User Guide

CONFIDENTIAL COMPUTING MANAGER – INTEGRATION WITH EXTERNAL LOGGING SYSTEMS

VERSION 2.0

TABLE OF CONTENTS

1.0 INTRODUCTION

This article describes how to integrate **Fortanix Confidential Computing Manager (CCM)** with **External logging systems**.

Fortanix CCM automatically maintains an internal audit log of system operations from different applications and services, and actions related to accounts, users and sessions.

The following events are logged:

- App Created
- App Updated
- App Updation Failed
- App Deleted
- App Certificate Downloaded
- App Creation Failed
- Node Enrolled
- Node Attested
- Node Attestation Failed
- Node Enrollment Failed
- Node Deactivated
- Node Certificate Downloaded
- Approve Domain
- Decline Domain
- Approve Image
- Decline Image
- Create Image
- Delete Image
- Image Conversion Succeeded
- Image Conversion Failed
- Certificate Requested by Application
- Create Registry
- Delete Registry
- Update Registry
- Node Reconnected

- Node Disconnected
- Configuration Creation

You can configure Fortanix CCM to send these audit log entries to an external logging system. In this article you will learn how to send Fortanix CCM audit logs to the following external logging systems:

- Splunk
- Azure Log Analytics
- Syslog Server

2.0 AUDIT LOGGING IN CONFIDENTIAL COMPUTING MANAGER

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

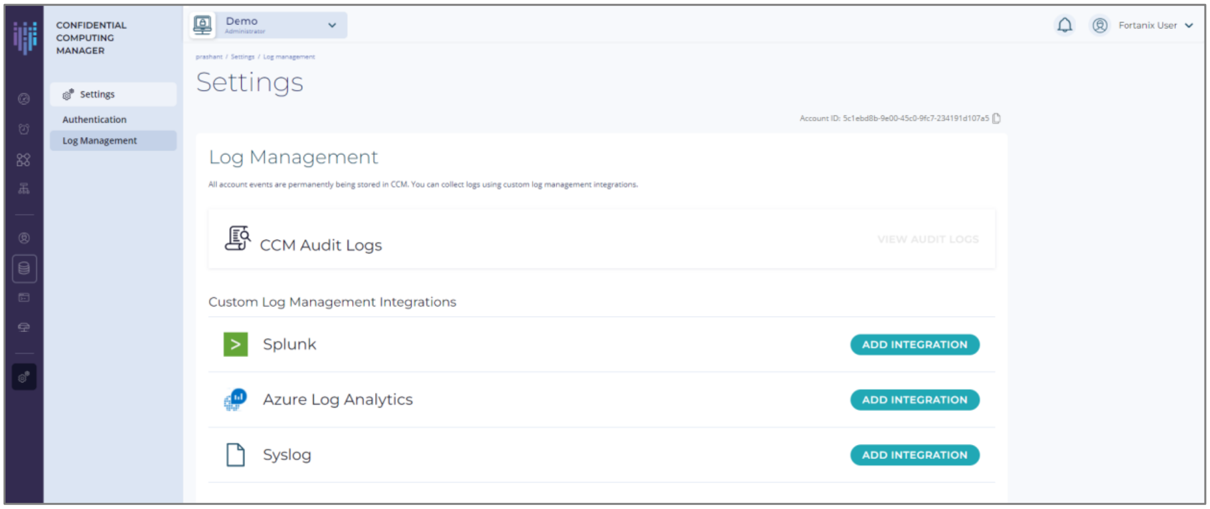
2.1 LOG MANAGEMENT

Currently, Fortanix CCM supports the following logging systems:

- Splunk
- Azure Log Analytics
- Syslog

NOTE: Only an **Account Administrator** in Fortanix CCM can set up integration with external logging systems like **Splunk**, **Azure Log Analytics**, and **Syslog**.

To integrate with the above logging systems, click the **Settings** menu item in the CCM UI left navigation bar, and then click the **Log Management** menu item. It will give you three options for integration: Splunk, Azure Log Analytics, and Syslog. It is possible to have more than one integration active at the same time. Logs will be pushed from Fortanix CCM to all logging facilities that are configured.



All account events are permanently being stored in CCM. You can collect logs using custom log management integrations.

