

Integrations

SymantecCloudSecurity

V5.0.0

CONTENTS

1	SymantecCloudSecurity Application	1
2	Installing the Application	2
2.1	Prerequisite	2
2.2	Installing the SymantecCloudSecurity Application in LogPoint	2
3	Configuring the Application	3
3.1	Adding a Normalization Policy	3
3.2	Configuring the SymantecCloudSecurity Fetcher	5
4	Accessing SymantecCloudSecurity Logs	10
4.1	Accessing Logs using the SymantecCloudSecurity Application	10
5	Uninstalling the Application	11
5.1	Uninstalling the SymantecCloudSecurity Application in LogPoint	11

SYMANTECCLOUDSECURITY APPLICATION

The *SymantecCloudSecurity* application enables you to fetch and analyze *Symantec Web Security Service* logs.

The application package consists of the following components:

1. **Fetcher**

- SymantecCloudSecurityFetcher

2. **Compiled Normalizer**

- SymantecCloudSecurityCompiledNormalizer

INSTALLING THE APPLICATION

2.1 Prerequisite

LogPoint v6.7.0 or later

2.2 Installing the SymantecCloudSecurity Application in LogPoint

1. Go to *Settings >> System >> Applications*.
2. Click **Import**.
3. **Browse** for the location of the downloaded *SymantecCloudSecurity_5.0.0.pak* file.
4. Click **Upload**.

After installing the application, you can find the *SymantecCloudSecurity Fetcher 5.0.0* and *SymantecCloudSecurityCompiledNormalizer 5.0.0* entries under *Settings >> System >> Plugins*.

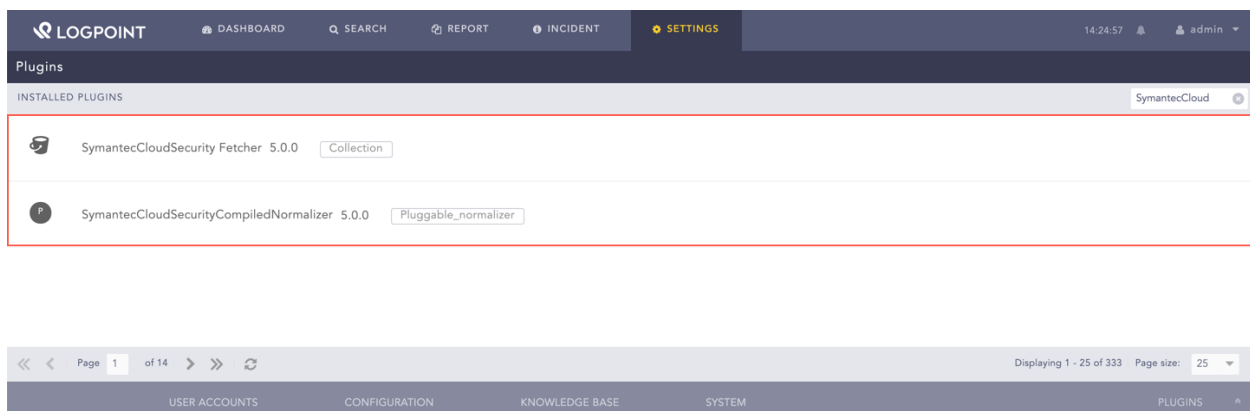


Fig. 1: SymantecCloudSecurity Installed

CONFIGURING THE APPLICATION

3.1 Adding a Normalization Policy

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

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

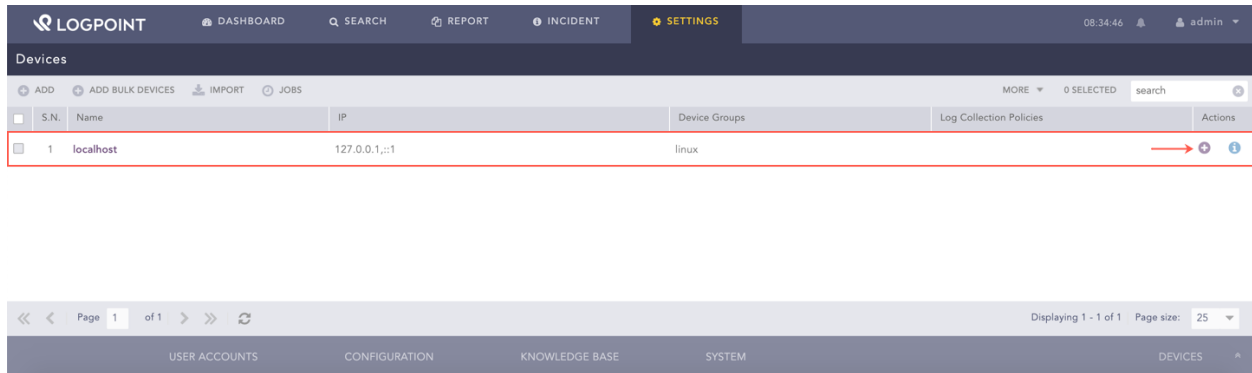
5. Click **Submit**.

