Cyber Command

Best Practices for Scenarios_How to Use Cyber Command to Manage Assets

Version 3.0.49

Change Log

Date	Change Description
Mar 16, 2021	Document release.
May 17, 2021	Document update.

CONTENT

Chapter 1 Scenario

1.1 Scenario

Difficult to manage asset life cycle

Due to the continuous evolution of IT architecture and the continuous innovation of system applications, coupled with the continuous addition of enterprises' assets on the cloud, the enterprise's assets have shown explosive and diversified growth. Asset categories are diversified, asset storage and withdrawal are frequent, asset information adjustments and changes are frequent, all of which make asset life cycle management more and more complicated and difficult to control.

Inefficient asset management methods

The difficulty of asset management has increased, and the current methods of asset management are low. Although many products currently have asset management functions, the management method still generally stays in the manual registration method, which is prone to omissions and errors. At the same time, each product is limited by manufacturers and functional applications, each forming an isolated island of asset information, leading to repeated maintenance and repeated configuration of information, increasing the difficulty of data maintenance, and making asset management face huge challenges.

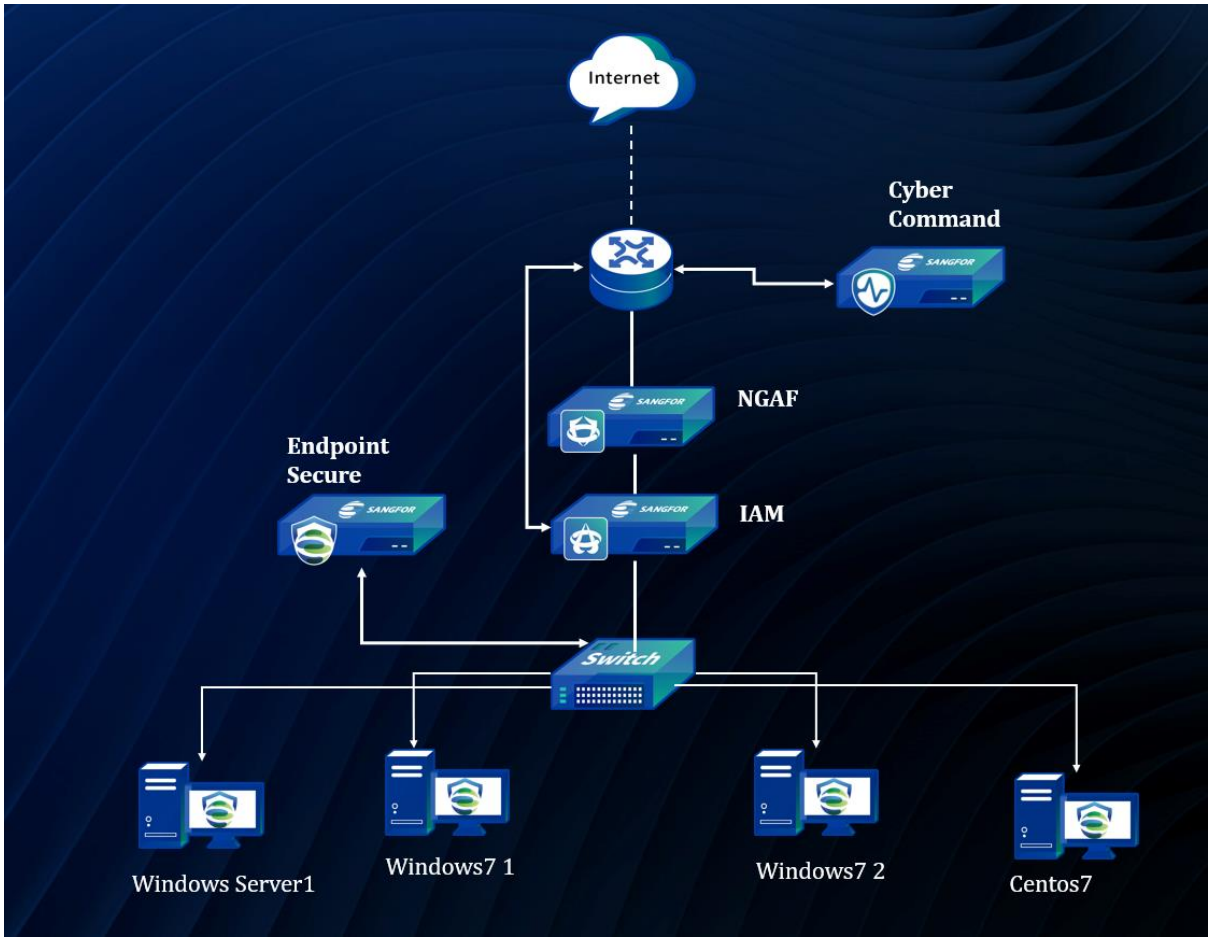
Asset vulnerability has increased significantly