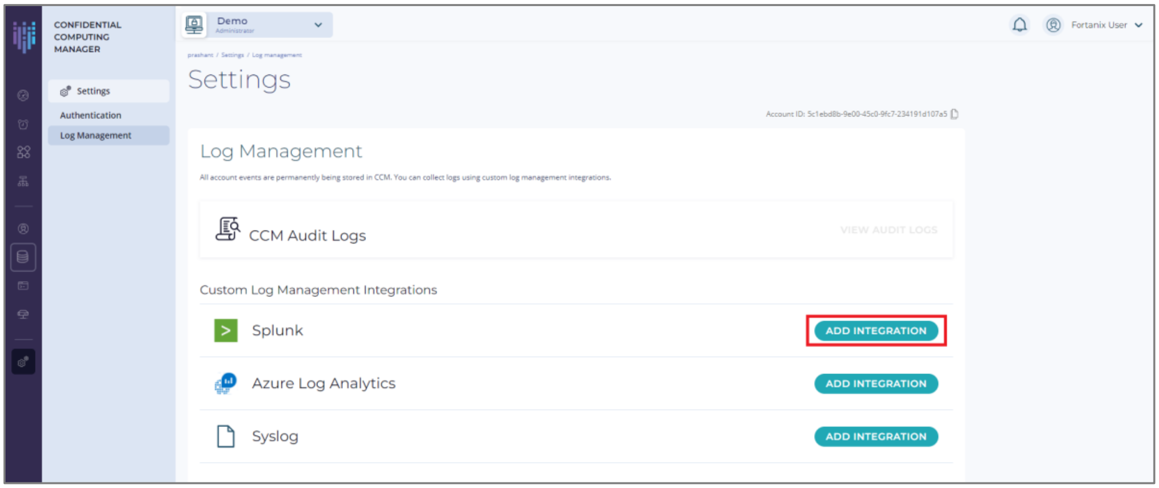
FIGURE 1: LOG MANAGEMENT

2.2 SENDING AUDIT LOGS TO SPLUNK

You can configure Fortanix CCM 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** → **Log Management** menu item from the CCM UI left navigation bar**.**
2. In the **Custom Log Management Integrations** section, click the **ADD INREGRATION** button for Splunk.



All account events are permanently being stored in CCM. You can collect logs using custom log management integrations.

FIGURE 2: ADD SPLUNK INTEGRATION

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

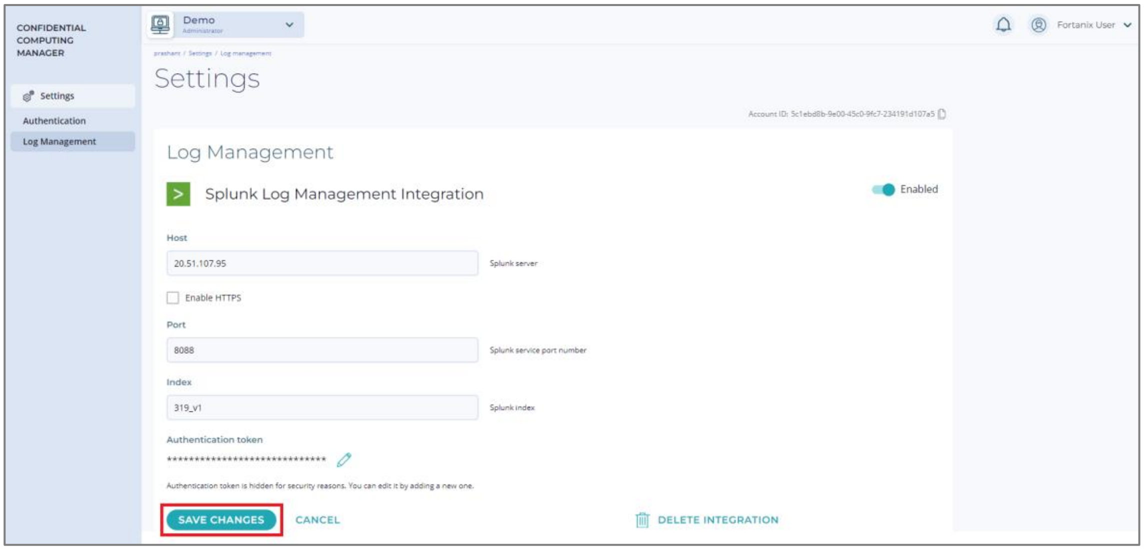
      iv. In case the Custom CA Certificate has a Common Name (CN) that does not match with the server in which Splunk is deployed, clear the **Validate Hostname** checkbox which prompts Fortanix CCM to ignore the hostname of the Splunk deployment instance. Only the certificate chain will be validated in this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

d. Enter a valid **Authentication token** to authenticate to the HTTP Event Collector of your Splunk instance. The Authentication token will authenticate Fortanix CCM 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.



Account ID: 5c1ebd8b-9e00-45c0-9fc7-234191d107a5

Log Management

Splunk Log Management Integration — Enabled

Host: 20.51.107.95 — Splunk server

☐ Enable HTTPS

Port: 8088 — Splunk service port number

Index: 319_v1 — Splunk index

Authentication token: ****************************

Authentication token is hidden for security reasons. You can edit it by adding a new one.

