

Integrations

SymantecCloudSecurity

V5.0.1

CONTENTS

1	Symantec Cloud Security	1
2	Installing Symantec Cloud Security	2
3	Configuring Symantec Cloud Security	3
3.1	Adding a Normalization Policy	3
3.2	Configuring Symantec Cloud Security Fetcher	5
4	Accessing Symantec Cloud Security Logs	9
5	Uninstalling Symantec Cloud Security	10

SYMANTEC CLOUD SECURITY

Symantec Cloud Security enables you to fetch and analyze *Symantec Web Security Service* logs.

Symantec Cloud Security Components:

1. Fetcher

- SymantecCloudSecurityFetcher

2. Compiled Normalizer

- SymantecCloudSecurityCompiledNormalizer

INSTALLING SYMANTEC CLOUD SECURITY

Prerequisite

Logpoint v6.7.0 or later

Installing Symantec Cloud Security in Logpoint

1. Go to *Settings >> System >> Applications*.
2. Click **Import**.
3. **Browse** for the location of the downloaded .pak file.
4. Click **Upload**.

After installing Symantec Cloud Security, you can find the installed plugins under *Settings >> System >> Plugins*.

CONFIGURING SYMANTEC CLOUD SECURITY

3.1 Adding a Normalization Policy

1. Go to *Settings >> Configuration >> Normalization Policies*.
2. Click **Add**.
3. Enter a **Policy Name**.
4. Select **SymantecCloudSecurityCompiledNormalizer**.
5. Click **Submit**.

CREATE NORMALIZATION POLICY

NORMALIZATION POLICY INFORMATION

Policy Name:

Compiled Normalizer:

Available

Search

A10WAFCompiledNormalizer
ADFSNormalizer
ARPGuardCompiledNormalizer
ApacheHTTPServerCompiledNormalizer
ArubaClearPassCompiledNormalizer
ArubaOSCompiledNormalizer
BitDefenderCompiledNormalizer
CEFCCompiledNormalizer
CentrifyCompiledNormalizer

Selected

Search

SymantecCloudSecurityCompiledNormalizer

Normalization Packages:

Available

Search

LP_A10 Web Application Firewall
LP_AIX Generic
LP_AIX v7_1
LP_ARP Guard
LP_Activtrak
LP_Airlock WAF
LP_Airlock WAF Generic

Selected

Search

View Signatures

Submit

Cancel

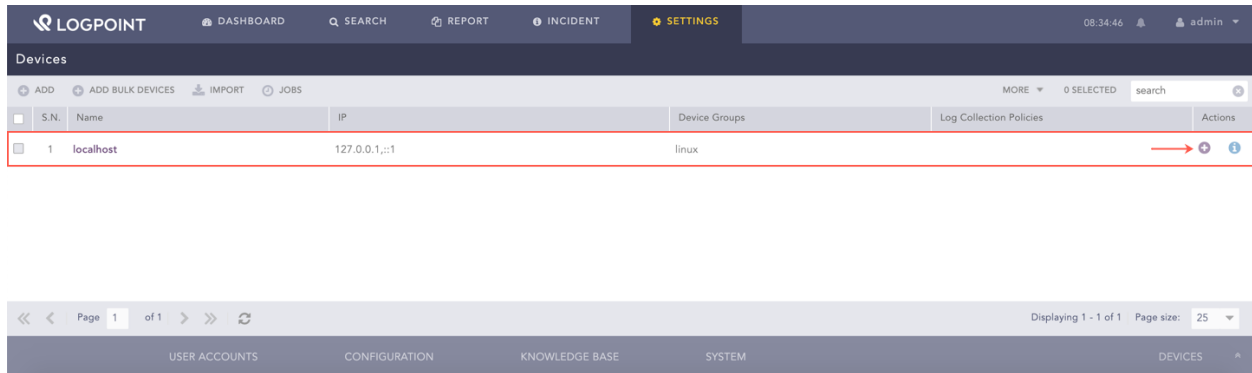
Fig. 1: Adding a Normalization Policy

3.1. Adding a Normalization Policy

4

3.2 Configuring Symantec Cloud Security Fetcher

1. Go to *Settings >> Configuration >> Devices*.
2. Click **Add collectors/fetchers** (+) under **Actions** of the *localhost* device.



