

# Integrations

## SymantecCloudSecurity

V5.1.1 (latest)

# CONTENTS

<b>1</b>	<b>Symantec Cloud Security</b>	<b>1</b>
<b>2</b>	<b>Installing Symantec Cloud Security</b>	<b>2</b>
<b>3</b>	<b>Uninstalling Symantec Cloud Security</b>	<b>3</b>
<b>4</b>	<b>Configuring Symantec Cloud Security</b>	<b>4</b>
4.1	Configuring a Repo for Symantec Cloud Security . . . . .	4
<b>5</b>	<b>Accessing Symantec Cloud Security Logs</b>	<b>10</b>
<b>6</b>	<b>Expected Log Sample</b>	<b>11</b>

## SYMANTEC CLOUD SECURITY

Symantec Cloud Security enables you to fetch and analyze *Symantec Web Security Service* logs. *SymantecCloudSecurityCompiledNormalizer* is compatible with [CNDP](#).

### **Supported Devices/Sources**

Symantec Web Security Service

### **Symantec Cloud Security Components:**

#### **1. Fetcher**

- *SymantecCloudSecurityFetcher*

#### **2. Compiled Normalizer**

- *SymantecCloudSecurityCompiledNormalizer*

## INSTALLING SYMANTEC CLOUD SECURITY

### Prerequisite

Logpoint v7.8.0

### To install Symantec Cloud Security:

1. Download the .pak file from the [Help Center](#).
2. Go to *Settings >> System Settings* from the navigation bar and click **Applications**.
3. Click **Import**.
4. **Browse** to the downloaded .pak file.
5. Click **Upload**.

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

## UNINSTALLING SYMANTEC CLOUD SECURITY

You must remove Symantec Cloud Security configuration to uninstall it.

### To remove SymantecCloud Fetcher:

1. Go to *Settings >> Configuration* from the navigation bar and click **Devices**.
2. Click **Add collectors/fetchers** from the **Actions** of the *localhost* device.
3. Click **SymantecCloud Fetcher**.
4. Click the **Delete** icon from **Actions** of the preferred SymantecCloud Fetcher for Symantec Cloud Security.
5. Click **Yes**.

### To remove Processing Policies:

1. Go to *Settings >> Configuration* from the navigation bar and click **Processing Policies**.
2. Click the **Delete** icon from **Actions** of the policy name for Symantec Cloud Security.
3. Click **Yes**.

### To remove Normalization Policies:

1. Go to *Settings >> Configuration* from the navigation bar and click **Normalization Policies**.
2. Click the **Delete** icon from **Actions** of the policy name for Symantec Cloud Security.
3. Click **Yes**.

### To uninstall Symantec Cloud Security:

1. Go to *Settings >> System Settings* from the navigation bar and click **Applications**.
2. Click the **Uninstall** icon from **Actions** of Symantec Cloud Security.
3. Click **Yes**.

## CONFIGURING SYMANTEC CLOUD SECURITY

### 4.1 Configuring a Repo for Symantec Cloud Security

1. Go to *Settings >> Configuration* from the navigation bar and click **Repos**.
2. Click **Add**.
3. Enter a **Repo Name**.
4. Select a **Repo Path** to store incoming logs.
5. Set a **Retention Day** to keep logs in a repository before they are automatically deleted.

---

**Note:** You can add and remove multiple **Repo Path** and **Retention Day**.

---

6. Select a **Remote LogPoint** and set a **Available for (day)**.
7. Click **Submit**.

**ADD REPO**

**REPO INFORMATION**

Repo Name:

Repo Path:  ▼ Retention (day):  ▲ ▼ + -

**AVAILABILITY**

*A copy of above repo will be created in the selected remote LogPoints. If somehow the repo is not accessible, its copy will be used in search. This will hence maintain the higher availability of the repo.*

Remote LogPoint:  ▼ Available for (day):  ▲ ▼ -

**Submit** **Cancel**

Fig. 1: Adding a Repo

#### 4.1.1 Adding a Normalization Policy

1. Go to *Settings >> Configuration* from the navigation bar and click **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

Q

A10WAFCompiledNormalizer  
ADFSNormalizer  
ARPGuardCompiledNormalizer  
ApacheHTTPServerCompiledNormalizer  
ArubaClearPassCompiledNormalizer  
ArubaOSCompiledNormalizer  
BitDefenderCompiledNormalizer  
CEFCCompiledNormalizer  
CentrifyCompiledNormalizer

⤴

⤶

⤷

⤵

⤴

⤶

⤷

⤵

Selected

Search

Q

SymantecCloudSecurityCompiledNormalizer

Normalization Packages:

