SANGFOR

Cyber Command

Best Practices for Configuration_How to Correlate with Endpoint Secure to Simply the Operation

Version 3.0.49

Change Log

Date	Change Description
April 2, 2021	Document release.
May 17, 2021	Document update.

CONTENT

Chapter 1 Basic

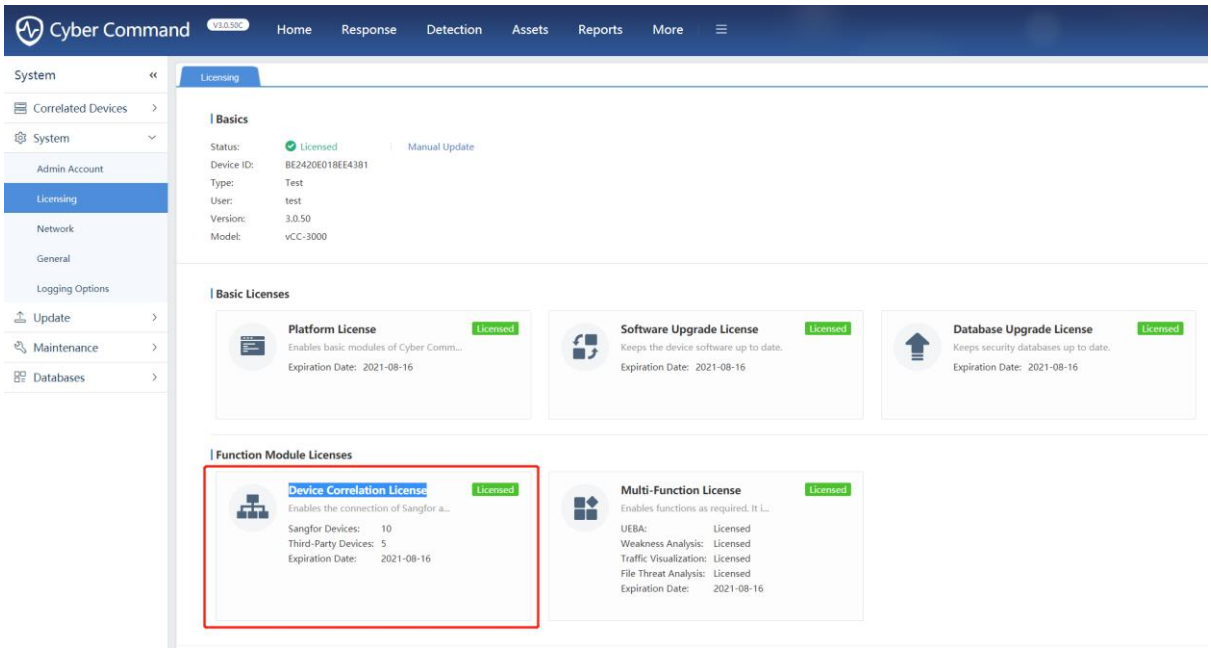
Related documents:

Best Practices for Configuration usually include selection of deployment mode, configuration ideas, information collection, function limitations, version differences. Regarding ***How to Correlate with Endpoint Secure to Simply the Operation***, if you want to learn about general POC scenarios and detailed configuration steps, please refer to the following link:

