



# **Cyber Command**

## **Implementasi yang Direkomendasikan untuk Konfigurasi\_Bagaimana untuk Berkorelasi dengan Endpoint Secure untuk Operasi Sederhana**

**Versi 3.0.49**



## Catatan Perubahan

Tanggal	Deskripsi Perubahan
April 2, 2021	Rilis Dokumen.
Mei 17, 2021	Dokumen update.

# Daftar Isi

Bab 1 Dasar .....	1
1.1 Konfirmasi Dasar Konfigurasi dan Deployment .....	1
1.2 Fungsi Korelasi.....	6

## Bab 1 Dasar

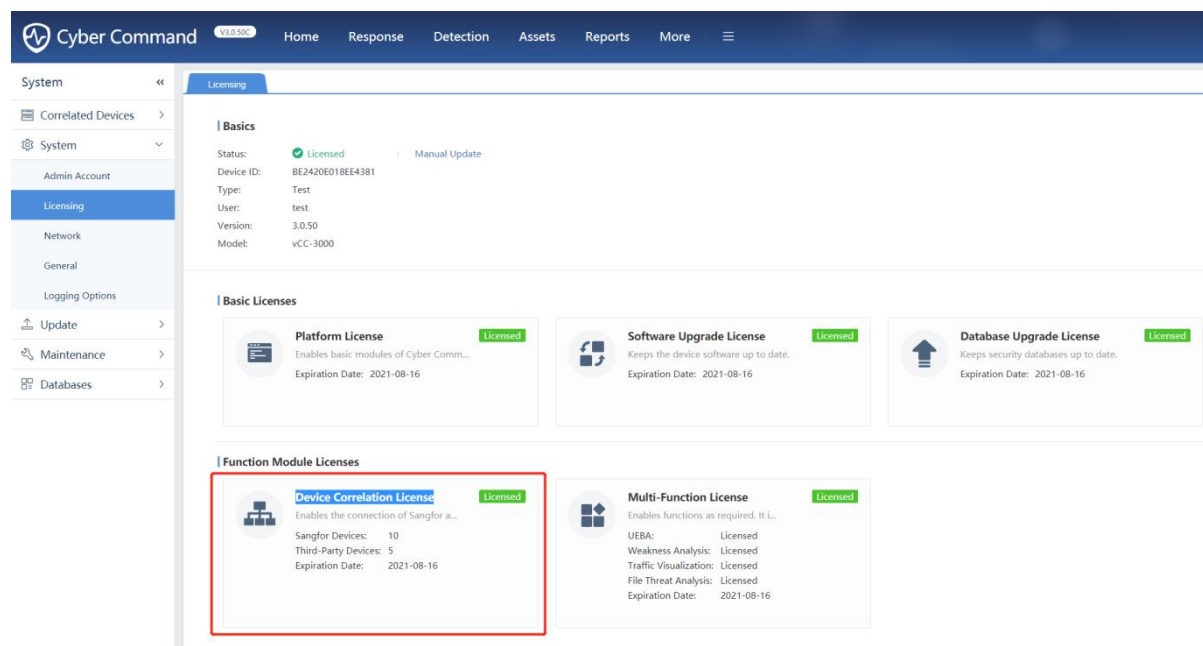
Dokumen terkait :

Praktik yang direkomendasikan untuk konfigurasi termasuk pilihan mode deployment, ide konfigurasi, koleksi informasi, keterbatasan fungsi, perbedaan versi. Mengenai ***How to Correlate with Endpoint Secure to Simply the Operation***, jika Anda ingin mempelajari tentang skenario POC umum dan langkah konfigurasi terperinci, silakan merujuk ke link berikut:

<https://sangforltd.sharepoint.com/:w:/s/PMO/Eb2759qybv9DtcB1qDbSmvAB1eeTzum6EO4W6smTQX7MMw?e=u0Jqhh>