Due to the frequent changes of IT assets, enterprises cannot control the status of existing assets in real time, and thus lose the cornerstone of conventional security inspection and emergency security reinforcement, and the vulnerability of assets will be more obvious. Corresponding to it is the increasing number of vulnerabilities and the ever-accelerating speed of response to black production, all of which make asset risk management and control face new challenges.

Long enterprise risk emergency response cycle

Under the traditional IT deployment method, enterprises spend the most time combing affected assets in the emergency response process, accounting for about 40%. Therefore, when a risk occurs, it is difficult for enterprises to accurately locate the affected assets, leading to risk spread The cycle is lengthened, and time is the lifeline of security offensive and defensive confrontation. Traditional risk emergency response cannot meet the gradually evolving security management and technological development needs.

1.2 Topology



1.3 Correlation Introduction

1. IAM before 13.0.15 version doesn't support synchronize assets to Cyber Command, only support synchronize online users information to Cyber Command by Sangfor Appliance of SSO.

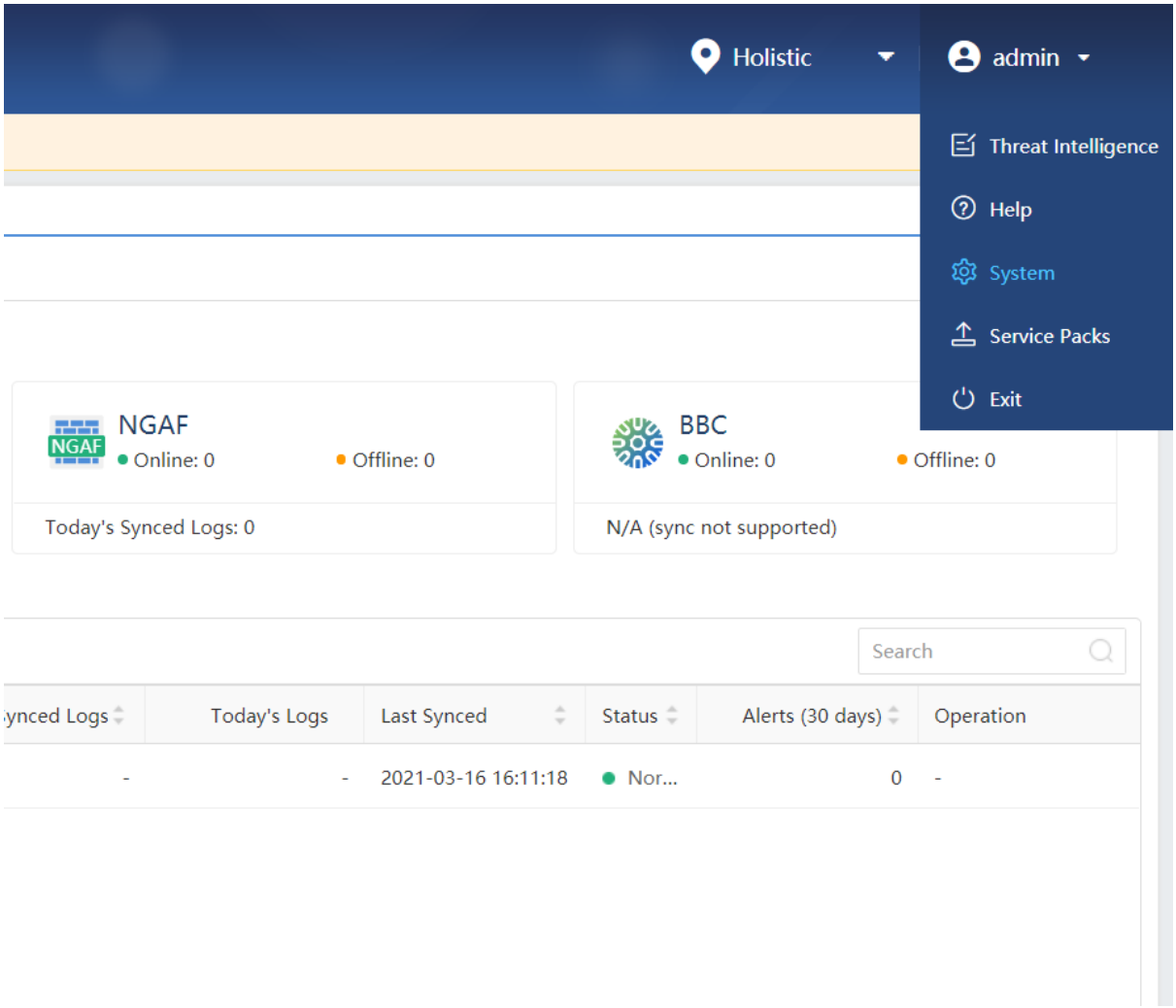
2. IAM after 13.0.15 version supports synchronize assets to Cyber Command, also supports synchronize online users information to Cyber Command by Sangfor Appliance of SSO.