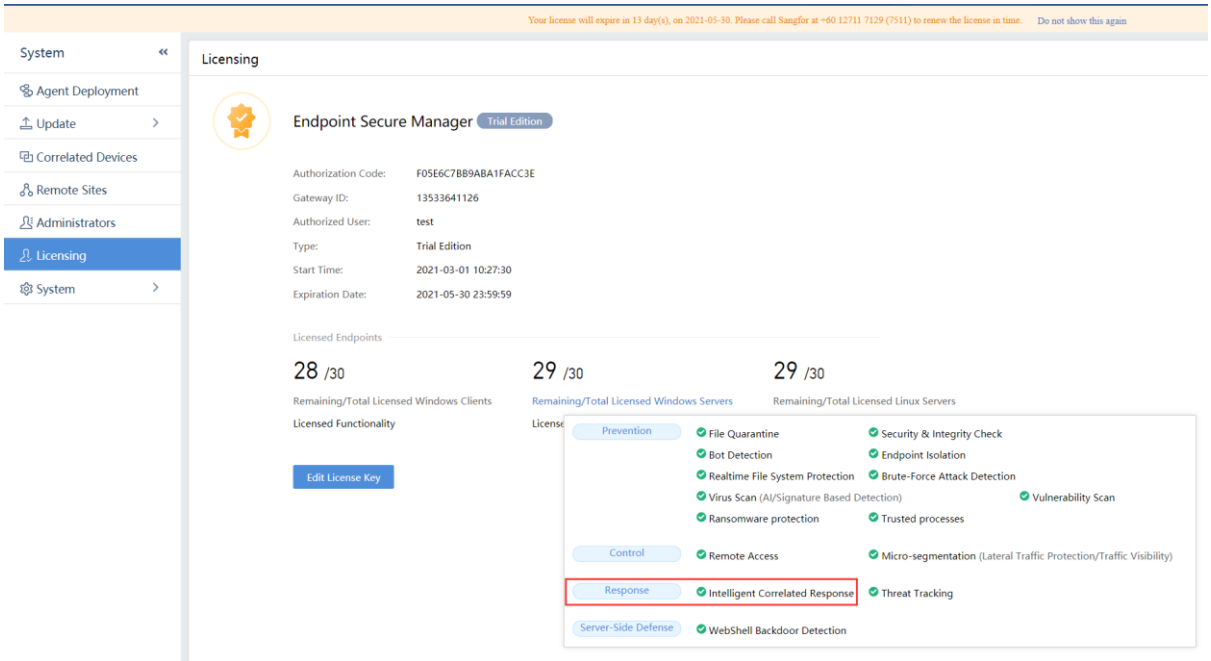
https://community.sangfor.com/plugin.php?id=sangfor_databases:index&mod=viewdatabase&tid=4589

1.1 Confirm Basic Configuration and Deployment

1. Confirm whether CCOM has enabled Device Correlation License.



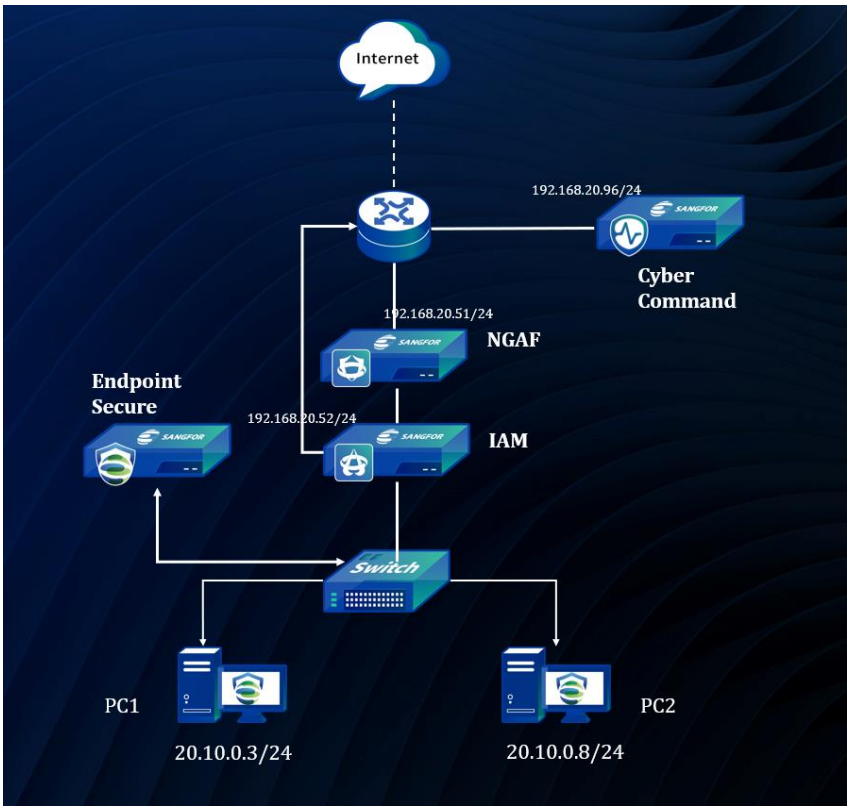
Confirm whether ES has enabled Response License.