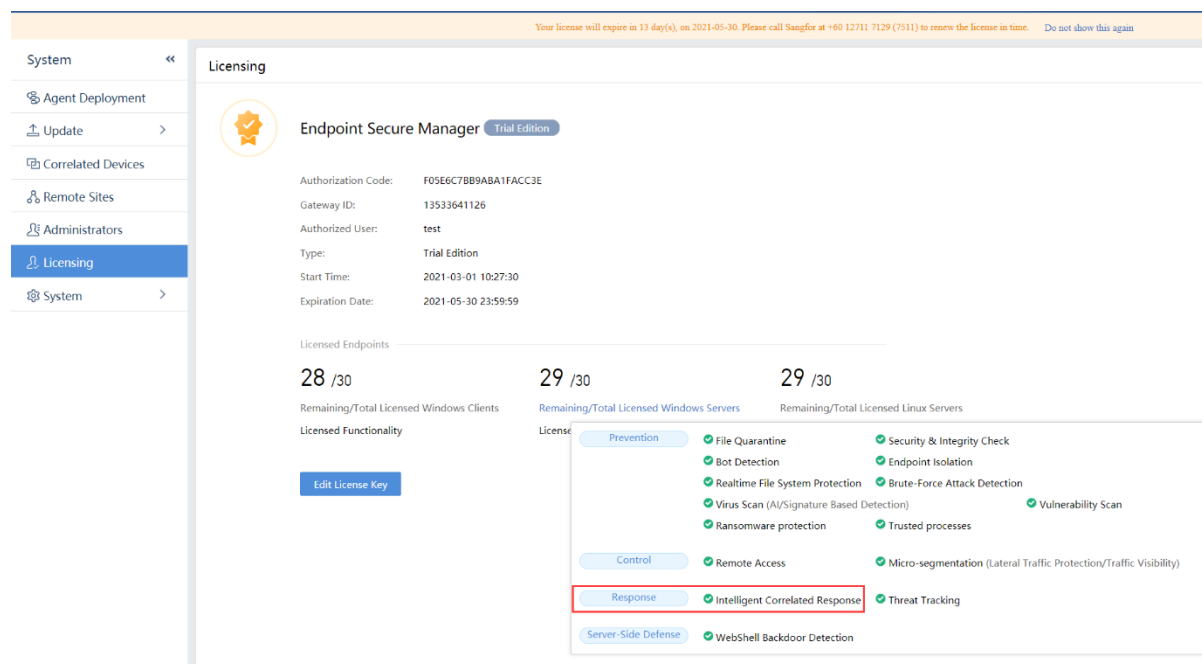
### 1.1 Konfirmasi Dasar Konfigurasi dan Deployment

1. Konfirmasi apakah CCOM telah mengaktifkan Device Correlation License.



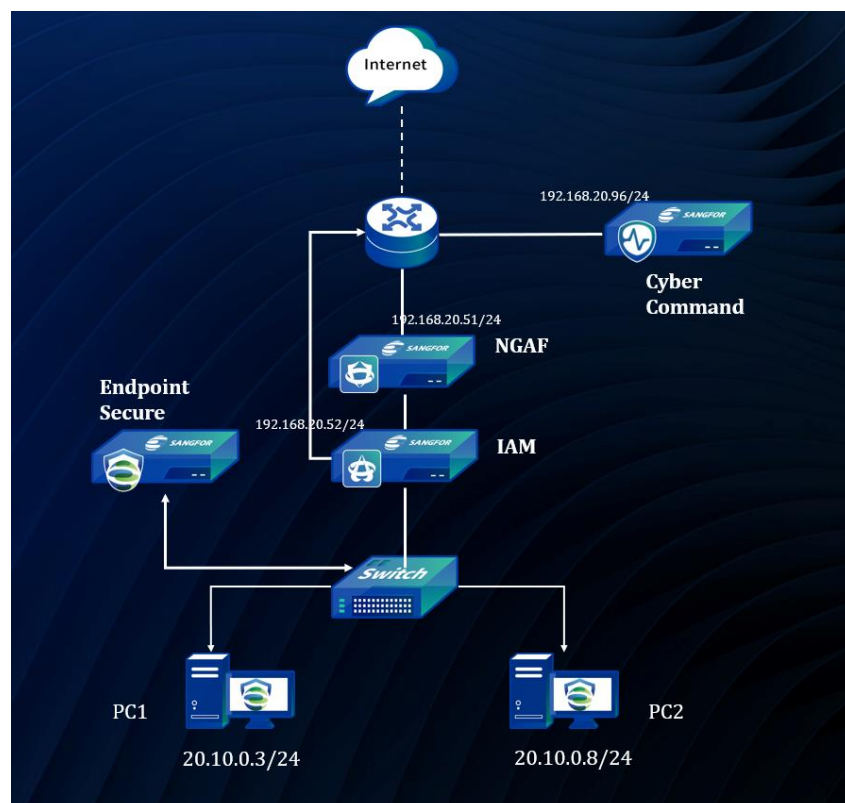
Konfirmasi apakah ES telah mengaktifkan Response License.

