LOGPOINT

Integrations

SymantecCloudSecurity

V5.0.1

CONTENTS

CHAPTER

ONE

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

CHAPTER

TWO

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*.

CHAPTER

THREE

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**.

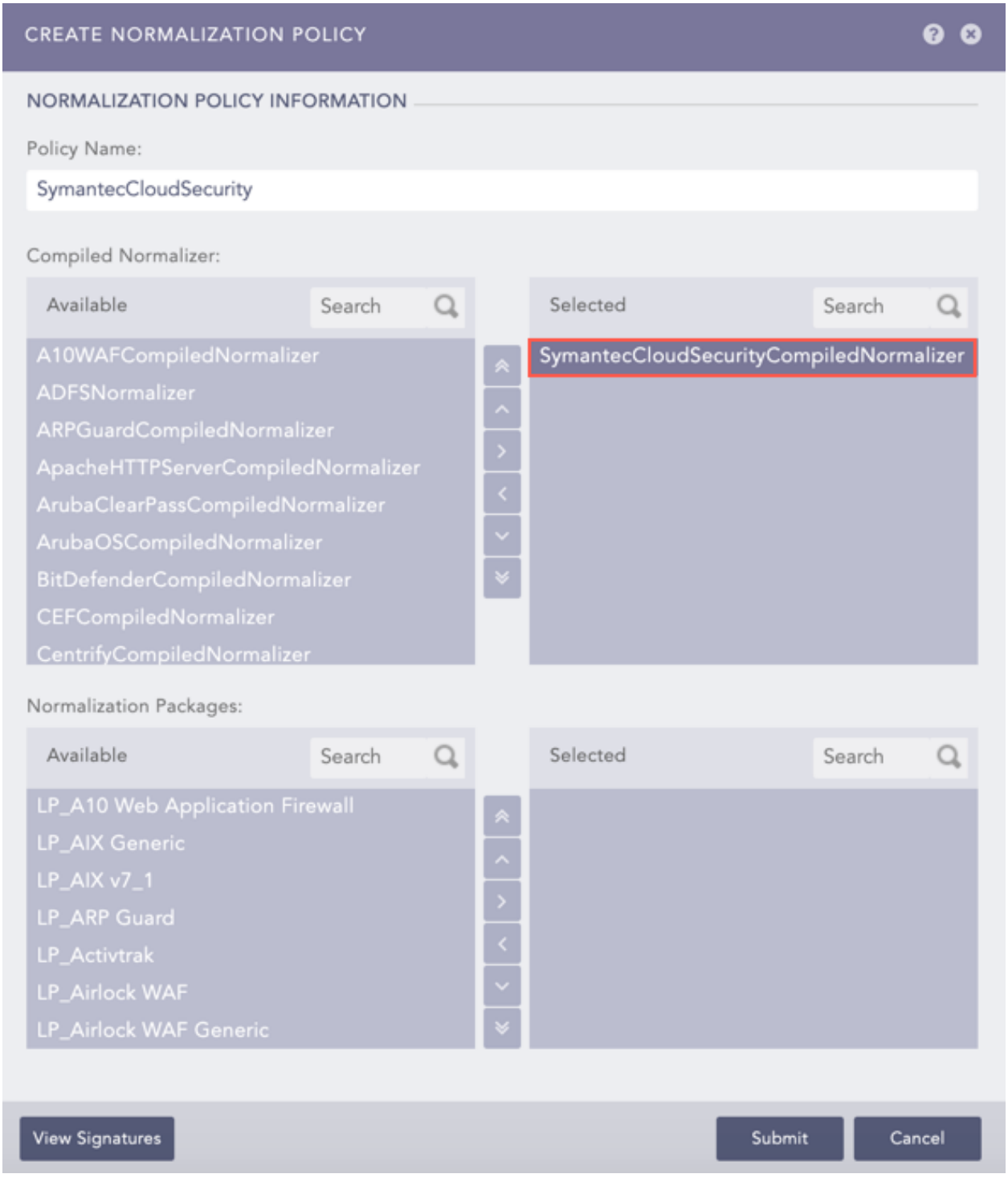
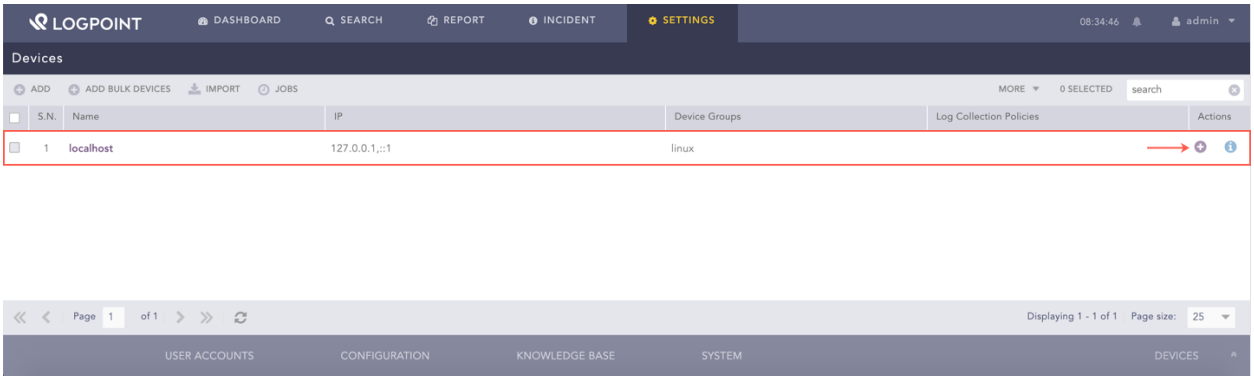