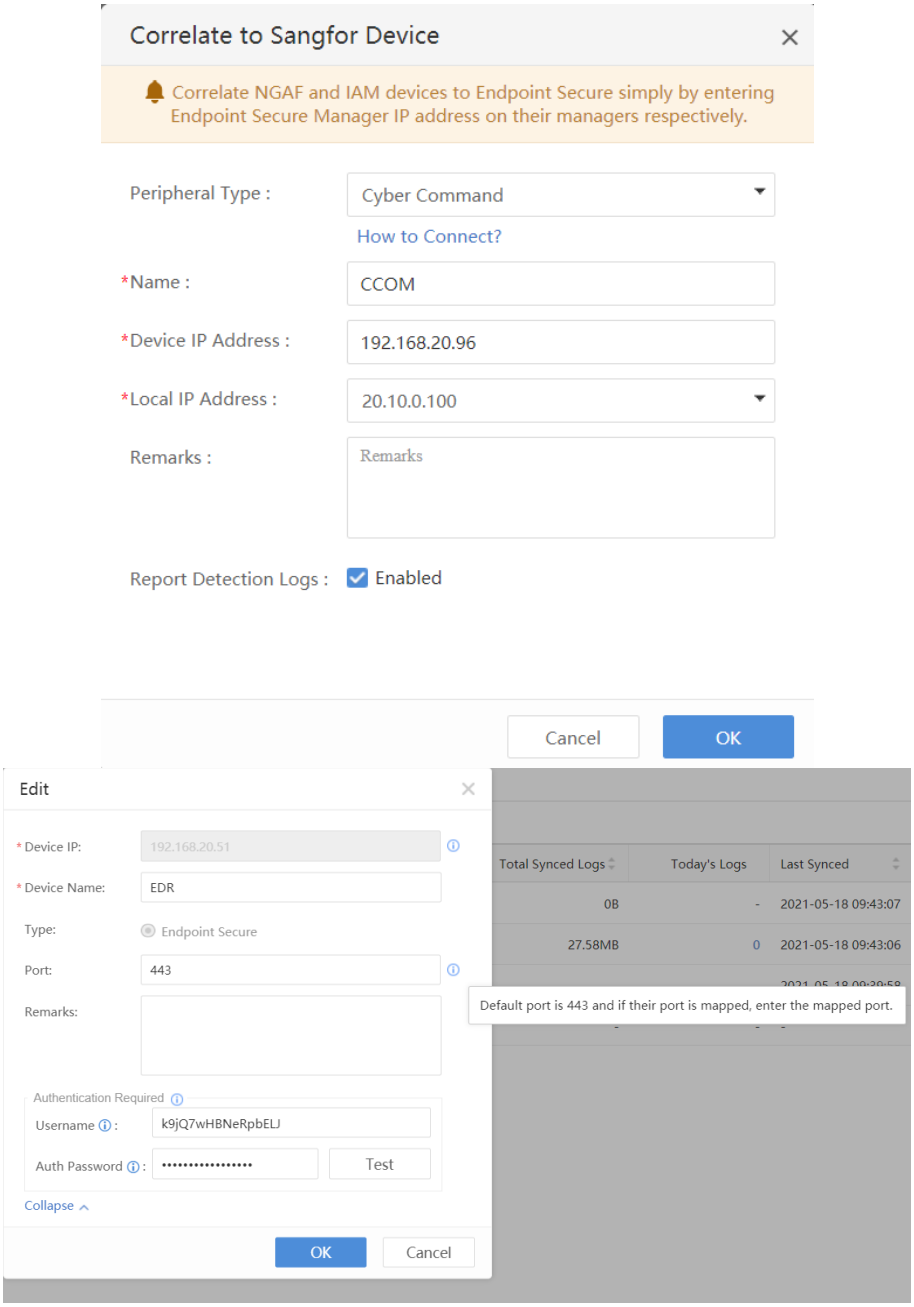
2. Confirm the network topology, such as whether CC and ES can communicate, whether the route is reachable, and whether there is a NAT device in the middle.

