Secureworks to Elastic Integration

STEP 1: Enable Log Sending from Secureworks

> This step happens inside your **Secureworks dashboard**.

Step-by-step:

1. **Login to Secureworks:**
   - Go to the Secureworks portal:
   - https://portal.secureworks.com
   - Enter your **Username** and **Password**
2. **Go to Log Export Settings:**
   - On the left-hand menu, look for **Settings** or **Administration**
   - Click **Data Export** or **Syslog Settings**
3. **Add a New Syslog Destination:**
   - Click **Add Destination** or **New Configuration**
   - In the form, fill in:
     - **IP Address** → Enter the IP of your Logstash server
     - **Port Number** → Enter `514`
     - **Protocol** → Select `UDP` or `TCP`
       (Ask IT which one your server accepts)
   - Check any box that says **"Enable"** or **"Activate"**
   - usually IT),Click **Save** or **Apply**

Secureworks is now ready to send logs!

STEP 2: Set Up Logstash to Receive Logs

> This step is done by whoever manages your Logstash server, but here's exactly what they need to do.

Step-by-step:

1. **Connect to the server (via SSH or terminal)**
2. Go to the folder:

   ```
   /etc/logstash/conf.d/
   ```

3. Create a new file:

   ```
   CopyEdit
   secureworks.conf
   ```

4. Paste this configuration inside:

```
input {
  udp {
    port => 514
    type => "secureworks"
  }
}

filter {
  if [type] == "secureworks" {
    json {
      source => "message"
      skip_on_invalid_json => true
    }
  }
}

output {
  elasticsearch {
```

```
    hosts => ["http://localhost:9200"]
    index => "secureworks-%{+YYYY.MM.dd}"
  }
}
```

5. Save the file
6. Restart Logstash by typing:

```
nginx
CopyEdit
 sudo systemctl restart logstash
```

Logstash is now waiting to receive logs.

STEP 3: View Logs in Kibana

> Now let's **see the logs** inside the Kibana dashboard.

Step-by-step:

1. **Open Kibana in your browser:**
   - Type the URL like:

```
cpp
CopyEdit
 http://<your-kibana-server-ip>:5601
```

2. **Go to Discover:**
   - On the left side menu, click **“Discover”**
3. **If it's your first time:**
   - A popup may ask you to create an **Index Pattern**
   - Click **Create index pattern**
   - In the box, type:

```
CopyEdit
 secureworks-*
```

   - Click **Next step**
   - Choose `@timestamp` (or the default time field)
   - Click **Create index pattern**
4. You will now see log data from Secureworks.

Optional

- Click **Dashboard** > Create new dashboard
- Add graphs or tables from Secureworks data
- Click **Alerts** to set up notifications for certain events

Troubleshooting (If You Don’t See Logs)

Problem	Solution
No logs in Kibana	Check that Secureworks export is enabled and points to the correct IP
Still empty?	Check if Logstash is running and port 514 is open
JSON parsing error?	check if logs are plain text or JSON

Revision #5
Created 19 June 2025 09:20:56 by John Polestico
Updated 19 June 2025 09:46:49 by John Polestico