Fig. 1: Adding a Normalization Policy

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**.

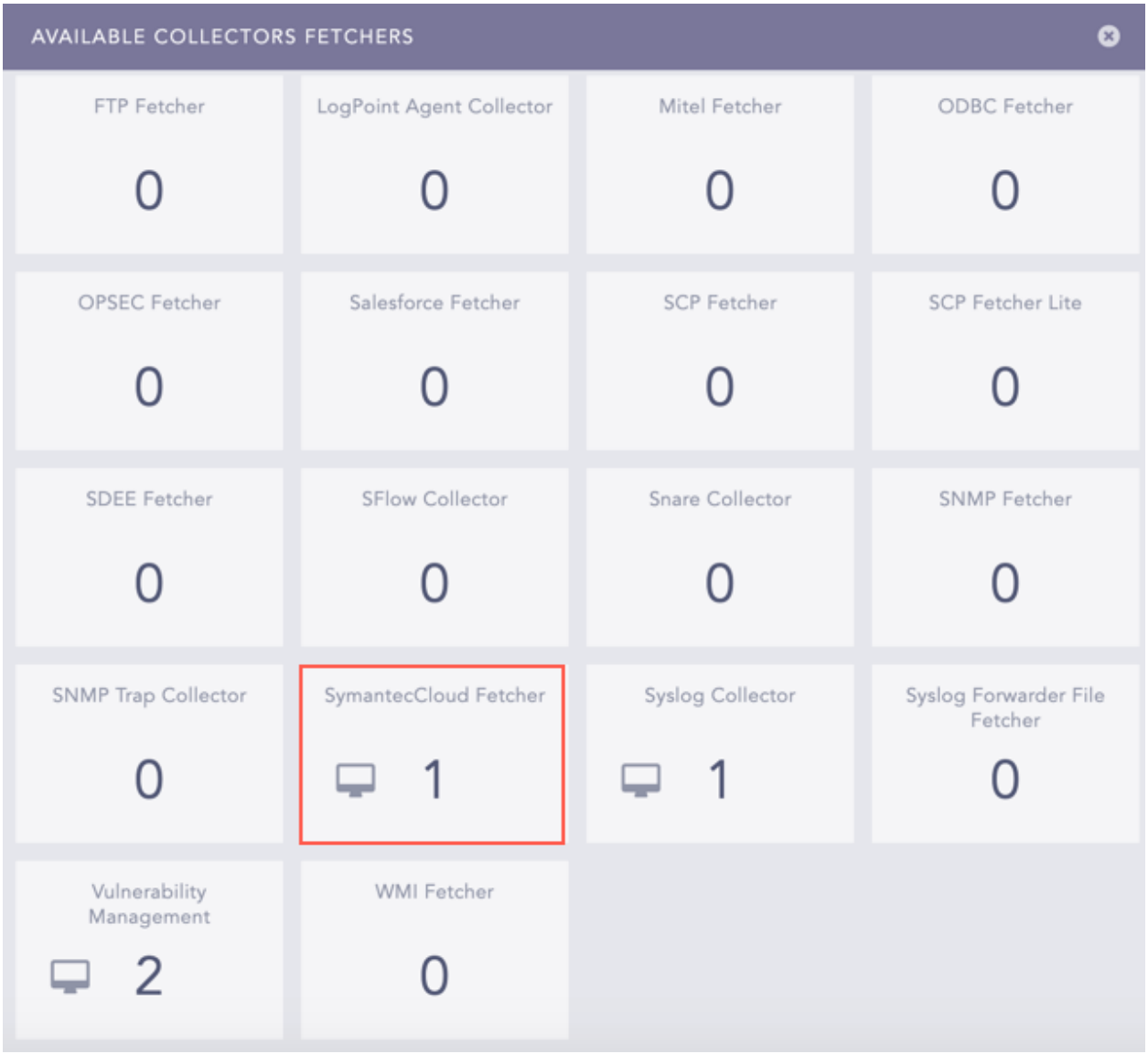


Fig. 2: Available Collectors Fetchers

4. Click **Add**.

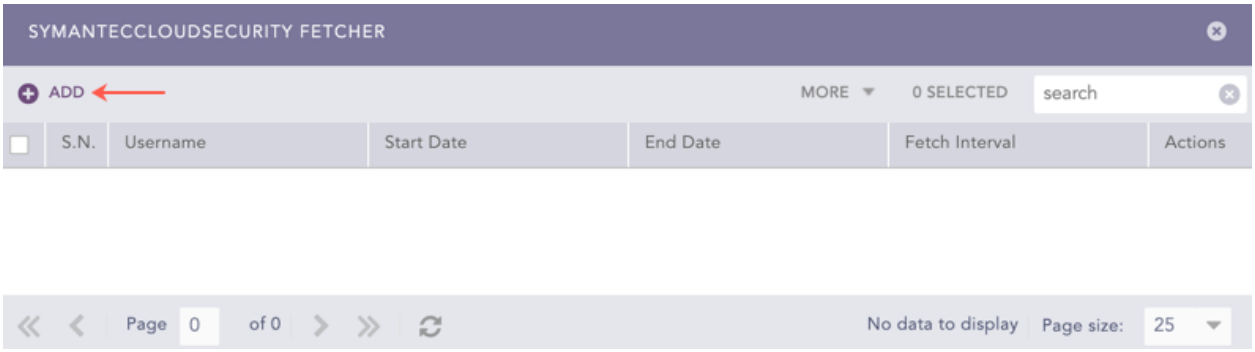


Fig. 3: SymantecCloudSecurity Fetcher

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**.

