suite.

1. To configure logging events to Google Cloud's operations suite, in the **Custom Log Management Integrations** section, click the **Add Integration** button for Google Cloud's operations suite.

   Configuring a Google Cloud's operations suite integration requires the following information:

   a. **Log ID** is the ID of the log to write to. **Log ID** must be a URL-encoded within the Log Name. Log Name is the resource name of the log to which this log entry belongs.
   For example,
   `organizations/1234567890/logs/cloudresourcemanager.googleapis.com%2Factivity`
   For more information, see Google Cloud's Operations Suite reference URL.

   b. Upload the **Service account key** or configuration file. To connect to Google Cloud's operations suite, you will need a configuration file that contains the Service account key and other information. Upload this configuration file using the **UPLOAD A FILE** button.

3.8 SENDING AUDIT LOGS TO SYSLOG

You can configure Fortanix DSM to send audit log entries to Syslog server.

To configure logging events to the Syslog, in the **Custom Log Management Integrations** section, click the **ADD INTEGRATION** button for Syslog.

- Configuring a Syslog management integration requires the following information:
  a. Enter the Host name or IP address of your Syslog server.
  b. You can communicate with a Syslog server either over a non-secure connection or a secure connection using TLS. Depending on the type of TLS certificate that the Syslog server is using,
     i. Select **Global Root CAs**, if you are using a certificate signed by a well-known public CA.

ii. Select **Custom CA Certificate**, if you as an enterprise want to self-sign the certificate using your own internal CA. To do this, upload the CA certificate using the **UPLOAD A FILE** button. When Fortanix DSM as a client connects to the Syslog server and is presented with the server's certificate, it will be able to validate it using the enrolled custom CA Certificate.

c. The default **Port** number is TCP `514` at which the server must listen for Syslog messages. If you are running on a different port, change to the applicable port number.

d. When you log an event in Syslog, you can choose to log it in different facilities. This allows you to filter your log for a specific facility. The facilities appearing in the **Facility** list are well-defined facilities in the Syslog protocol. For example: User, Local0, Local1, and so on. You can configure the Fortanix DSM system to use Local0 facility for instance. This will help in filtering logs from a particular appliance using a facility.

3.9 SENDING AUDIT LOGS TO RAPID7 INSIGHTIDR

For a detailed list of instructions on how to export the Fortanix DSM log files to the Rapid7 InsightIDR centralized log management utility, refer to Using Fortanix DSM with Rapid7 InsightIDR.

4.0 LOG STRUCTURE

A system event in Fortanix DSM generates a log that has the following components:

a. **Log Severity** – Severity of the message (Critical issues, Errors, Warnings, and Info). As of today, the backend for Logging only supports the Severities – "Info" and "Errors". A severity is logged as "Error" when logging requests have failed for some reason such as client error or internal server error. For all the other cases where the audit logs describe crypto operations, object updates and so on the severity is logged as "Info".

b. **Groups** – The Fortanix DSM group that the event belongs to.

c. **IP-Address** – This is the IP address of the client/user whose request triggered the log message. The client IP is recorded whenever it is available. For some logs, the IP-Address field might appear empty due to one of the following reasons:

- When Kubernetes is used for load balancing instead of an external load balancer, the Kubernetes reroutes requests and does not preserve the original client IP address. This is something Fortanix will address in the future.

- Since this was a new field introduced recently the older logs would have the IP_Address field empty.

d. **Apps/Users** – The log message can be a user event or application event.

e. **Time** – Timestamp of when the event occurred.

f. **Type** – Type of event (Administrative, Auth, and Crypto Operations).

- **Administrative** - Operations that users can perform such as importing/updating/deleting a key and creating/deleting/updating apps, groups, and accounts are classified as "Administrative" events.
- **Crypto Operation** – Operations such as generating/encrypting/decrypting/signing/verifying/wrapping/unwrapping a key are classified as "Crypto Operation" events.
- **Auth** – Operations such as logging in or logging out, applications authenticating to get a session or terminating their session are classified as "Auth" events.

When a log is pushed to a third-party external logging system, the log structure with all the log components above is sent to the server.

The format of a message logged on any external logging system is as follows:

```
<message string> acct_id=<corresponding account id> groups=[corresponding group ids] actor=<Actor type>:<Actor Id> obj=<Object Id> action=<Action Type>
```

Where,

- All the `ids` are UUID of the respective object
- `Actor types` can be User or App
- `Action types` can be Administrative, Auth, or Crypto Operation

For Example,

```
User "bob@company.com" created key "key_test" acct_id=8fb9b132-0b68-4d33-aba2-f1f9db3ab0e9 groups=[5f1d12e9-614a-4f5b-a4ed-837d9fb001b8]
```

```
actor=User:9dbd5192-ee09-46f6-89fd-812e96863aa4 obj=3da3bf54-610b-4e89-816d-
d4931f59f102 action=CRYPTOOPERATION
```

NOTE: Time and severity are set based on the logging system and they are not included in the actual message logged.