3. NGAF after 8.0.23 version doesn't support synchronize assets to Cyber Command for NGAF use new structure of database

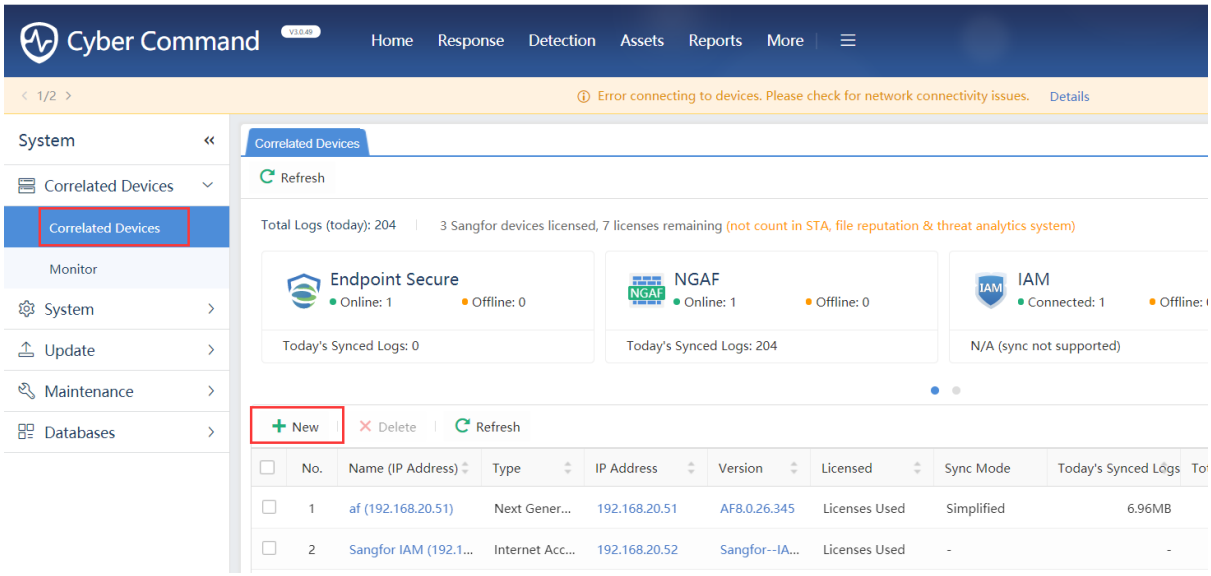
Chapter 2 Correlate with Endpoint Secure to Manage Assets