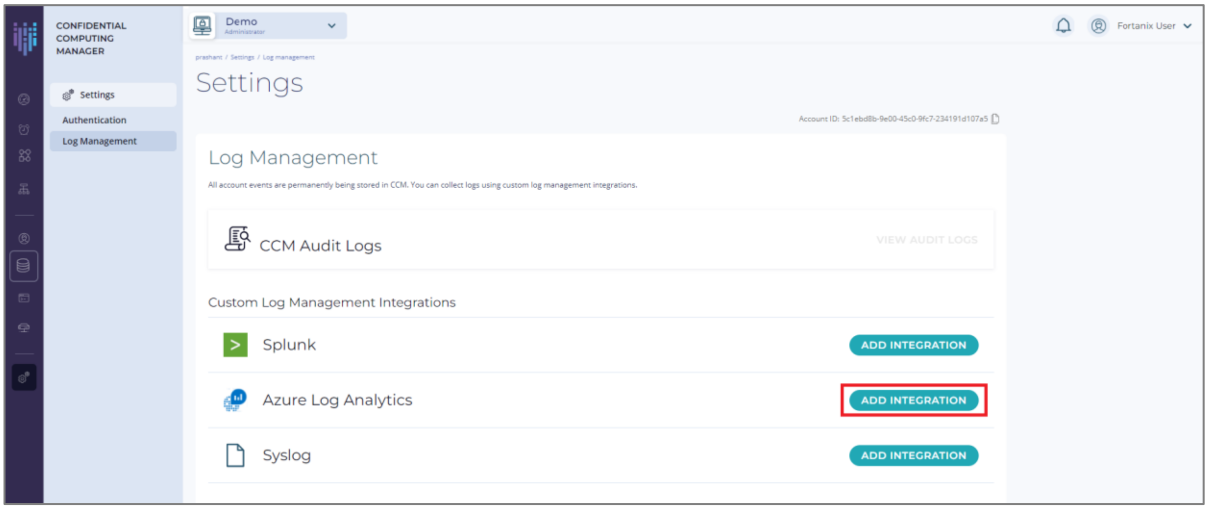
FIGURE 3: SPLUNK LOG MANAGEMENT INTEGRATION FORM

4. Click **SAVE CHANGES** to save the Splunk integration.

2.3 SENDING AUDIT LOGS TO AZURE LOG ANALYTICS

You can configure Fortanix CCM to send audit log entries to Azure Log Analytics in the Azure Portal to write log queries and interactively analyse the Fortanix CCM log data.

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



CONFIDENTIAL COMPUTING MANAGER
Settings
Authentication
Log Management
Demo
Administrator
Fortanix User
prashant / Settings / Log management

Settings

Account ID: 5c1ebd8b-9e00-45c0-9fc7-234191d107a5

Log Management

All account events are permanently being stored in CCM. You can collect logs using custom log management integrations.

CCM Audit Logs — VIEW AUDIT LOGS

Custom Log Management Integrations

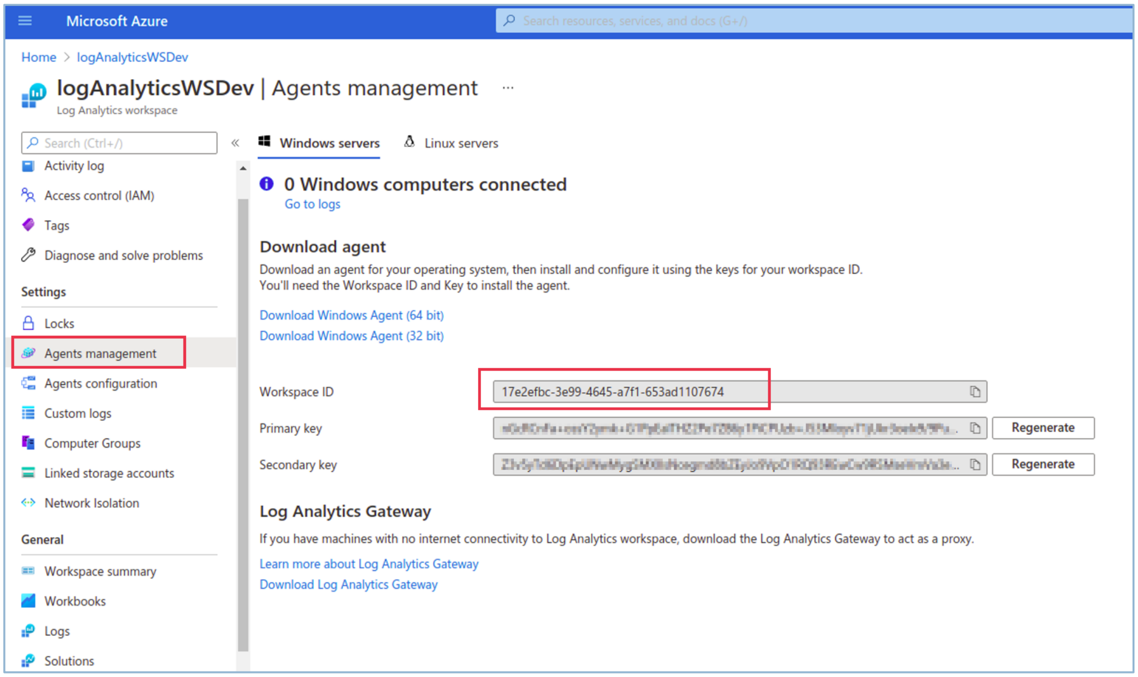
Splunk — ADD INTEGRATION

Azure Log Analytics — ADD INTEGRATION

Syslog — ADD INTEGRATION

FIGURE 4: ADD INTEGRATION FOR AZURE LOG ANALYTICS

1. Configuring an Azure Log Analytics integration requires the following information:
   a. Enter the **Workspace ID** which is the Log Analytics workspace in the Azure portal. It is a GUID to identify the specific log analytics workspace in the Azure cloud. To create a log-analytics workspace refer to https://docs.microsoft.com/en-us/azure/azure-monitor/logs/quick-create-workspace. To get the Workspace ID after you create a log-analytics workspace:
      i. In the log analytics workspace, click the **Agents management** tab to see the **Workspace ID**.



