Splunk Integration Guide

STEP 1: Enable Splunk HTTP Event Collector (HEC)

1. Navigate to:
   Settings → Data Inputs → HTTP Event Collector
2. Click on "New Token" and configure the following:
   - Name: CertSecure Logs
   - Source Type: _json
   - Index: (create one, see below)
3. After creation, share the following details with the CertSecure team:
   - HEC Token: Token string used for authentication
   - HEC Endpoint URL: e.g., https://splunk.example.com:8088
   - Protocol: Confirm whether HTTP or HTTPS is used

   Note: If HTTPS is used, ensure that the SSL certificate used by Splunk is trusted by CertSecure's backend.

STEP 2: Create a Dedicated Index

1. Navigate to:
   Settings → Indexes → New Index.
2. Enter:
   - **Index Name**: certsecure_logs.
3. Click **Save**.
4. Share this index name with the CertSecure Manager admin.

STEP 3: Ensure Network Connectivity

1. On the CertSecure backend server, ensure outbound access to **port 8088**.
2. If using firewalld, run:
   - sudo firewall-cmd --permanent --add-port=8088/tcp
   - sudo firewall-cmd –reload
3. If IP whitelisting is enabled in Splunk:
   - Add the CertSecure backend's IP to the **allowed list**.

Once the above prerequisites are met, follow these steps on the CertSecure Manager platform:

STEP 4: Configure Splunk Integration in CertSecure Manager

1. Login to **CertSecure Manager** (Admin portal).

2. Go to:
   Utilities → SIEM Integration → Splunk.
3. Click **“Add Configuration”**.
4. Fill in:
   - **HEC Endpoint URL**: https://splunk.example.com:8088
   - **HEC Token**: Paste the token from Step 1
   - **Protocol**: HTTPS or HTTP (as used in Splunk)
5. Click **“Save”**.

STEP 5: Validate Connection

1. CertSecure Manager will automatically attempt to connect:
   - Checks **token validity**
   - Confirms **network access**
   - Verifies **SSL certificate trust** (if HTTPS)
2. A message like **“Connection Successful”** will be shown on success.

STEP 6: Log Ingestion Begins

Once validated, CertSecure Manager will begin periodic log ingestion into Splunk.

All logs will be:

- Sent in JSON format
- Tagged with appropriate source type for parsing
- Indexed under certsecure_logs