Available

Search

Q

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

Q

View Signatures

Submit

Cancel

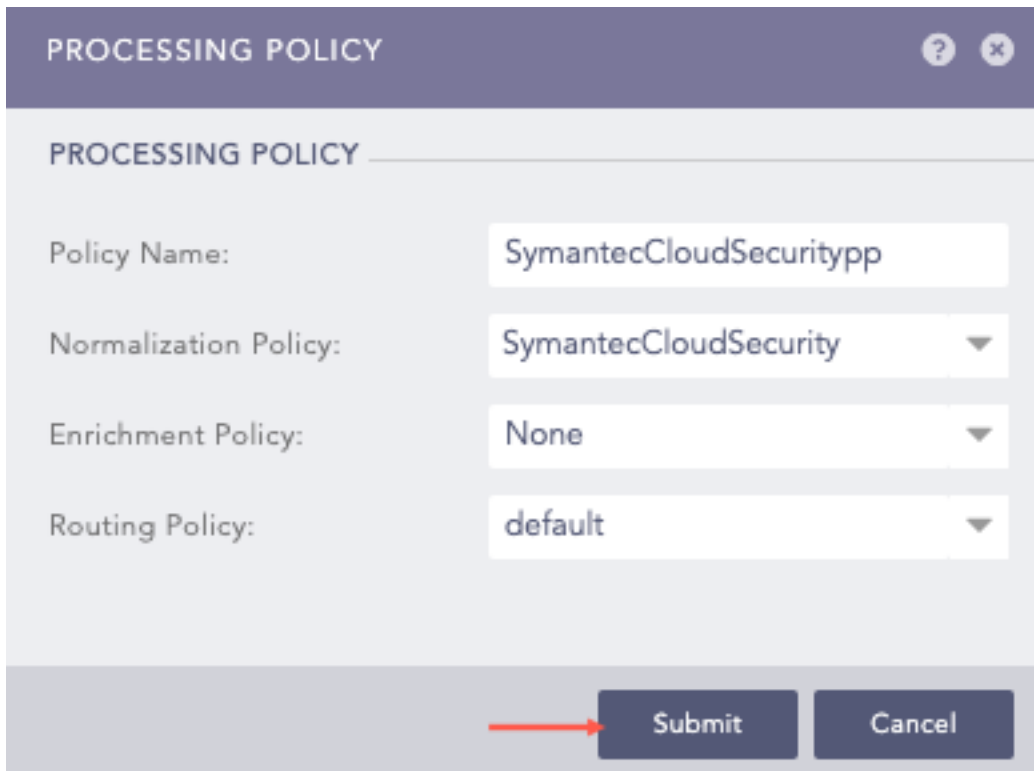
Fig. 2: Adding a Normalization Policy

4.1. Configuring a Repo for Symantec Cloud Security

6

### 4.1.2 Configuring a Processing Policy for Symantec Cloud Security

1. Go to *Settings >> Configuration* from the navigation bar and click **Processing Policies**.
2. Click **Add**.
3. Enter a **Policy Name**.
4. Select the previously created **Normalization Policy**.
5. Select the **Enrichment Policy**.
6. Select the **Routing Policy**.



PROCESSING POLICY

PROCESSING POLICY

Policy Name: SymantecCloudSecuritypp

Normalization Policy: SymantecCloudSecurity

Enrichment Policy: None

Routing Policy: default

Submit Cancel

Fig. 3: Adding a Processing Policy

### 4.1.3 Configuring Symantec Cloud Security Fetcher

1. Go to *Settings >> Configuration* from the navigation bar and click **Devices**.
2. Click **Add collectors/fetchers (+)** from **Actions** of the *localhost* device.
3. Click **SymantecCloud Fetcher**.

4. Click **Add**.



Fig. 4: 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 the previously created **Processing 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. 5: 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' and tabs for 'DASHBOARD', 'SEARCH', 'REPORT', 'INCIDENT', and 'SETTINGS'. The 'SEARCH' tab is active. Below the navigation bar, a search bar contains the query 'col\_type=symanteccloud'. To the right of the search bar, there are buttons for 'Use wizard', '1/1', 'LAST 7 DAYS', and 'SEARCH'. Below the search bar, it says 'Found 455,805 logs'. On the left side, there's a section titled 'Interesting Fields' with a table showing fields and their counts:

