# On-premise SIEM

# How to send Trustelem logs to an on-premise SIEM?

Here we'll explain how to connect Trustelem to a SIEM or an agent capable of receiving logs and hosted in your infrastructure.
To begin with, it's important to know that Trustelem **sends new events every 30s**, and has a queuing system if an error is detected during transmission.

Now, how to do the setup?

## 1/ Install Trustelem Connect.

More information is available here:

LDAP-Radius - Trustelem Connect
For this usecase, you don't need to add any applications to the Trustelem Service, just a connector capable of joining your infra. You can use an existing Trustelem

## 2/ Add or edit the config.ini file.

In the folder where Trustelem Connect service is installed, edit or create the config.ini file.
Add the following lines:

```
outgoing_allowed = "true"
[targert.choose_a_name]
addr = "The IP/FQDN of your SIEM"
port = "The port of your SIEM"
```

Don't forget to change the name, the IP/FQDN, and the port!

## 3/ Restart Trustelem AD Connect

# 4/ On the Trustelem Service enable the logs sending

- Under **Send logs**, choose the date from which you'll get the logs.
- Click **Add send logs tasks**
- Click **enabled**
- Under **Target name**, enter the name choose on the config.ini file
- Under **format**, choose **JSON** (strongly recommended, as Trustelem logs are not properly designed for syslog)
- Under **types of logs to send**, choose **ALL** or a specific type of logs
- Click **Save**

# Debug

## Linux

- Use the command `nc -l -k VM_IP available_port` to build a server able to receive and display the logs
  *For instance: nc -l -k 10.10.126.203 6812*
- Provide the IP and the Port on the config.ini file and restart Trustelem Connect service
- Verify if Trustelem is sending the logs

## Windows

- Download Nmap and install it **with ncat checked**
- Using Powershell, go on the Nmap folder `cd C:\Program Files (x86)\Nmap\`
- Use the command `.\ncat.exe -l -k --allow VM_IP available_port` to build a server able to receive and display the logs
  *For instance: .\ncat.exe -l -k --allow 10.10.126.232 6812*
- Provide the IP and the Port on the config.ini file and restart Trustelem Connect service
- Verify if Trustelem is sending the logs

---

Revision #6
Created 11 March 2025 08:16:15 by WALLIX Admin
Updated 12 March 2025 10:07:18 by WALLIX Admin