0 Windows computers connected
Go to logs

Download agent

Download an agent for your operating system, then install and configure it using the keys for your workspace ID.
You'll need the Workspace ID and Key to install the agent.

Download Windows Agent (64 bit)
Download Windows Agent (32 bit)

Workspace ID: 17e2efbc-3e99-4645-a7f1-653ad1107674
Primary key: [redacted] Regenerate
Secondary key: [redacted] Regenerate

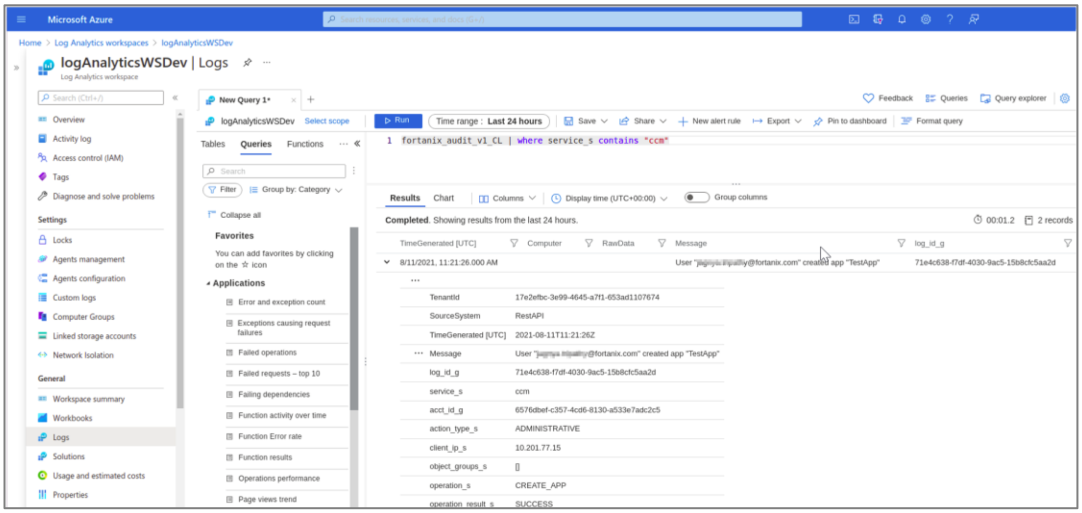
Log Analytics Gateway

If you have machines with no internet connectivity to Log Analytics workspace, download the Log Analytics Gateway to act as a proxy.

Learn more about Log Analytics Gateway
Download Log Analytics Gateway

FIGURE 5: WORKSPACE ID

b. The **Custom Log Type** is set to "`fortanix_audit_v1_CL`" for all event logs published to Azure Log collector from Fortanix services. This field is set in `HTTP POST` request header of all the logs published to the Azure log collector and therefore it is used to query logs from Fortanix services in Azure Log Analytics Workspace. For more details refer to https://docs.microsoft.com/en-us/azure/azure-monitor/logs/queries.



Time range : Last 24 hours

```
fortanix_audit_v1_CL | where service_s contains "ccm"
```

