



# 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>

---

CHAPTER  
**ONE**

---

## 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*

---

CHAPTER  
**TWO**

---

## 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: SymantecCloudSecurity

Repo Path: /opt/immune/storage/ Retention (day): 3

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: None Available for (day): 1

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**.

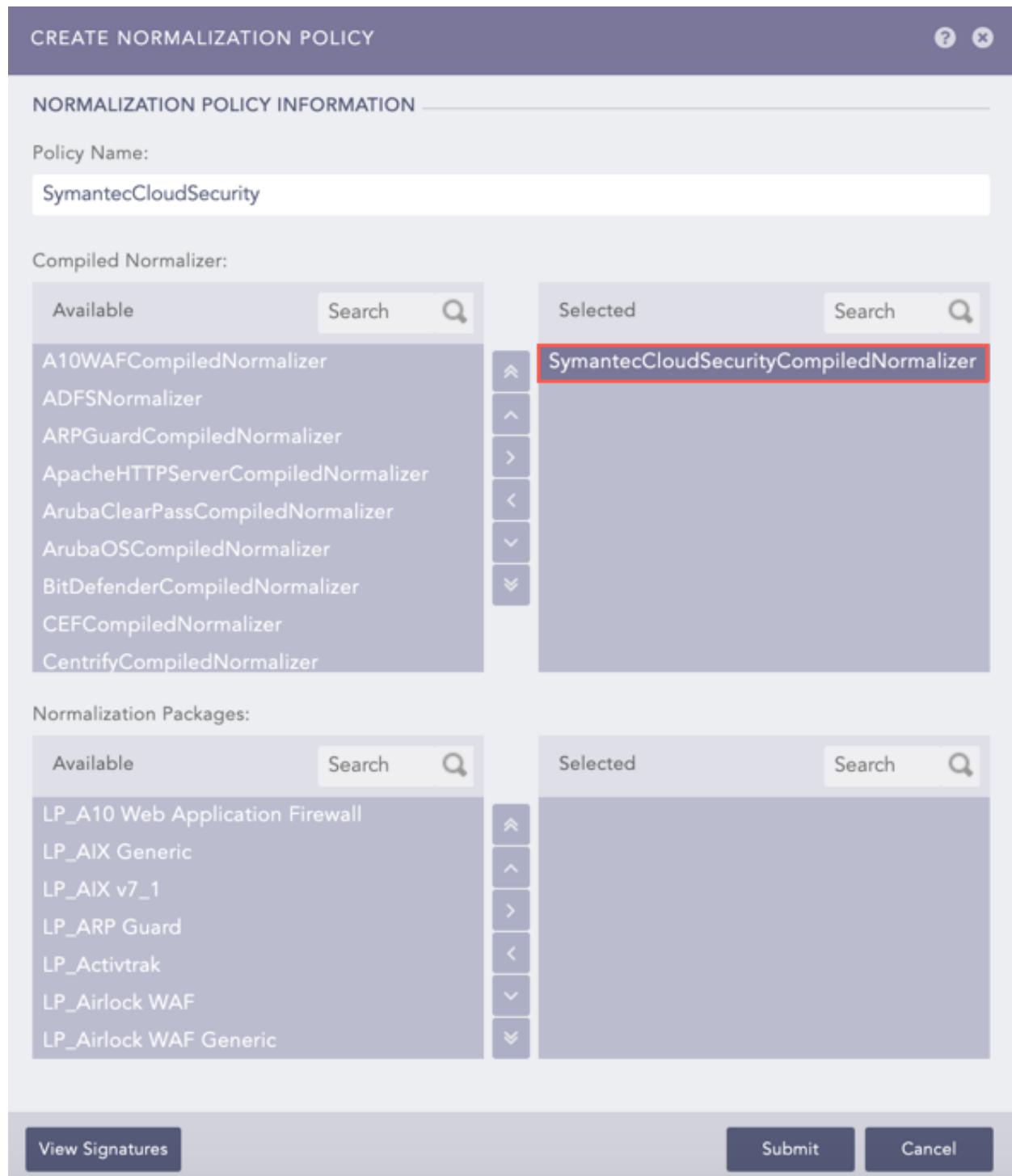


Fig. 2: Adding a Normalization Policy

#### 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

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:  ▲ ▼

Start Date:  calendar

End Date:  calendar

Processing Policy:  ▼

Charset:  ▼

**Enable Proxy**

▲ **Proxy Configuration**

IP/Port:  4 ▲ ▼

Protocol:  **HTTP**  
 **HTTPS**

Submit Cancel

Fig. 5: Adding a New Configuration for SymantecCloud Fetcher

---

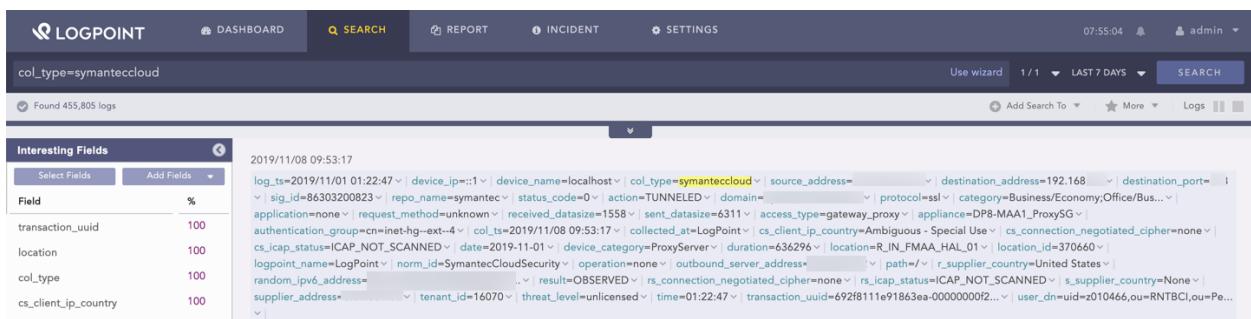
## CHAPTER FIVE

---

# 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 search interface. The search bar at the top contains the query `col_type = symanteccloud`. Below the search bar, a message indicates `Found 455,805 logs`. The main area displays a table of 'Interesting Fields' with the following data:

Field	%
transaction_uuid	100
location	100
col_type	100
cs_client_ip_country	100

Below the table, a large log entry is shown in a monospaced font. The log entry starts with the timestamp `2019/11/08 09:53:17` and contains numerous log fields and their values, such as `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_datasize=1558`, `sent_datasize=6311`, `access_type=gateway_proxy`, `appliance=DP8-MAAT_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=R_IN_FMAA_HA_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_uid=692f811e91863ea-0000000002...`, `user_dn=uid=z010466,ou=RNTBCI,ou=Pe...`.

Fig. 1: Symantec Cloud Security Log

---

## CHAPTER SIX

---

### 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-xxxxxxxx": "-", "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(Rerer)": "-", "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": "xxxxxxxxxxxxxxxxxxxx-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-reqmod-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": "-"}}
```