5.0 APPENDIX

Following are the Splunk Server screenshots-

- If you are using an HTTPS connection, then select the **Enable SSL** check box below in the Global Settings.

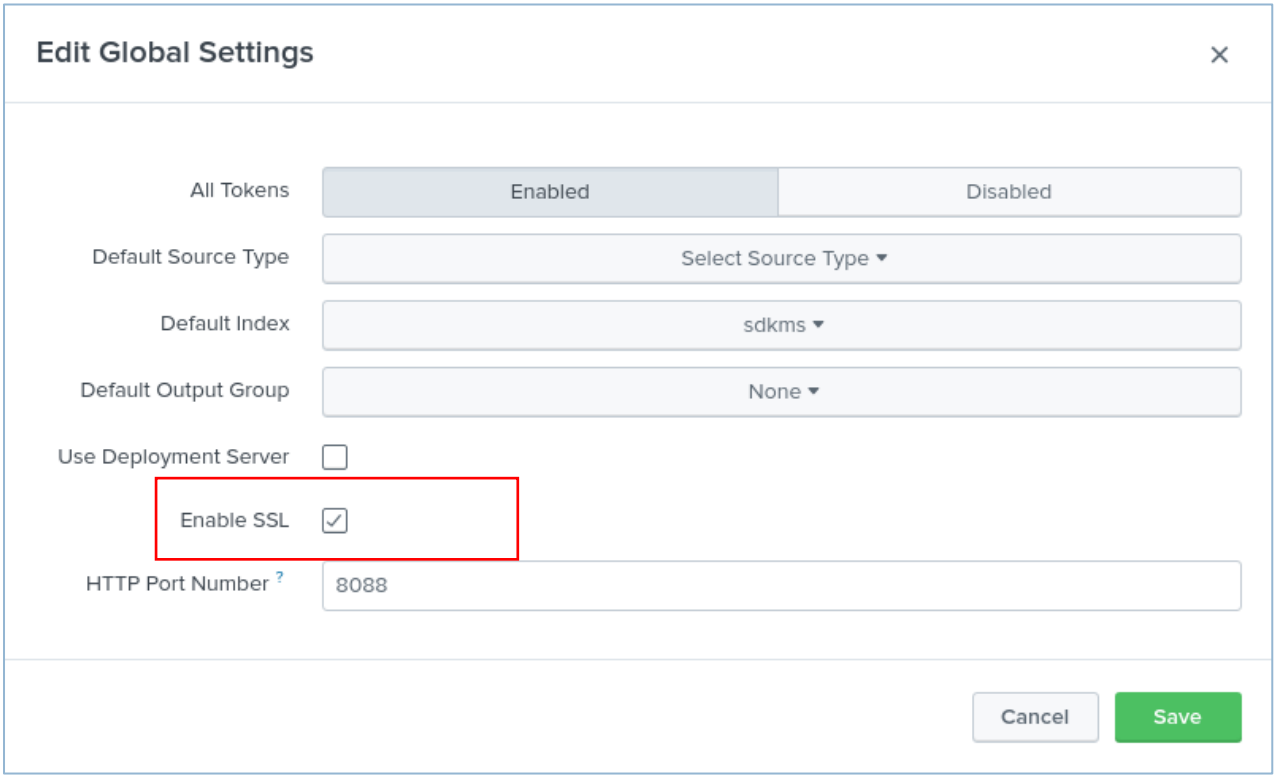

FIGURE 1: ENABLE SSL

- Port number on the Splunk server used for generating Custom CA Certificate.

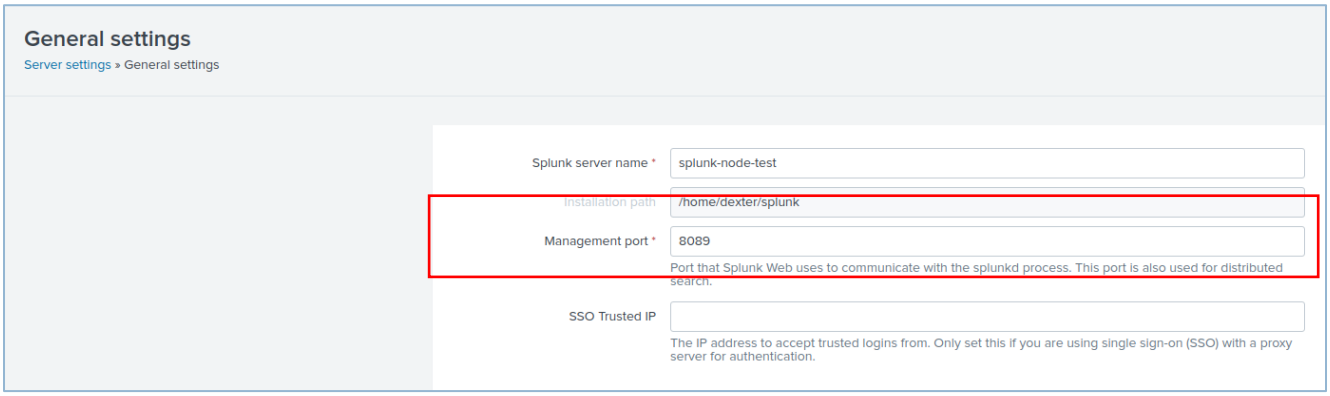

FIGURE 2: MANAGEMENT PORT NUMBER

- The index value in the Fortanix DSM Splunk Log Management Integration form should be the same as the Default Index value.

