Cyber Command

Best Practices for Configuration_How to Correlate with IAM to Simply the Operation

Version 3.0.49

Change Log

Date	Change Description
May 7, 2021	Document release.
May 17, 2021	Document update.

CONTENT

Chapter 1 Basic

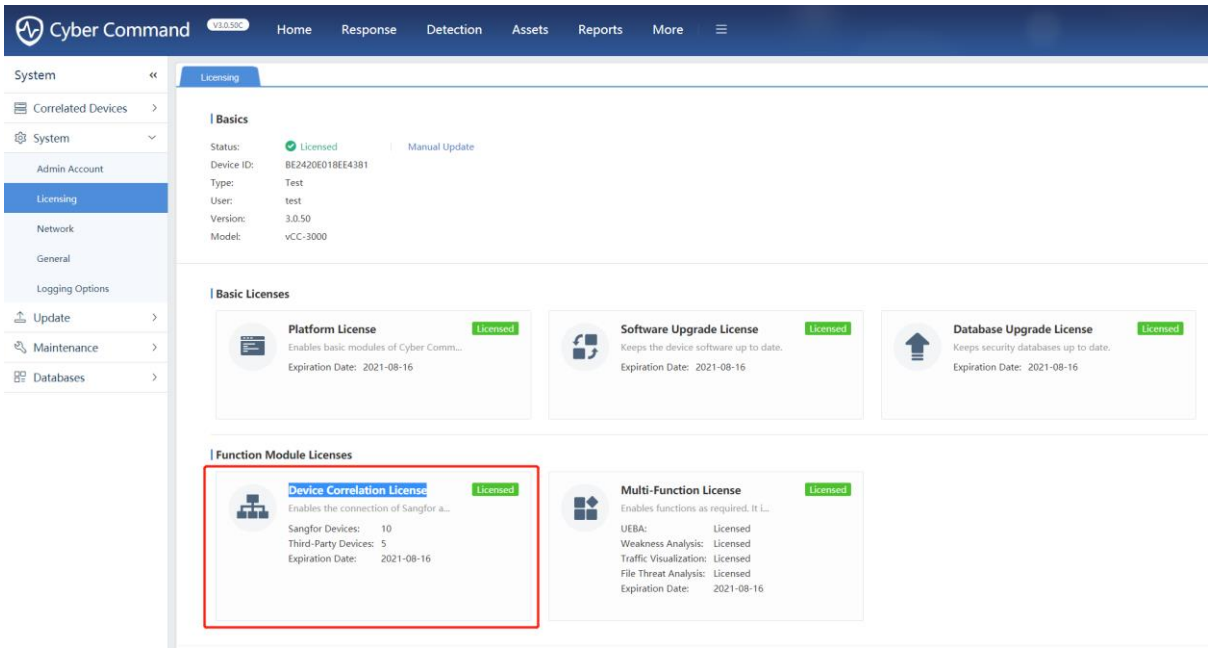
Related documents:

Best Practices for Configuration usually include selection of deployment mode, configuration ideas, information collection, function limitations, version differences. Regarding ***How to Correlate with IAM 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=4590