2.1 Configure Cyber Command

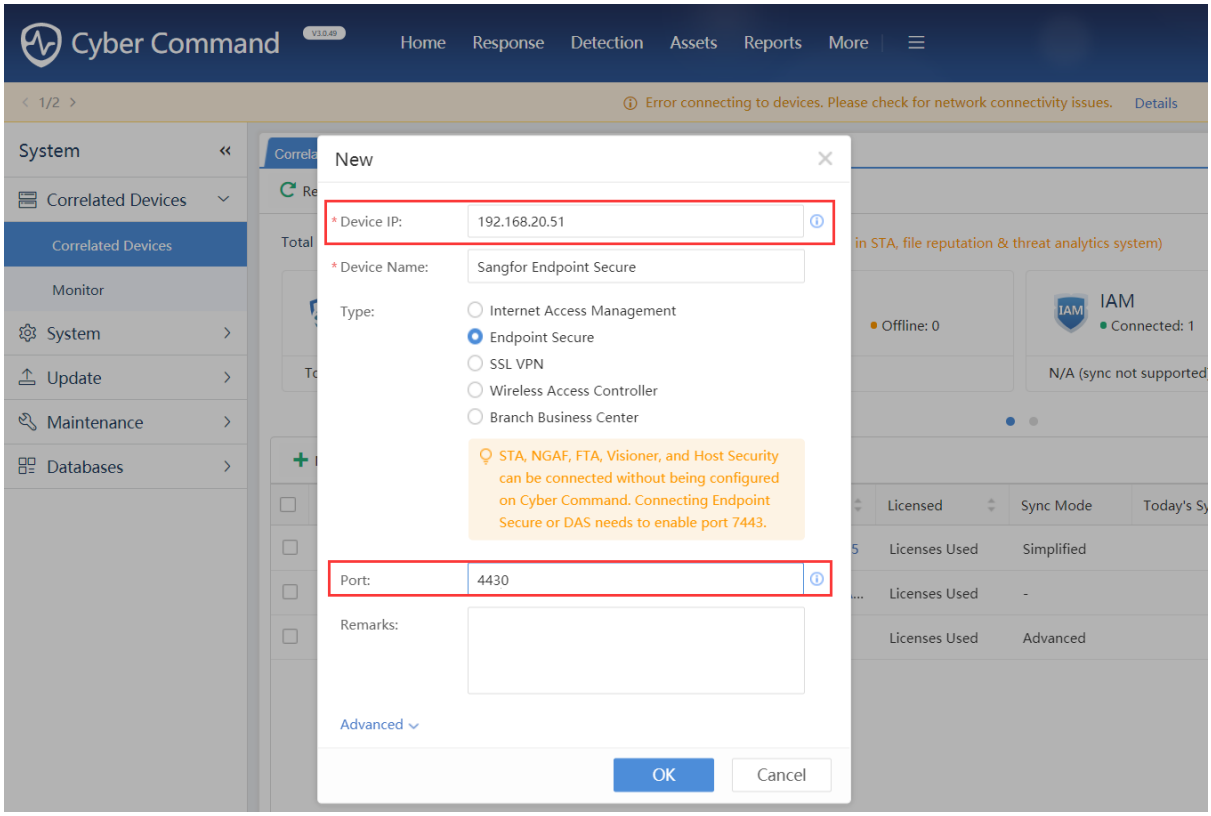
1. Go to System Path.



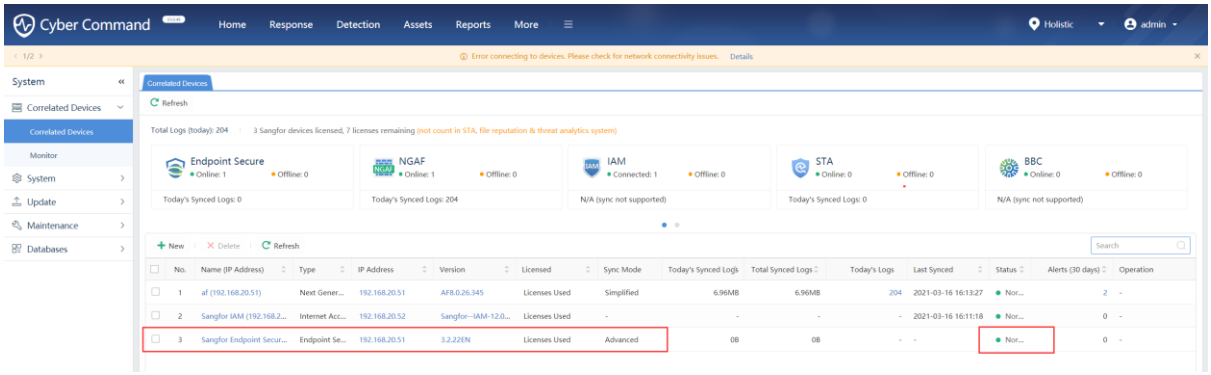
2. Go to Correlated Devices-> Correlated Devices path, and click New to create Correlation.