Completed. Showing results from the last 24 hours. 00:01.2 2 records

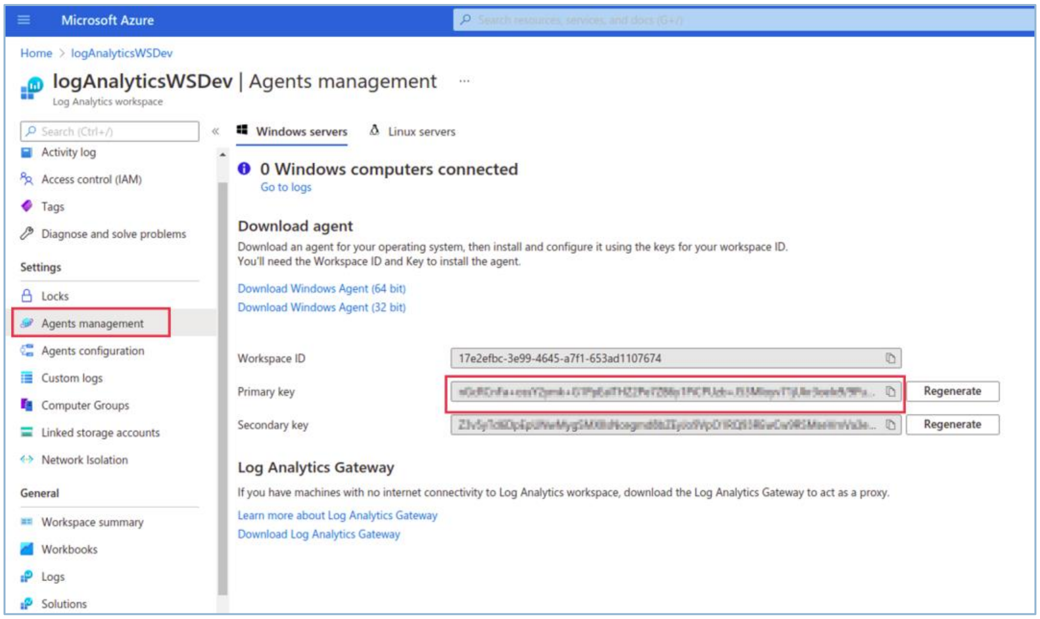
TimeGenerated [UTC]	Computer	RawData	Message	log_id_g
8/11/2021, 11:21:26.000 AM			User "[redacted]@fortanix.com" created app "TestApp"	71e4c638-f7df-4030-9ac5-15b8cfc5aa2d

TenantId	17e2efbc-3e99-4645-a7f1-653ad1107674
SourceSystem	RestAPI
TimeGenerated [UTC]	2021-08-11T11:21:26Z
Message	User "[redacted]@fortanix.com" created app "TestApp"
log_id_g	71e4c638-f7df-4030-9ac5-15b8cfc5aa2d
service_s	ccm
acct_id_g	6576dbef-c357-4cd6-8130-a533e7adc2c5
action_type_s	ADMINISTRATIVE
client_ip_s	10.201.77.15
object_groups_s	[]
operation_s	CREATE_APP
operation_result_s	SUCCESS

FIGURE 6: CCM EVENT LOG QUERY

c. Click **ADD PRIMARY SHARED KEY** to add a shared key. Any request to the Azure Monitor HTTP Data Collector API must include an authorization header. Each event log posted to azure log analytics workspace from the logging service is authenticated by the log monitor service in azure by validating the request and checking whether it is signed with either the primary or the secondary key for the workspace that is making the request. To get the Primary Shared Key:

i. In the log analytics workspace, click the **Agents management** menu item to see the **Primary key**. The Primary key of the log-analytics workspace is referred as `shared_key`.



0 Windows computers connected

Go to logs

Download agent

Download an agent for your operating system, then install and configure it using the keys for your workspace ID. You'll need the Workspace ID and Key to install the agent.

Download Windows Agent (64 bit)

Download Windows Agent (32 bit)

Workspace ID: 17e2efbc-3e99-4645-a7f1-653ad1107674

Primary key: [redacted] Regenerate

Secondary key: [redacted] Regenerate

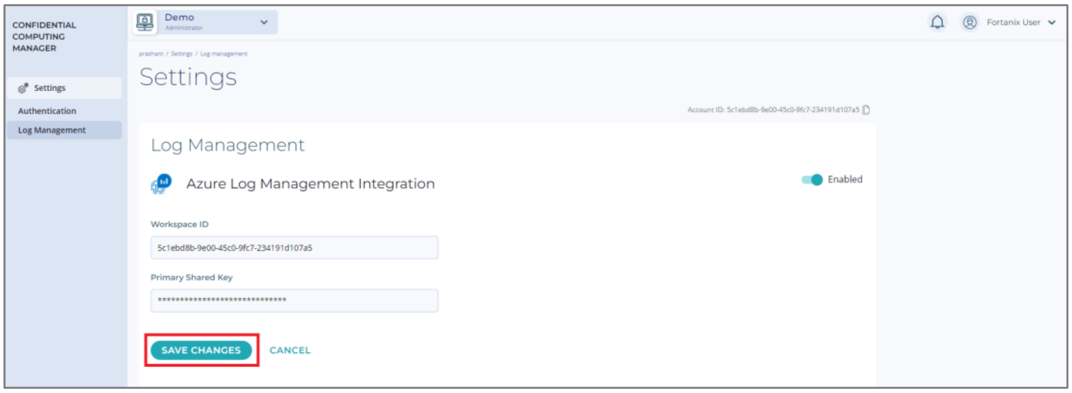
Log Analytics Gateway

If you have machines with no internet connectivity to Log Analytics workspace, download the Log Analytics Gateway to act as a proxy.