1.1 Confirm Basic Configuration and Deployment

1. Confirm whether CCOM has enabled Device Correlation License.

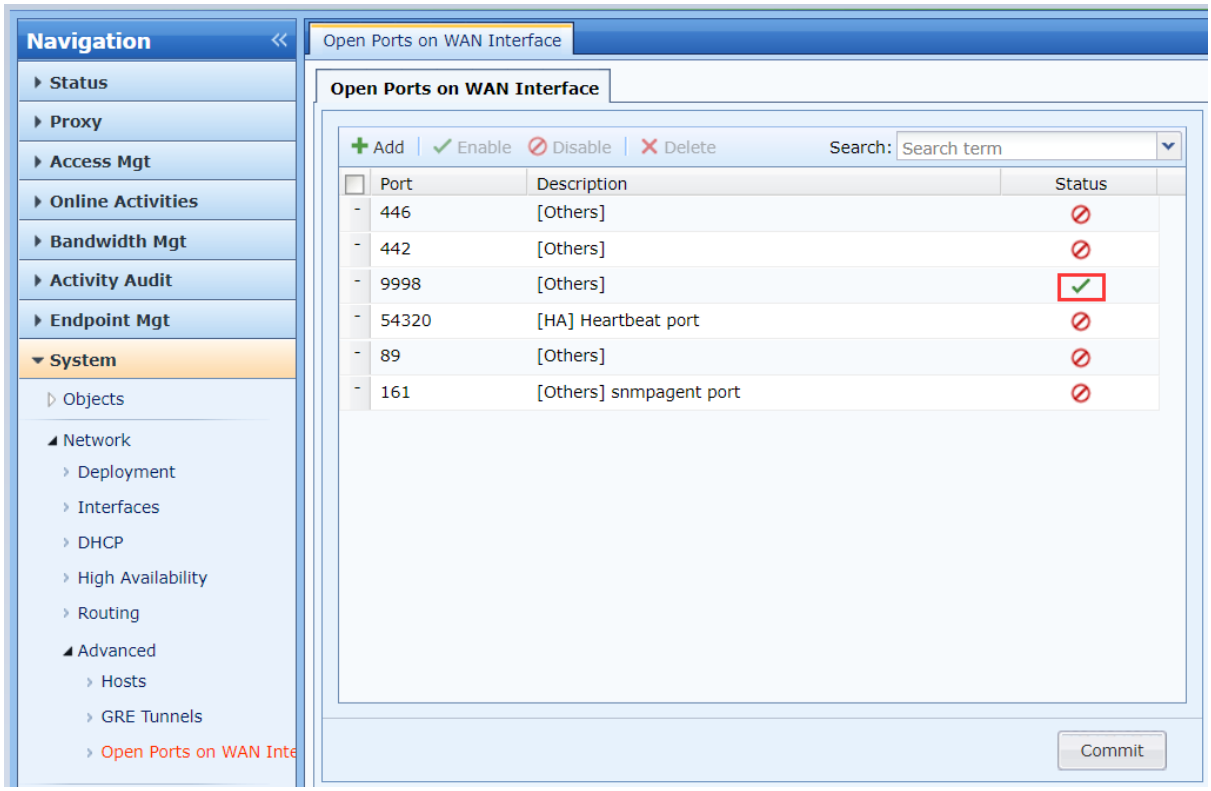


2. Confirm the network topology, such as whether CC and IAG can communicate, whether the route is reachable, and whether there is a NAT device in the middle.

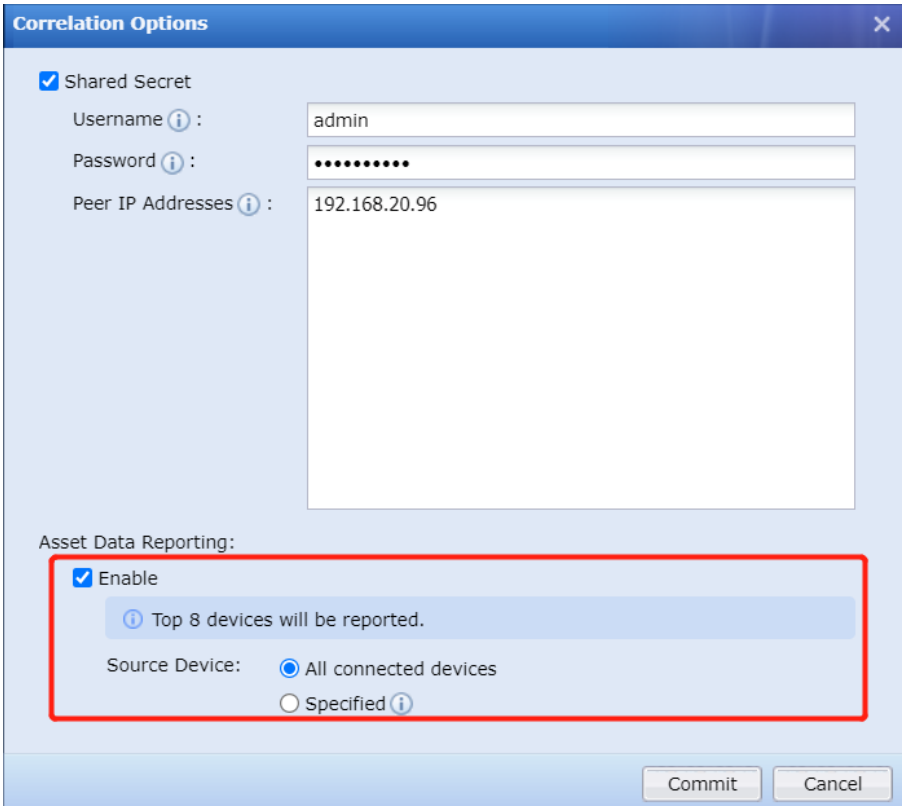
3. When IAG is correlated to CC, it needs to be configured on IAG and CC at the same time.