3. Click **SymantecCloud Fetcher**.

AVAILABLE COLLECTORS FETCHERS			
FTP Fetcher 0	LogPoint Agent Collector 0	Mitel Fetcher 0	ODBC Fetcher 0
OPSEC Fetcher 0	Salesforce Fetcher 0	SCP Fetcher 0	SCP Fetcher Lite 0
SDEE Fetcher 0	SFlow Collector 0	Snare Collector 0	SNMP Fetcher 0
SNMP Trap Collector 0	SymantecCloud Fetcher 1	Syslog Collector 1	Syslog Forwarder File Fetcher 0
Vulnerability Management 2	WMI Fetcher 0		

Fig. 2: Available Collectors Fetchers

4. Click **Add**.

SYMANTECCLOUDSECURITY FETCHER

+ ADD MORE 0 SELECTED search

S.N.	Username	Start Date	End Date	Fetch Interval	Actions
------	----------	------------	----------	----------------	---------

Page 0 of 0 No data to display Page size: 25

Fig. 3: SymantecCloudSecurity Fetcher

5. Enter your API credentials of *Symantec Web Security Service* in **Username** and **Password**.
6. Select the **Fetch Interval** in minutes.
7. Select the **Start Date**. Symantec Cloud Security fetches logs from the specified date.
8. Select the **End Date**. Symantec Cloud Security fetches logs until the specified date.
9. Select a **Processing Policy** that uses the previously created *normalization policy*.
10. Select the **Charset**.
11. Select **Enable Proxy** to use a proxy server.
12. In **Proxy Configuration**:
 - 12.1 Enter the **IP address** and the **Port** number of the proxy server.
 - 12.2 Select **HTTP** or **HTTPS** protocol as required.
13. Click **Submit**.

SYMANTECCLOUDSECURITY FETCHER

SYMANTECCLOUDSECURITY FETCHER

Username:

Password:

••••••

Show

Fetch Interval:

70

Start Date:

11/12/2019

End Date:

12/12/2019

Processing Policy:

symantec

Charset:

utf_8

☒ Enable Proxy

Proxy Configuration

IP/Port:

192.168.1.1

4

Protocol:

☒ HTTP

☐ HTTPS

Submit

Cancel

Fig. 4: Adding a New Configuration for SymantecCloud Fetcher

ACCESSING SYMANTEC CLOUD SECURITY LOGS

Use the following search query to access the logs fetched by Symantec Cloud Security:

`col_type = symanteccloud`

The screenshot shows the Logpoint web interface. At the top, there's a navigation bar with 'LOGPOINT', 'DASHBOARD', 'SEARCH', 'REPORT', 'INCIDENT', and 'SETTINGS'. The 'SEARCH' tab is active. Below the navigation bar, a search query 'col_type=symanteccloud' is entered. The interface shows 'Found 455,805 logs'. On the left, there's a sidebar with 'Interesting Fields' and a table listing fields like 'transaction_uuid', 'location', 'col_type', and 'cs_client_ip_country' with their respective counts. The main area displays a log entry for '2019/11/08 09:53:17' with detailed fields such as 'log_ts', 'device_ip', 'device_name', 'col_type', 'source_address', 'destination_address', 'destination_port', 'sig_id', 'repo_name', 'status_code', 'action', 'domain', 'protocol', 'category', 'application', 'request_method', 'received_data_size', 'sent_data_size', 'access_type', 'appliance', 'authentication_group', 'col_ts', 'collected_at', 'cs_client_ip_country', 'cs_icap_status', 'date', 'device_category', 'duration', 'location', 'logpoint_name', 'norm_id', 'operation', 'outbound_server_address', 'path', 'r_supplier_country', 'result', 'rs_connection_negotiated_cipher', 'rs_icap_status', 's_supplier_country', 'supplier_address', 'tenant_id', 'threat_level', 'time', 'transaction_uuid', 'user_dn', and 'ou'.

Fig. 1: Symantec Cloud Security Log

UNINSTALLING SYMANTEC CLOUD SECURITY

1. Go to *Settings >> System >> Applications*.
2. Click on **Uninstall** (🗑️) from **Actions**.

Note: You must remove Symantec Cloud Security Fetcher configuration to delete Symantec Cloud Security.