Learn more about Log Analytics Gateway

Download Log Analytics Gateway

FIGURE 7: PRIMARY SHARED KEY



CONFIDENTIAL COMPUTING MANAGER
Settings
Authentication
Log Management
Demo
Administrator
Fortanix User
prashant / Settings / Log management

Settings

Account ID: 5c1ebd8b-9e00-45c0-9fc7-234191d107a5

Log Management

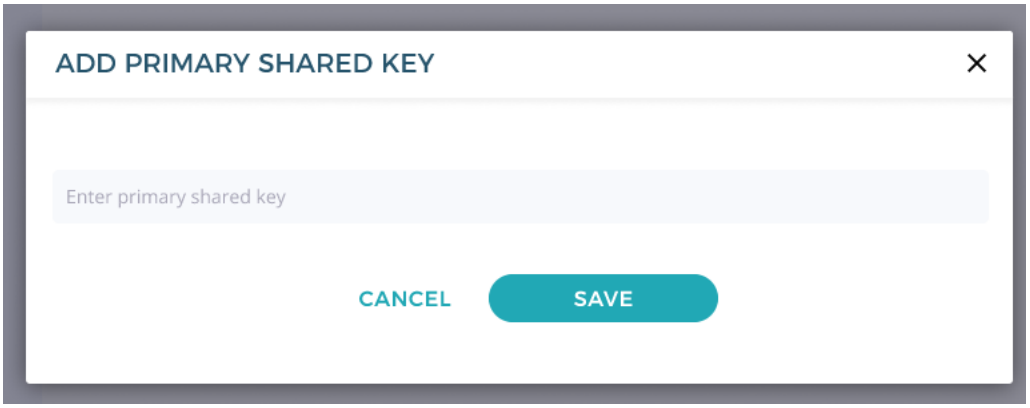
Azure Log Management Integration — Enabled

Workspace ID: 5c1ebd8b-9e00-45c0-9fc7-234191d107a5

Primary Shared Key: ******************************

SAVE CHANGES   CANCEL

FIGURE 8: CONFIGURE AZURE LOG ANALYTICS



ADD PRIMARY SHARED KEY

FIGURE 9: ADD PRIMARY SHARED KEY

📌 **NOTE:** For security reasons, the Primary Shared Key is not displayed in the interface when editing an existing shared key.

2. Click **SAVE CHANGES** to save the Azure Log Analytics integration.

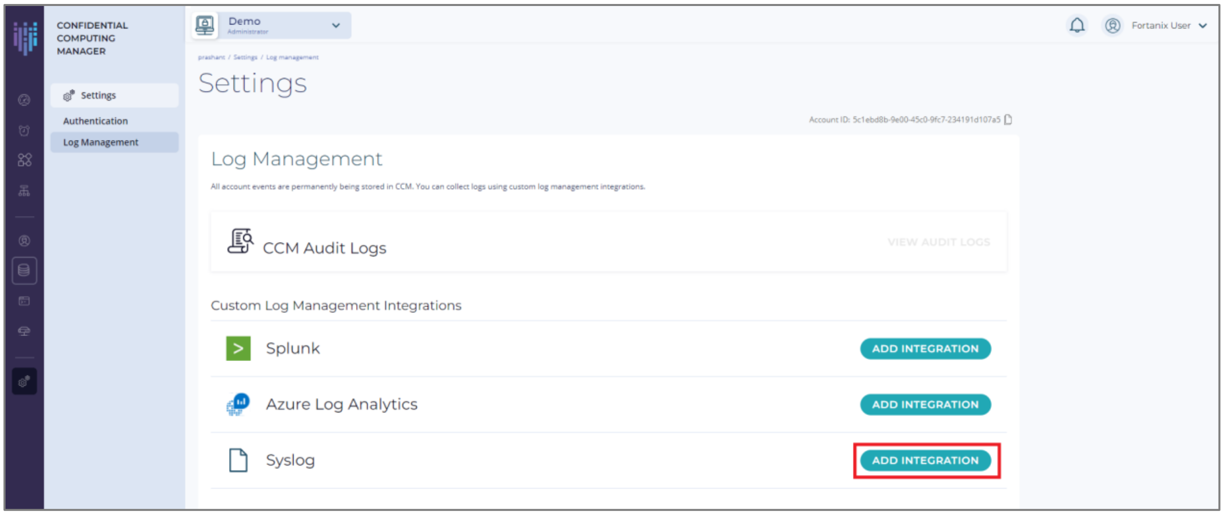
2.3.1 REFERENCES

- Create log-analytics workspace: https://docs.microsoft.com/en-us/azure/azure-monitor/logs/quick-create-workspace. *In the URL refer to the section: **Create a workspace***.
- Create log-analytics workspace using CLI - https://docs.microsoft.com/en-us/azure/azure-monitor/logs/quick-create-workspace-cli. *In the URL refer to the sections: **Prerequisites** and **Create a workspace***.
- Monitoring logs: https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-overview.
- Querying logs: https://docs.microsoft.com/en-us/azure/azure-monitor/logs/queries.

2.4 SENDING AUDIT LOGS TO SYSLOG

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

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


CONFIDENTIAL COMPUTING MANAGER
Settings
Authentication
Log Management
Demo
Administrator
Fortanix User
prashant / Settings / Log management

Settings

Account ID: 5c1ebd8b-9e00-45c0-9fc7-234191d107a5

Log Management

All account events are permanently being stored in CCM. You can collect logs using custom log management integrations.