3. When ES is correlated to CC, it is sufficient to initiate a connection from any party, which means that the configuration correlation is one-way

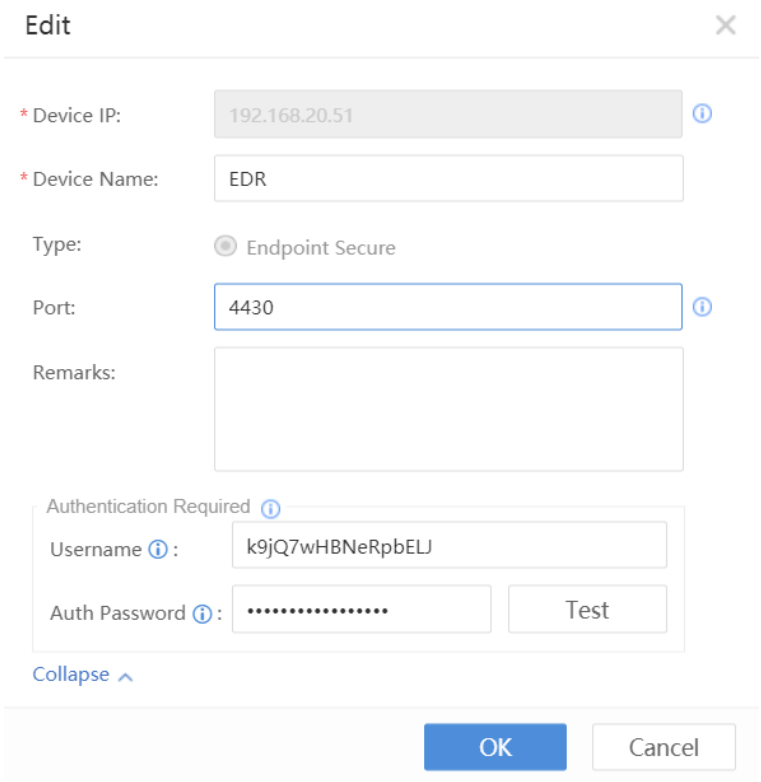
4. ES needs to access the TCP port 7443 of the CC, and CC needs to access the TCP port 443. Special attention should be paid to the NAT scenario. If the ES port 443 is mapped to the 4430 port of the routing NGAF device



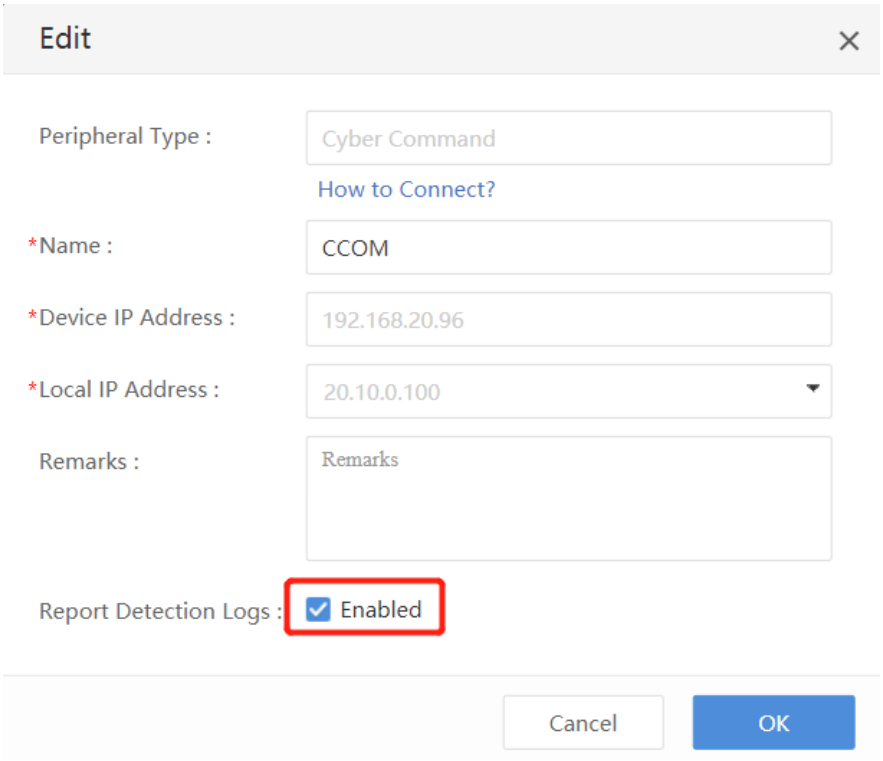
Then you need to confirm the correctness of the port when configuring the linkage. For example, when connecting on the ES, the CC does not know that the NAT between the ES and the CC is passed, and it will automatically be set to the default TCP 443 port of the ES.