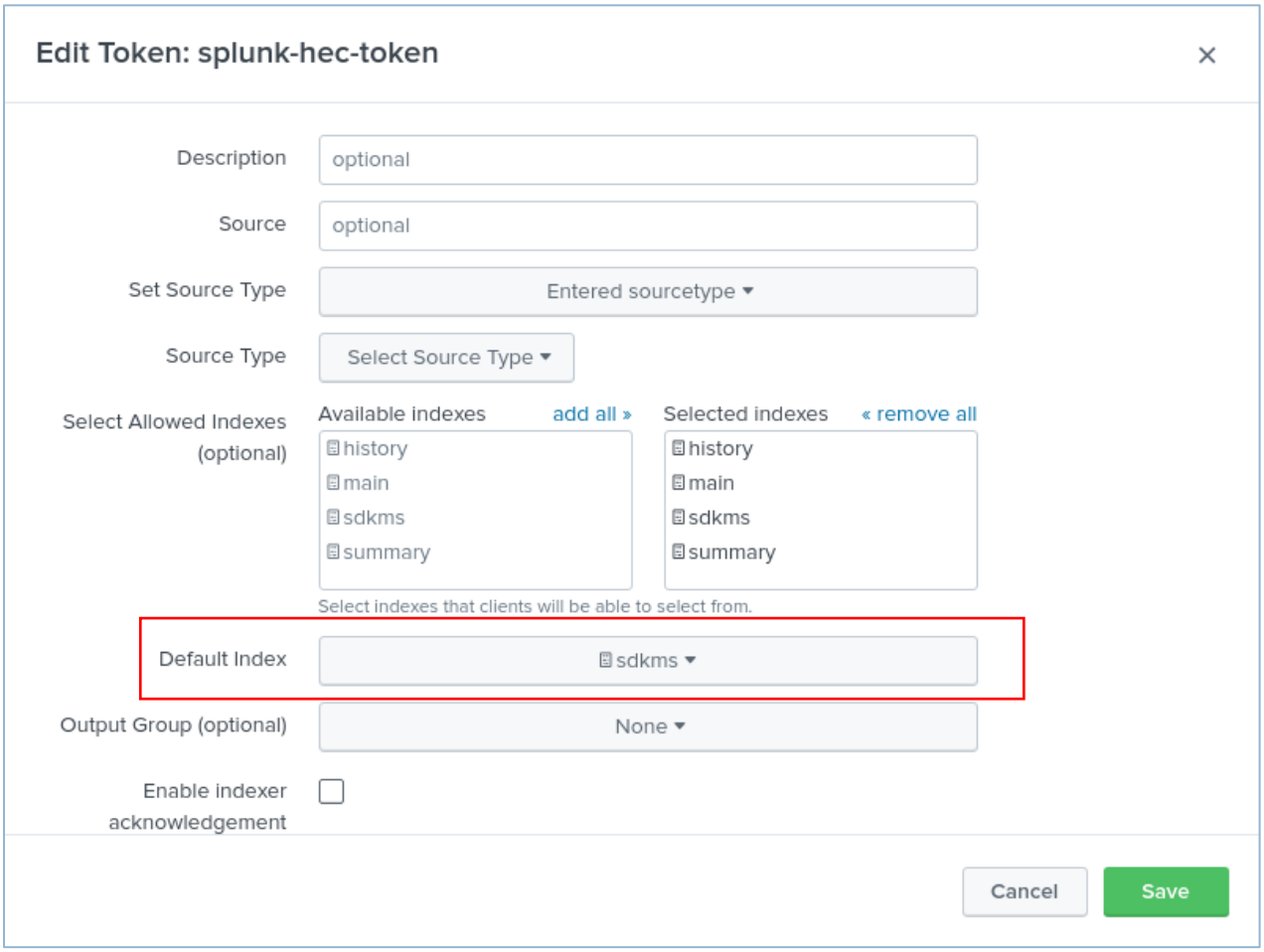

FIGURE 3: INDEX VALUE OF THE SPLUNK SERVER

6.0 DOCUMENT INFORMATION

6.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL:

https://support.fortanix.com/hc/en-us/articles/360016047631-User-s-Guide-Logging

6.2 DOCUMENT UPDATES

This document will typically be updated on a periodic review and update cycle.

For any urgent document updates, please send an email to: support@fortanix.com