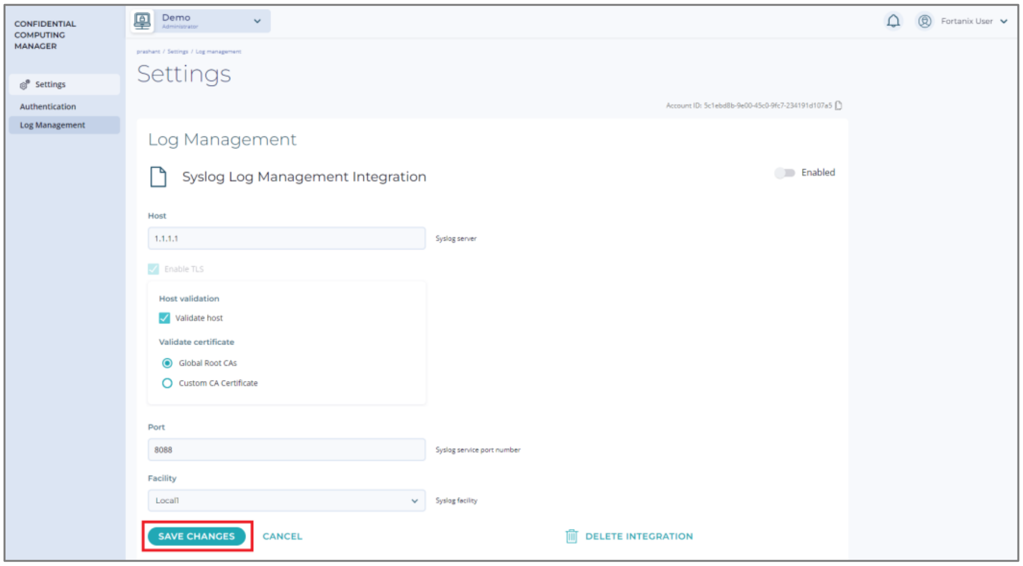
CCM Audit Logs VIEW AUDIT LOGS

Custom Log Management Integrations

Splunk	ADD INTEGRATION
Azure Log Analytics	ADD INTEGRATION
Syslog	ADD INTEGRATION

FIGURE 10: ADD SYSLOG INTEGRATION

1. Configuring a Syslog management integration requires the following information:
   a. Enter the Hostname 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 that is 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 CCM 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 CCM system to use the Local0 facility for instance. This will help in filtering logs from a particular appliance using a facility.



Settings

Account ID: 5c1ebd8b-9e00-45c0-9fc7-234191d107a5

Log Management

Syslog Log Management Integration — Enabled

Host: 1.1.1.1 — Syslog server

☑ Enable TLS

Host validation

☑ Validate host

Validate certificate

● Global Root CAs

○ Custom CA Certificate

Port: 8088 — Syslog service port number

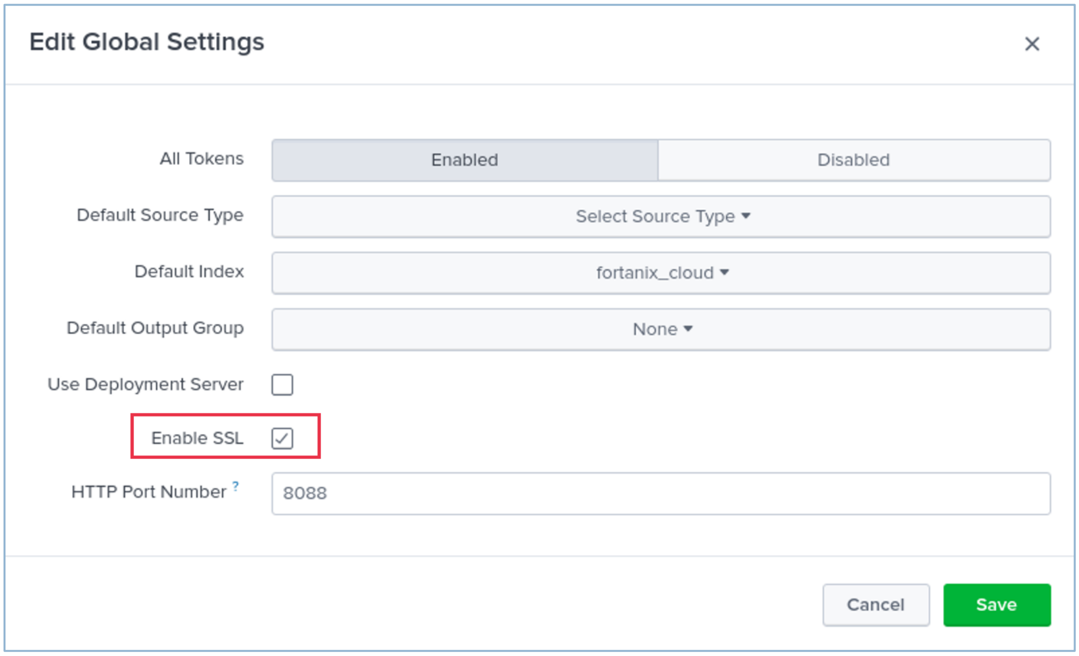
Facility: Local1 — Syslog facility

Figure 11: Syslog Integration Form

3.0 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.