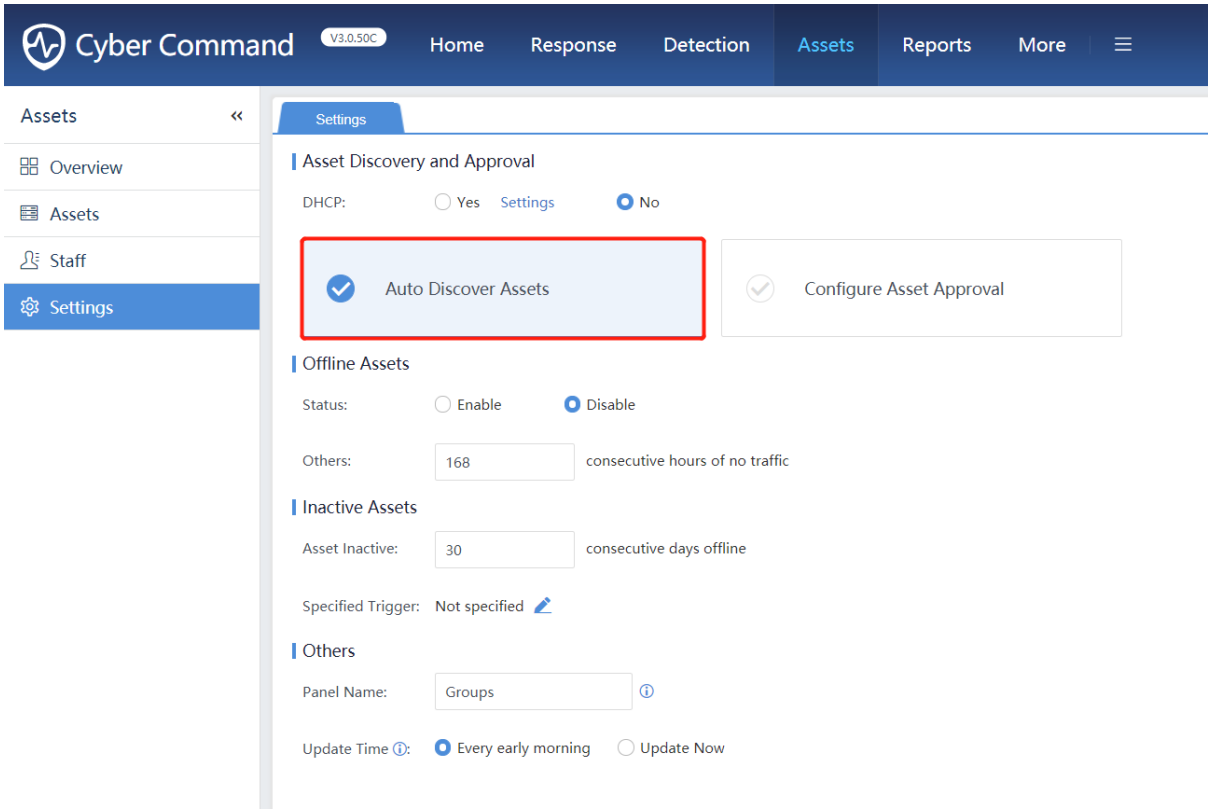
In fact, port 443 of ES is mapped to port 4430 of NGAF export, you need to modify it manually.



5. When configuring the correlation policy on the ES, Report Detection Logs must be enabled.



6. About asset synchronization: When ES and CC are successfully correlated, ES will automatically synchronize assets to CC. The premise is that you must enable Auto Discover Assets on CC.



1.2 Correlation Function

1. After ES is correlated to CC, it will synchronize the logs of brute force cracking, botnet, antivirus, and webshell to CC

2. ES and CC linkage: support Correlated Block, Log reporting, Threat Scan, Process Forensics, Threat Incident Handling. Does not support the promotion and deployment of Agent

3. In order to improve the security detection ability, you'd better upgrade the virus database of ES and CC to the latest.

4. If you want to be able to automatically link with ES to deal with the threat after CC finds it, please don't forget to configure the automatic response policy on CC.

5. When CC shows that ES Agent is not installed, the following information needs to be confirmed:

The Agent installation time is too short, and the assets have not been synchronized to the CC, and the Agent installation status does not occur every 6 hours.

Different assets have the same IP, and the prompt to install is the assets of other asset groups.

CC is not enabled to automatically discover assets.