4. IAG accesses the port 1775 (UDP, used to synchronize users) of CC, and CC accesses the TCP port 7443 and port 9998 of IAG. If connected device IP address is translated, enter the translated IP address.

5. If IAG is deployed in routing mode, and CC is connected to IAG's WAN port IP to communicate with IAG, then the port needs to be opened on IAG.



6. IAG supports reporting assets to CC starting from version 13.0.15, which needs to be enabled in the correlation settings. The user and password here are not the account and password of CC or IAG console, you can customize it.

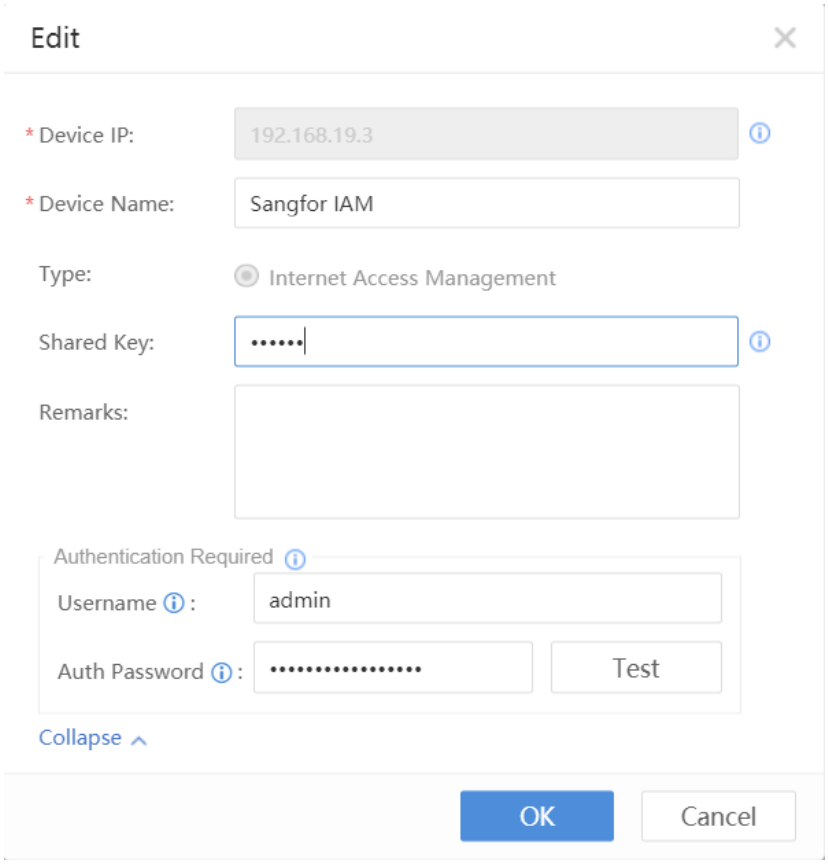


7. If you need to synchronize online users on IAG to CC, you must configure Sangfor Appliance on IAG, and the shared secret key must be consistent with the shared secret key in the linkage configuration on CC.