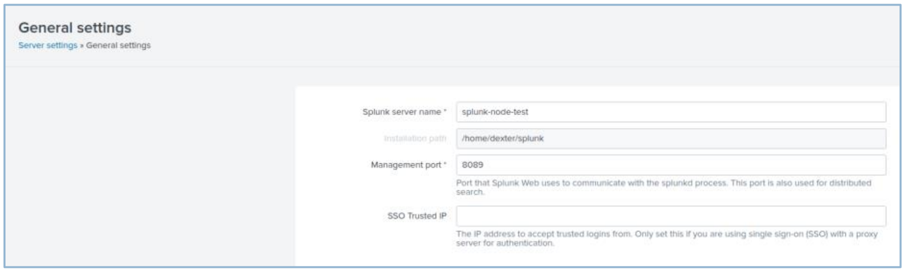


Edit Global Settings

All Tokens	Enabled / Disabled
Default Source Type	Select Source Type ▾
Default Index	fortanix_cloud ▾
Default Output Group	None ▾
Use Deployment Server	□
Enable SSL	☑
HTTP Port Number ?	8088

Figure 12: Enable SSL

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



General settings

Server settings » General settings

Splunk server name * splunk-node-test

Installation path /home/dexter/splunk

Management port * 8089

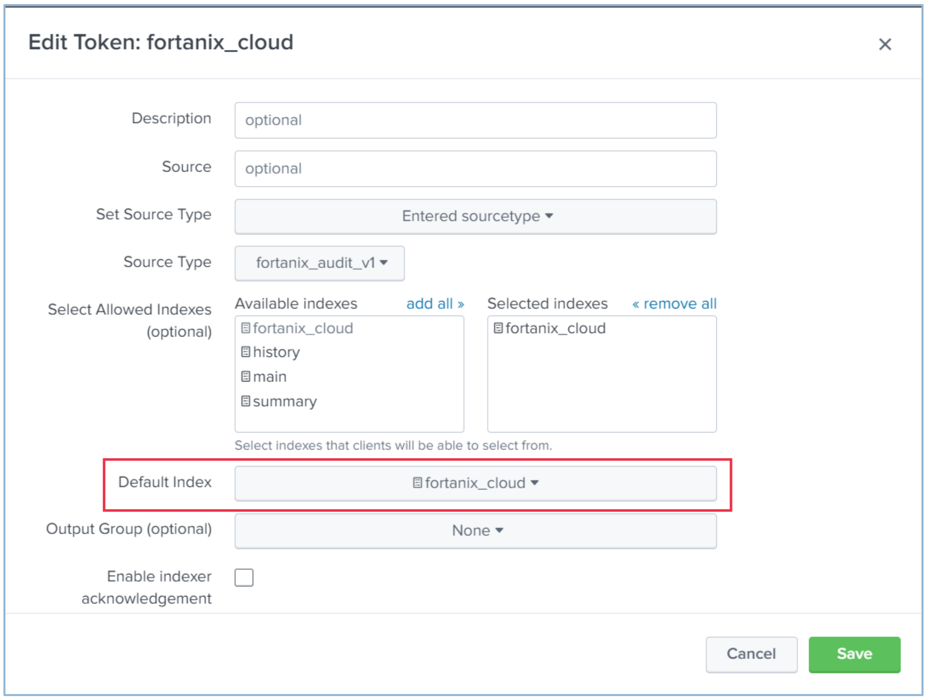
Port that Splunk Web uses to communicate with the splunkd process. This port is also used for distributed search.

SSO Trusted IP

The IP address to accept trusted logins from. Only set this if you are using single sign-on (SSO) with a proxy server for authentication.

FIGURE 13: MANAGEMENT PORT NUMBER

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



Edit Token: fortanix_cloud

Description	optional
Source	optional
Set Source Type	Entered sourcetype
Source Type	fortanix_audit_v1
Select Allowed Indexes (optional)	Available indexes: fortanix_cloud, history, main, summary Selected indexes: fortanix_cloud Select indexes that clients will be able to select from.
Default Index	fortanix_cloud
Output Group (optional)	None
Enable indexer acknowledgement	□

FIGURE 14: INDEX VALUE OF THE SPLUNK SERVER

4.0 DOCUMENT INFORMATION

4.1 DOCUMENT LOCATION

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

https://support.fortanix.com/hc/en-us/articles/4405381586708-User-s-Guide-Logging

4.2 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

NOTICE: This document was produced by Fortanix, Inc. (Fortanix) and contains information which is proprietary and confidential to Fortanix. The document contains information that may be protected by patents, copyrights, and/or other IP laws. If you are not the intended recipient of this material, please destroy this document and inform info@fortanix.com immediately.