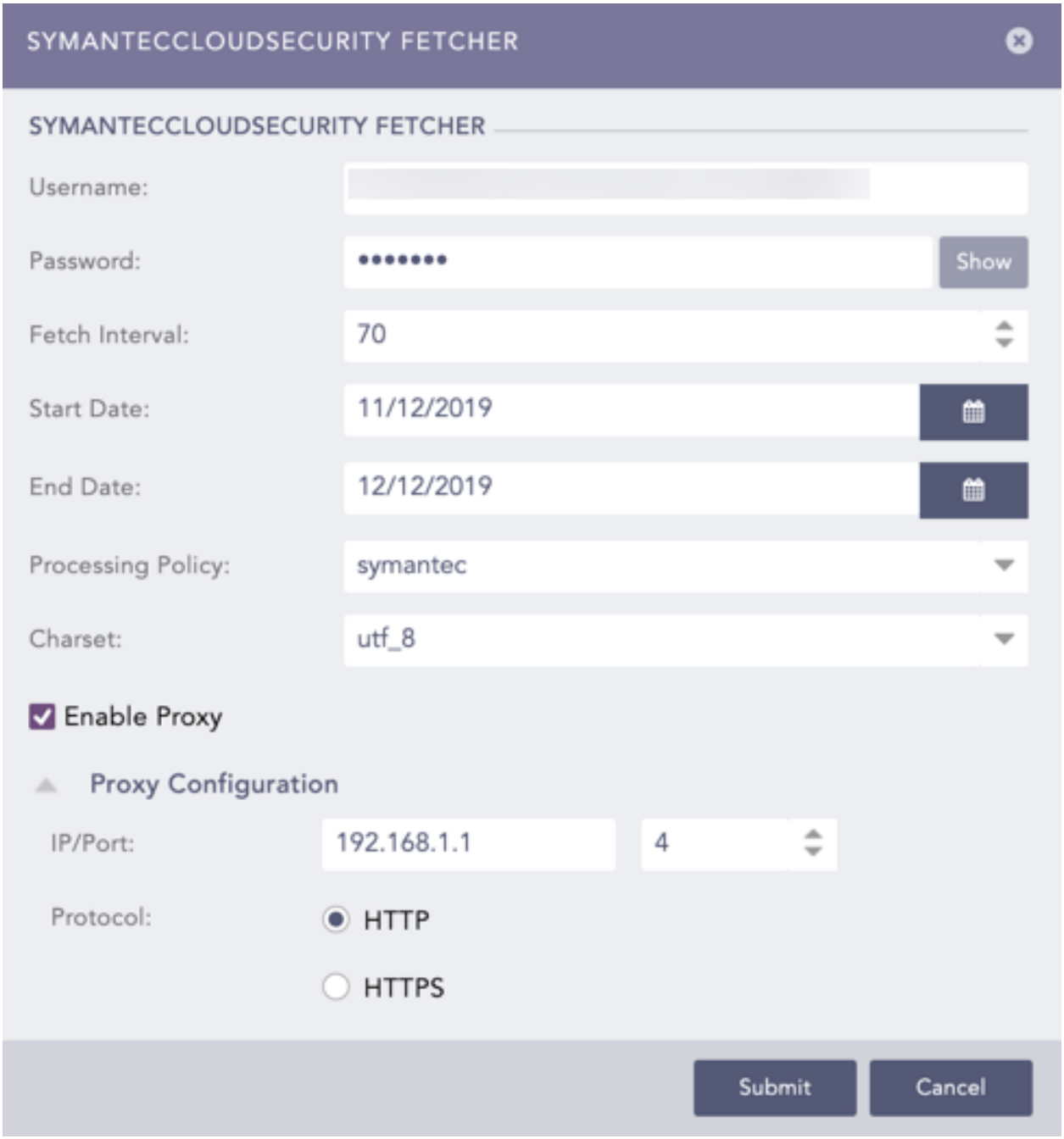


Fig. 4: Adding a New Configuration for SymantecCloud Fetcher

CHAPTER

FOUR

ACCESSING SYMANTEC CLOUD SECURITY LOGS

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

```
col_type = symanteccloud
```

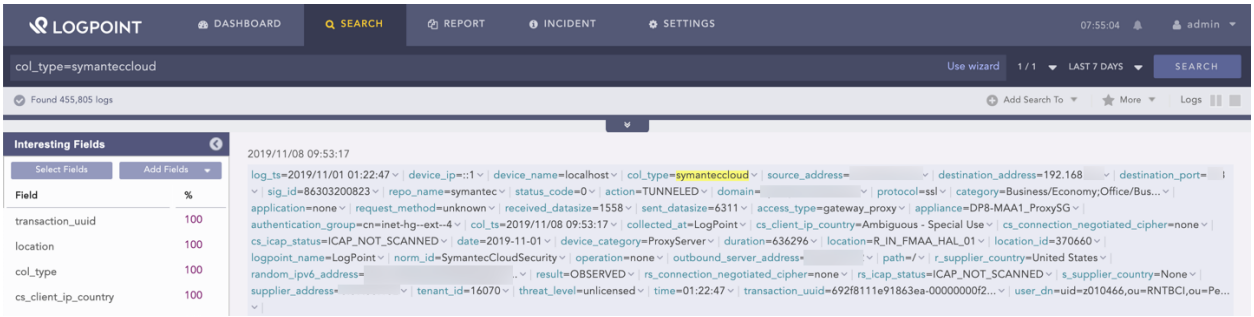


Fig. 1: Symantec Cloud Security Log

CHAPTER

FIVE

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.