## Bagaimana untuk Berkorelasi dengan Endpoint Secure untuk Operasi Sederhana



2. Konfirmasi topologi network, seperti apakah CC dan ES dapat berkomunikasi, apakah route dapat dijangkau, and apakah ada perangkat NAT di tengah.
3. Ketika ES berkorelasi dengan CC, cukup untuk memulai koneksi dari pihak mana pun, yang berarti bahwa korelasi adalah satu arah.
4. ES perlu mengakses TCP port 7443 dari CC, dan CC perlu untuk mengakses TCP port 443. Perhatian khusus harus dibayar untuk skenario NAT . Jika ES port 443 dipetakan ke port 4430 port dari routing perangkat NGAF.

Bagaimana untuk Berkorelasi dengan Endpoint Secure untuk Operasi Sederhana



Maka Anda perlu untuk konfirmasi kebenaran dari port ketika konfigurasi linkage. Misalnya, ketika menghubungkan pada ES, CC tidak tahu bahwa NAT antara ES dan CC dilewatkan, dan secara otomatis akan diatur ke default TCP port 443 dari ES.

Correlate to Sangfor Device

Correlate NGAF and IAM devices to Endpoint Secure simply by entering Endpoint Secure Manager IP address on their managers respectively.

Peripheral Type :

Cyber Command

How to Connect?

\*Name :

CCOM

\*Device IP Address :

192.168.20.96

\*Local IP Address :

20.10.0.100

Remarks :

Remarks

Report Detection Logs :

☒ Enabled

Cancel

OK

## Bagaimana untuk Berkorelasi dengan Endpoint Secure untuk Operasi Sederhana

Total Synced Logs	Today's Logs	Last Synced
08	-	2021-05-18 09:43:07
27.58MB	0	2021-05-18 09:43:06

Faktanya, port 443 dari ES dipetakan ke port 4430 NGAF export, Anda perlu modifikasi secara manual.

Total Synced Logs	Today's Logs	Last Synced
08	-	2021-05-18 09:43:07
27.58MB	0	2021-05-18 09:43:06

5. Ketika konfigurasi korelasi policy pada ES, Report Detection Logs harus diaktifkan.

Edit

Peripheral Type :

Cyber Command

How to Connect?

\*Name :

CCOM

\*Device IP Address :

192.168.20.96

\*Local IP Address :

20.10.0.100

Remarks :

Remarks

Report Detection Logs :

☒ Enabled

Cancel

OK

6. Tentang sinkronisasi assets: Ketika ES dan CC berhasil berkorelasi, ES akan secara otomatis melakukan sinkronisasi assets ke CC. Premisnya adalah Anda harus mengaktifkan Auto Discover Assets di CC.

Cyber Command

V3.0.50C

Home

Response

Detection

Assets

Reports

More

≡

Assets

«

Settings

Asset Discovery and Approval

DHCP: ☐ Yes [Settings](#) ☒ No

☒ Auto Discover Assets

☒ Configure Asset Approval

Offline Assets

Status: ☐ Enable ☒ Disable

Others:  consecutive hours of no traffic

Inactive Assets

Asset Inactive:  consecutive days offline

Specified Trigger: Not specified [✎](#)

Others

Panel Name:  [?](#)

Update Time [?](#): ☒ Every early morning ☐ Update Now



## 1.2 Fungsi Korelasi

1. Setelah ES berkorelasi dengan CC, itu akan sinkronisasi logs dari brute force cracking, botnet, antivirus, dan webshell ke CC
2. ES dan CC linkage: menyediakan Korelasi Blok, Laporan Log, Scan Ancaman, Proses Forensik, Penanganan insiden Ancaman. Tidak menyediakan promosi dan deployment dari Agent
3. Untuk meningkatkan kemampuan deteksi security, Anda sebaiknya upgrade virus database ES dan CC ke yang terbaru.
4. Jika Anda ingin dapat terhubung secara otomatis dengan ES untuk menangani ancaman setelah CC menemukannya, jangan lupa untuk konfigurasi otomatis response policy di CC.
5. Ketika CC menunjukkan bahwa ES Agent tidak ter-instal, informasi berikut perlu dikonfirmasi:  
  
Waktu instalasi Agen terlalu pendek, dan assets belum disinkronkan ke CC, dan status instalasi Agent tidak muncul setiap 6 jam.  
  
Assets yang berbeda memiliki IP yang sama, dan prompt untuk menginstal adalah assets dari group asset lainnya.  
  
CC tidak diaktifkan secara otomatis discover assets.



**SANGFOR**

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc