empow i-SIEM Quick Installation Guide

Contents

General

This document contains quick installation guide for empow's i-SIEM platform in its basic deployment. For advanced installations, please contact empow support at support@empow.co.

The following installation guide support i-SIEM versions: 3.5.x, 3.6.x

System Requirements

OS Support

i-SIEM platform supports installation on Centos 7 or 8 operating system.

Browser Support

i-SIEM web client UI is compatible with commonly used web browsers like Google Chrome™ and Firefox®. For the features in empow i-SIEM to work properly, you must use a supported web browser.

Network & System Architecture

Figure 1: i-SIEM System Architecture and network connectivity

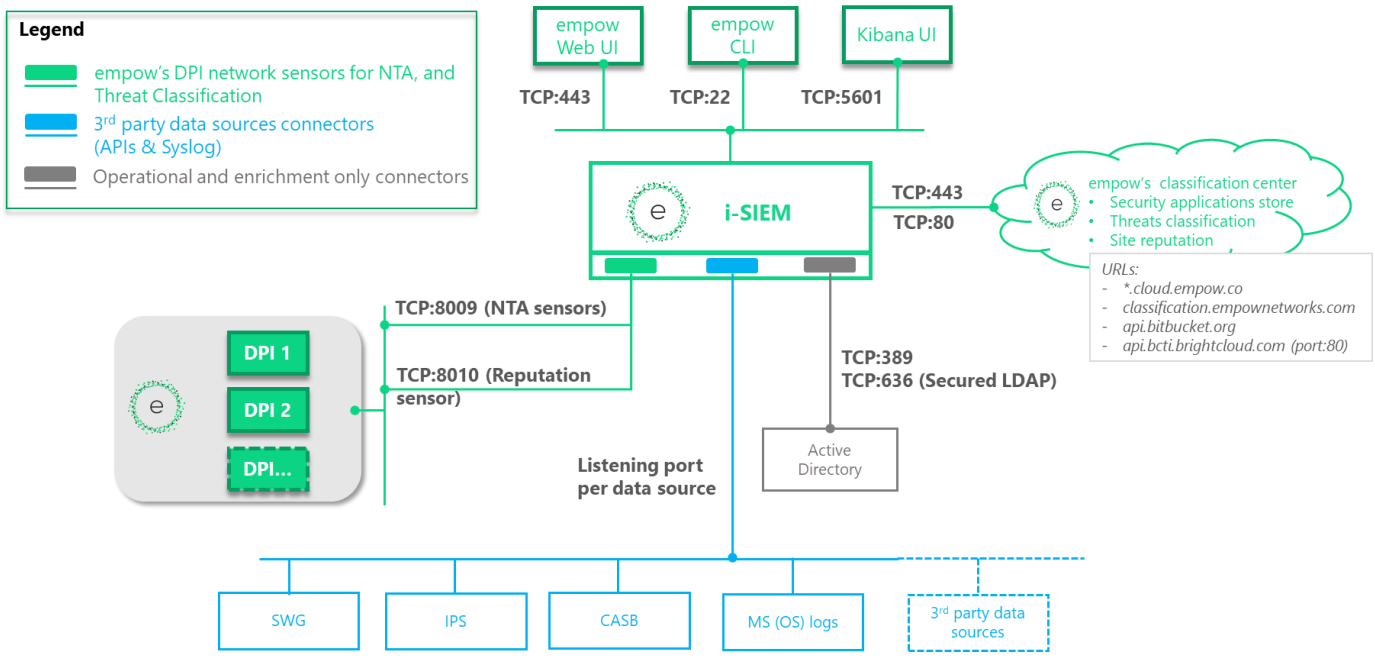


Table 1: i-SIEM network connectivity

Communication channel	Protocol & Port		Details
i-SIEM → empow's cloud classification center	TCP	443	URLs: ▪ *.cloud.empow.co ▪ classification.emponetworks.com ▪ api.bitbacket.org
		80	URL: api.bcti.brightcloud.com
i-SIEM → Microsoft AD	TCP	389/636	LDAP/S queries for enrichment of user organizational information
DPI → i-SIEM	TCP	8009	Applications traffic flows for NTA
DPI → i-SIEM	TCP	8010	Application traffic flows for Site reputation
System user → i-SIEM web client	TCP	8443	i-SIEM web client UI
System user → Kibana web client	TCP	5601	Kibana web client UI
System user → i-SIEM machines	TCP	22	CLI access

Deployment type

This quick installation guide describes the installation process of a single node (non-cluster) i-SIEM software.