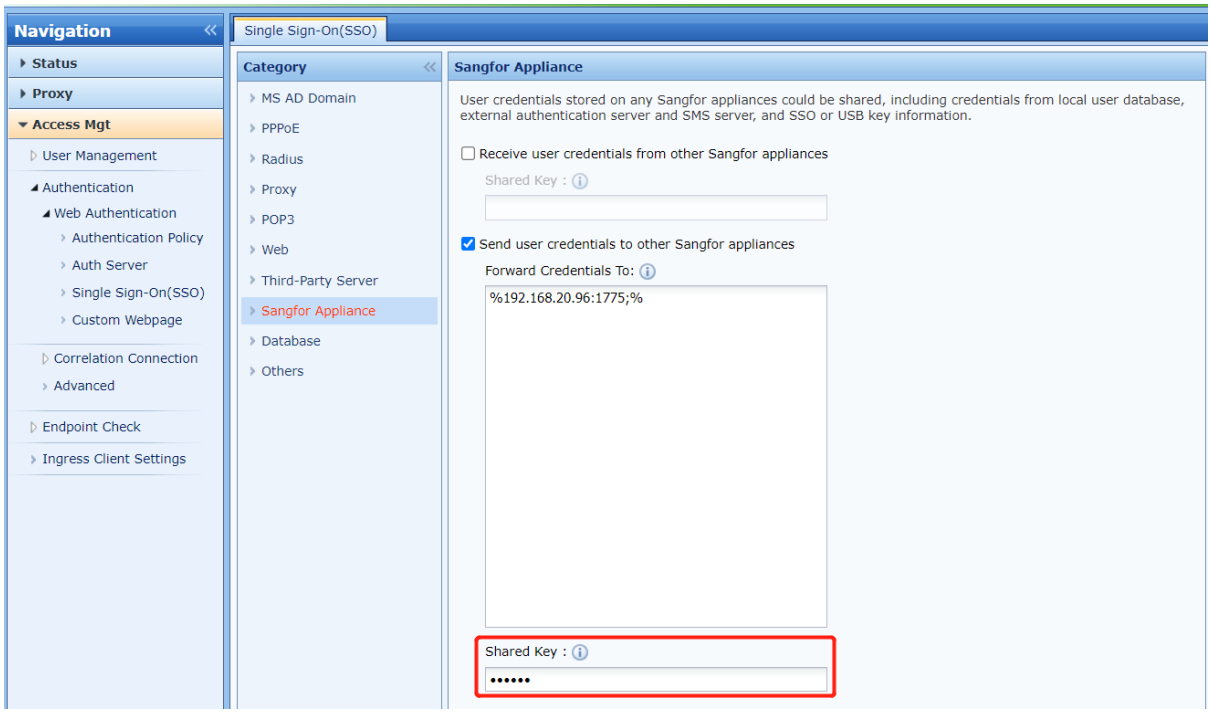
IAG's Sangfor authentication forwarding is to forward the authentication information of local password

authentication, external password authentication, SMS authentication, single sign-on, and dkey authentication users. It will not forward the information of Open Authentication users to CC.

CC Side:



IAG Side:



1.2 Correlation Function

1. After the IAG is connected to the CC, the CC is linked to the IAG to do Browsing Risk Notification, which can remind the user of the security incidents discovered by the terminal through web redirection, and then freeze the users who have found the security problem to reduce the impact of the threat surface.

2. IAG can detect botnets, but IAG does not upload security logs to CC. Therefore, IAG and CC are usually not used alone, but ES is used to further check the security of the terminal.

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

4. The CC correlated with IAG is mainly used for detecting high-risk hosts, and then issuing a policy to freeze the user. So please make sure that the frozen user is in the online user list of IAG. If the user is not among the online users, the freezing policy will be invalid.