Field	%
transaction_uuid	100
location	100
col_type	100
cs_client_ip_country	100

The main area displays a log entry for '2019/11/08 09:53:17'. The log entry is a long string of key-value pairs, including: log\_ts=2019/11/01 01:22:47, device\_ip=:1, device\_name=localhost, col\_type=symanteccloud, source\_address=, destination\_address=192.168..., destination\_port=, sig\_id=86303200823, repo\_name=symantec, status\_code=0, action=TUNNELED, domain=, protocol=ssl, category=Business/Economy/Office/Bus..., application=none, request\_method=unknown, received\_data\_size=1558, sent\_data\_size=6311, access\_type=gateway\_proxy, appliance=DP8-MAA1\_ProxySG, authentication\_group=cn=inet-hg-ext-4, col\_ts=2019/11/08 09:53:17, collected\_at=LogPoint, cs\_client\_ip\_country=Ambiguous - Special Use, cs\_connection\_negotiated\_cipher=none, cs\_icap\_status=ICAP\_NOT\_SCANNED, date=2019-11-01, device\_category=ProxyServer, duration=636296, location=RJIN\_FMAA\_HAL\_01, location\_id=370660, logpoint\_name=LogPoint, norm\_id=SymantecCloudSecurity, operation=none, outbound\_server\_address=, path=/, r\_supplier\_country=United States, random\_ipv6\_address=, result=OBSERVED, rs\_connection\_negotiated\_cipher=none, rs\_icap\_status=ICAP\_NOT\_SCANNED, s\_supplier\_country=None, supplier\_address=, tenant\_id=16070, threat\_level=unlicensed, time=01:22:47, transaction\_uuid=692f811e91863ea-00000000f2..., user\_dn=uid=z010466,ou=RNTBCI,ou=Pe...

Fig. 1: Symantec Cloud Security Log

## EXPECTED LOG SAMPLE

### SymantecCloud

```
{ "SymantecCloud": { "cs-icap-error-details": "-", "x-exception-id": "-", "sc-filter-result":  
→ "OBSERVED", "x-sc-connection-issuer-keyring-alias": "-", "s-supplier-ip": "00.xxx.00.00", "cs-  
→ uri-query": "-", "cs-method": "HEAD", "cs-categories": "Technology/Internet;Technique;  
→ Technique Extended", "x-cloud-rs": "-", "x-client-security-posture-details": "-", "x-xx-xxx-error  
→ ": "-", "s-action": "TCP_NC_MISS", "x-xx-certificate-xxxxxxx": "-", "x-cs-certificate-subject": "-  
→ ", "x-rs-connection-negotiated-cipher": "none", "x-rs-certificate-validate-status": "-", "cs-icap-  
→ status": "ICAP_NOT_SCANNED", "x-sc-connection-issuer-keyring": "-", "sc-status": "301", "x-  
→ bluecoat-application-operation": "none", "s-supplier-failures": "-", "sc-bytes": "199", "x-cs-  
→ client-ip-country": "Ambiguous - Special Use", "time-taken": "263", "cs-uri-port": "80", "cs(X-  
→ Requested-With)": "-", "cs-auth-groups": "cn=TECH-INET", "x-icap-reqmod-header(X-ICAP-  
→ Metadata)": "-", "x-client-security-posture-risk-score": "-", "s-supplier-country": "None", "rs-  
→ icap-error-details": "-", "x-client-device-name": "-", "x-client-agent-sw": "-", "x-cs-connection-  
→ negotiated-ssl-version": "TLSv1.2", "x-rs-ocsp-error": "-", "cs-uri-path": "/", "x-bluecoat-  
→ appliance-name": "DP7-GRU1_proxysg", "rs(Content-Type)": "text/html;%20charset=iso-0000-  
→ 1", "cs-userdn": "uid=awaws02,ou=XXX,ou=People,o=renault", "x-cs-connection-negotiated-  
→ cipher": "AES128-SHA256", "x-client-device-type": "-", "cs-bytes": "314", "x-virus-id": "-",  
→ "cs(Referer)": "-", "x-bluecoat-access-type": "gateway_proxy", "x-client-device-id": "-", "rs-  
→ icap-status": "ICAP_NOT_SCANNED", "x-bluecoat-application-name": "Amazon", "x-rs-  
→ connection-negotiated-cipher-size": "-", "cs-host": "console.aws.amazon.com", "date": "0000-  
→ 11-01", "x-client-agent-type": "-", "c-ip": "10.000.31.00", "x-rs-certificate-hostname-threat-risk  
→ ": "-", "x-bluecoat-reference-id": "-", "r-supplier-country": "United States", "cs-uri-extension":  
→ "-", "x-cs-connection-negotiated-cipher-size": "128", "x-client-os": "-", "r-ip": "00.000.00.00",  
→ "s-ip": "192.168.1.2", "x-bluecoat-location-name": "R_BR_ACUR_NET_01", "x-bluecoat-  
→ request-tenant-id": "16070", "x-bluecoat-transaction-uuid": "xxxxxxxxxxxxxxxxxx-  
→ 00000000b0000000-0000000050000000", "x-bluecoat-location-id": "370900", "x-data-leak-  
→ detected": "no", "x-random-ipv6": "2000:0D00:0000:0000:0e1f:fe7e:252f:0000", "x-rs-  
→ connection-negotiated-ssl-version": "-", "time": "01:22:47", "x-rs-certificate-observed-errors":  
→ "-", "x-icap-respmod-header(X-ICAP-Metadata)": "-", "cs-threat-risk": "unlicensed", "cs-uri-  
→ scheme": "http", "x-bluecoat-placeholder": "-", "cs(User-Agent)": "curl/7.00.0", "x-rs-  
→ certificate-hostname-categories": "-" }}
```