For more information about multi-node (cluster) installation, as well as for installation of empow's DPI network agents please contact empow support at support@empow.co

Installation Instructions

Physical/Virtual Server Configuration

After obtaining the required HW (virtual or physical) for the single node deployment, install the following OS: centos 7 or 8

NOTE: Recommended version centos 7 or 8 (CentOS-7/8-x86_64-DVD-1908.iso ~4GB)

The server shall be installed with user 'empow' as administrator.

The following configuration and deployment steps shall be done under user empow –

You must not switch to root user.

Download Installation Package

Pull deployment scripts from empow library:

```
sudo yum install git
```

```
git clone https://bitbucket.org/empownetworks/swarm-installation.git
```

Configure the Host

Configure the host by executing the 'config_host.sh' on the server:

```
cd $HOME/swarm-installation/
```

```
./config_host.sh
```

Host configuration will cover the following steps:

i. Change default password
ii. Configure static IP address and hostname
iii. Install required tools (e.g. docker, python packages)
iv. Server Configuration
v. Docker configuration

Swarm Configuration

Configure swarm cluster by executing the following commands on the Host:

Create a swarm cluster consisted on a manager

```
cd $HOME/swarm-installation
```

```
./config_manager.sh
```

Deployment of Components

According to the deployment plan as set in the config_parameters.sh file, execute the following in Host:

vi. Move the deployment directory:
`cd $HOME/swarm-installation`

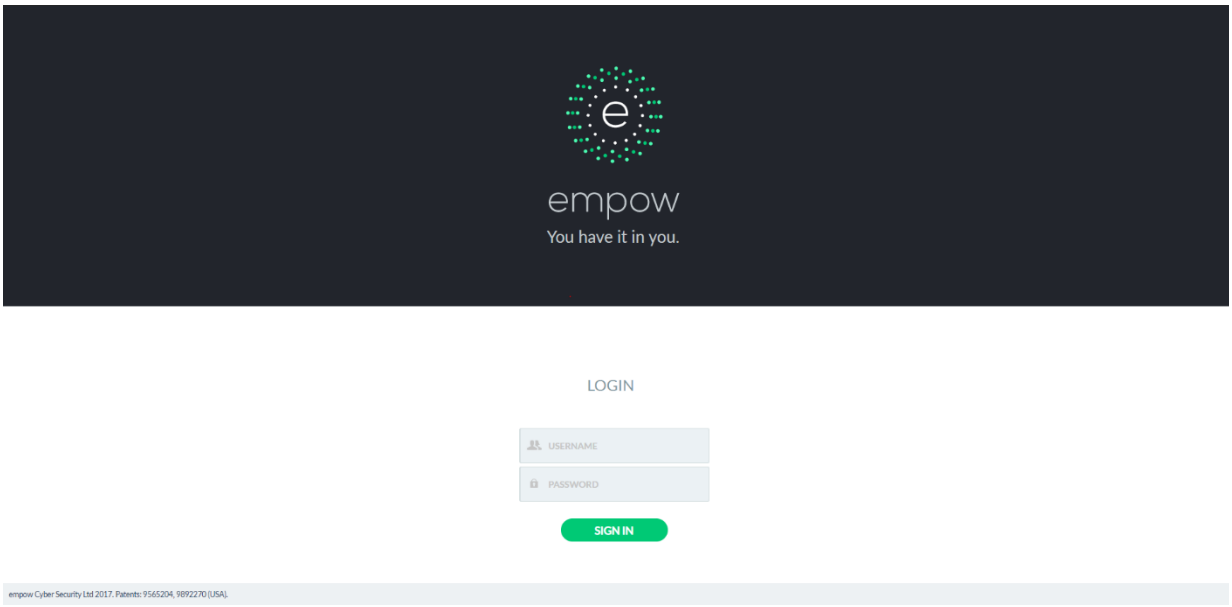
vii. Config parameters:
`./config_parameters.sh`

viii. Deploy
`./deploy_3.6.sh`

ix. Verify that all the services are up and running
`docker service ls`

Post Installation Steps

Open the browser and browse to "http://localhost/dist/index.html#/login", you should see the following login page:



x. Enter the default credentials:
Username: admin
Password: admin (make sure to change the default password)
You should now see i-SIEM main dashboard.
For more configuration details please refer the i-SIEM user guide (look for the link  at the top bar of the dashboards).