3.1. Adding a Normalization Policy

4

3.2 Configuring the SymantecCloudSecurity Fetcher

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



3. Click **SymantecCloud Fetcher**.

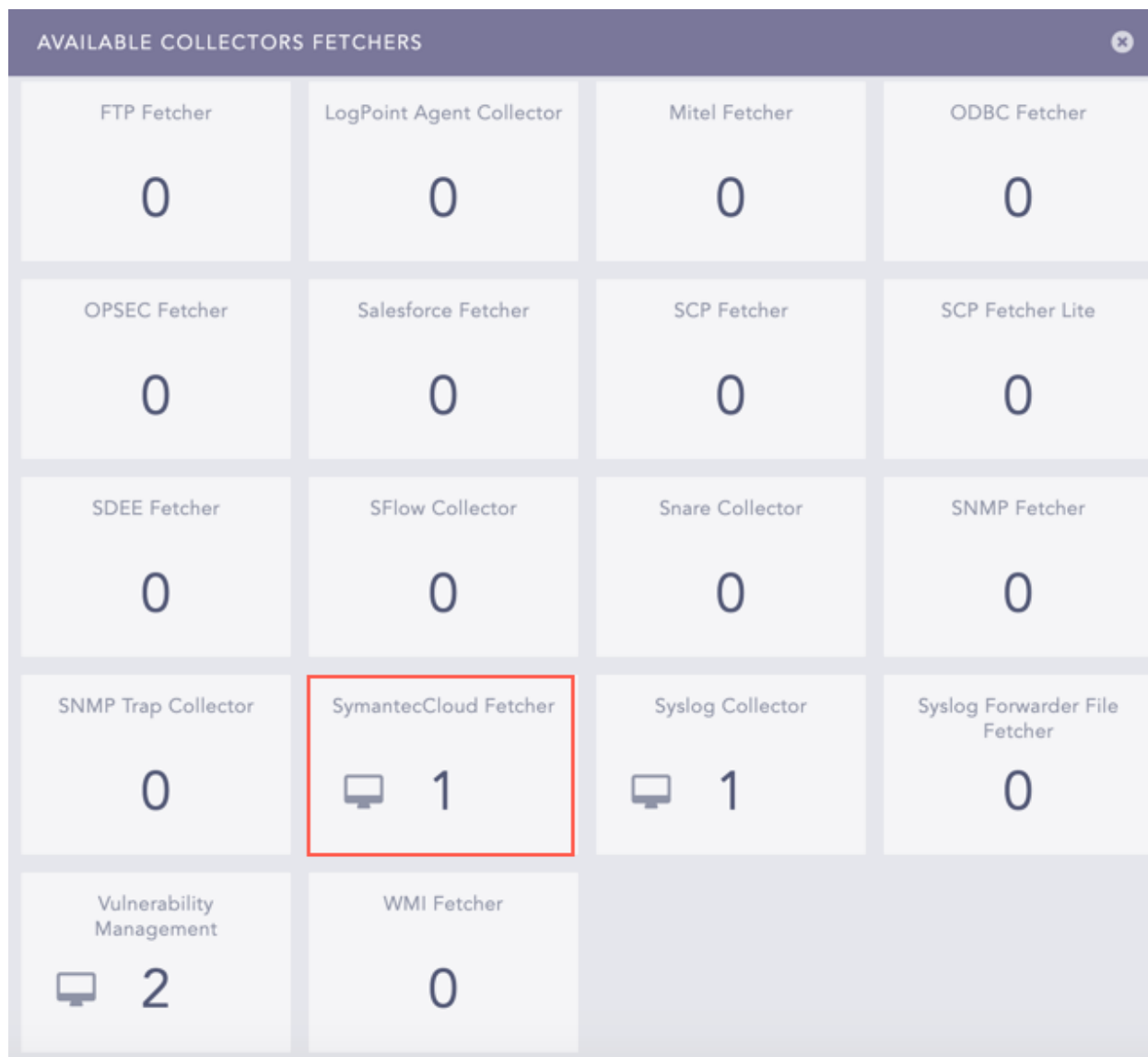


Fig. 2: Available Collectors Fetchers Panel

4. Click **Add**.



Fig. 3: SymantecCloudSecurity Fetcher Panel

SYMANTECCLOUDSECURITY FETCHER

SYMANTECCLOUDSECURITY FETCHER

Username:

Password: Show

Fetch Interval:

Start Date:

End Date:

Processing Policy:

Charset:

☒ Enable Proxy

▲ Proxy Configuration

IP/Port:

Protocol: ☒ HTTP ☐ HTTPS

Submit Cancel

Fig. 4: Adding a New Configuration for SymantecCloud 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**. The application fetches logs from the specified date.
8. Select the **End Date**. The application 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** if you use a proxy server.
12. In the *Proxy Configuration* section:
 - 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**.

4.1 Accessing Logs using the SymantecCloudSecurity Application

Use the following search query to access the logs fetched by the SymantecCloudSecurity application:

```
col_type = symanteccloud
```

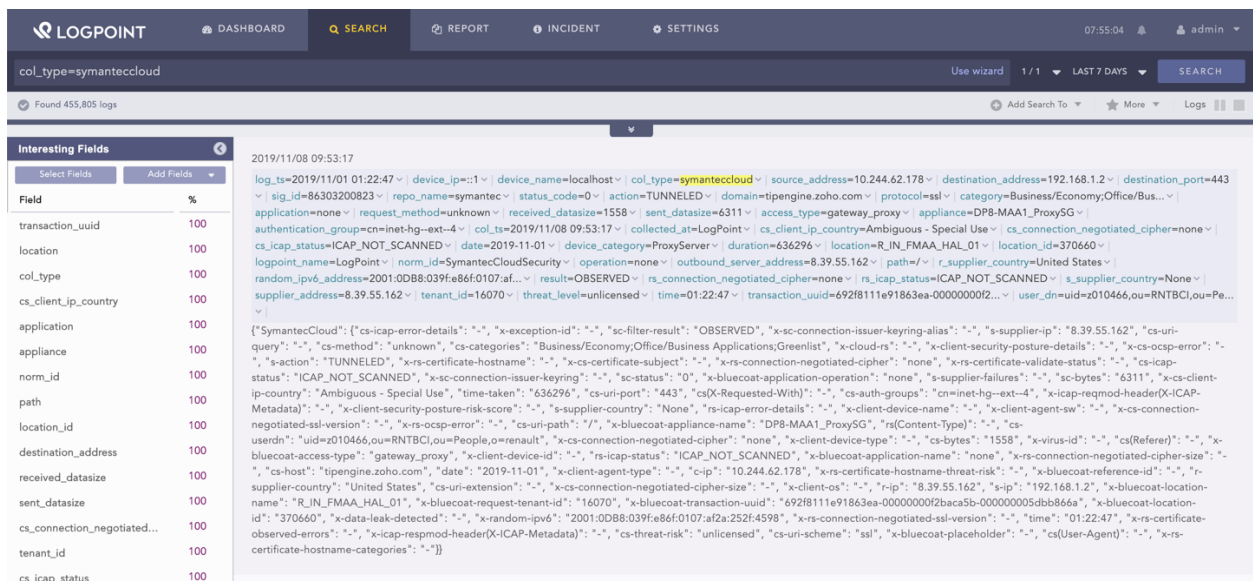


Fig. 1: SymantecCloudSecurity Log

UNINSTALLING THE APPLICATION

5.1 Uninstalling the SymantecCloudSecurity Application in LogPoint

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

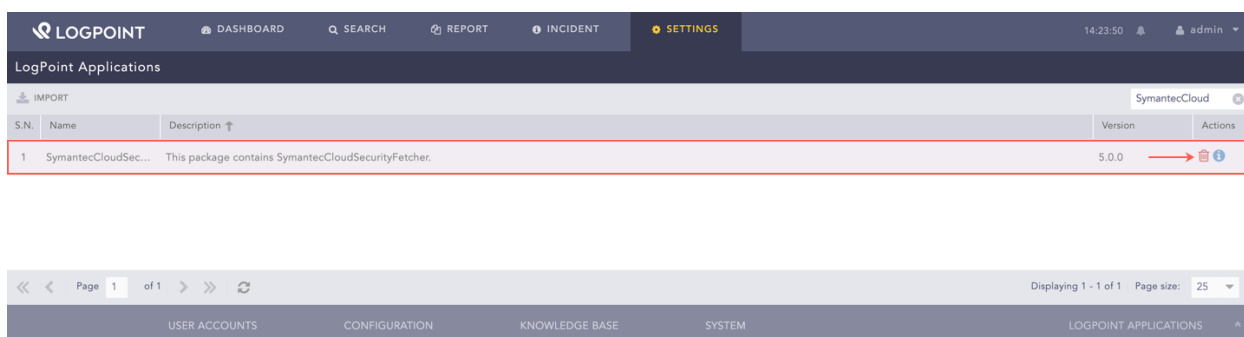


Fig. 1: SymantecCloudSecurity Uninstallation

Note: You must remove the **SymantecCloudSecurity Fetcher** configuration to delete the application.