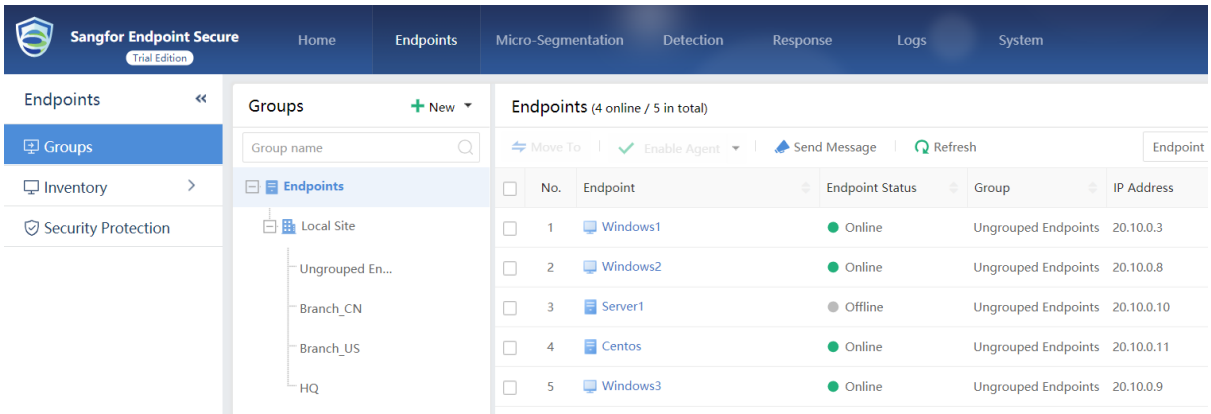
3. Input the IP of Endpoint Secure and the Port, if Endpoint Secure deployed after a NAT device, Please map the 443 port of Endpoint Secure to the NAT device. For example, here is the 4430 port mapped to the NAT device.



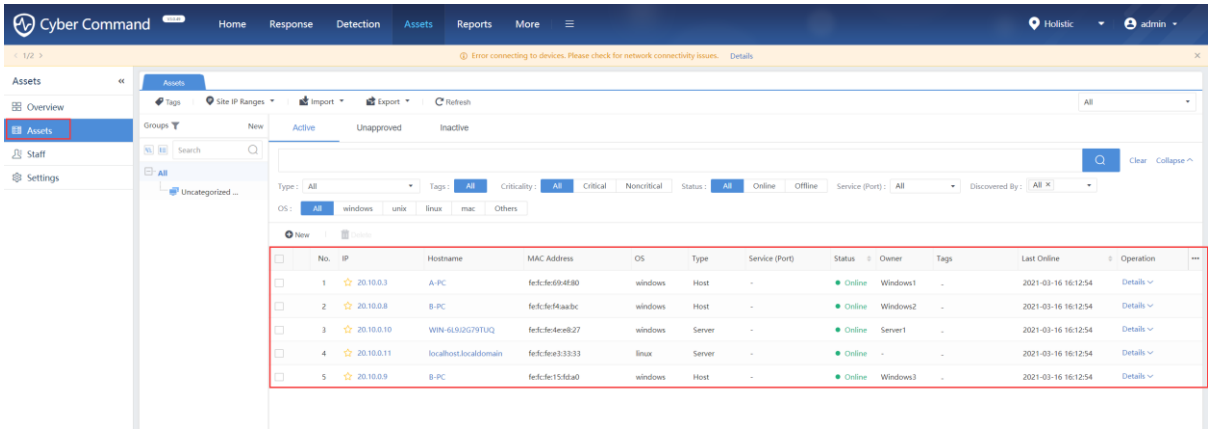
4. After click OK, you can see the correlation status in console.



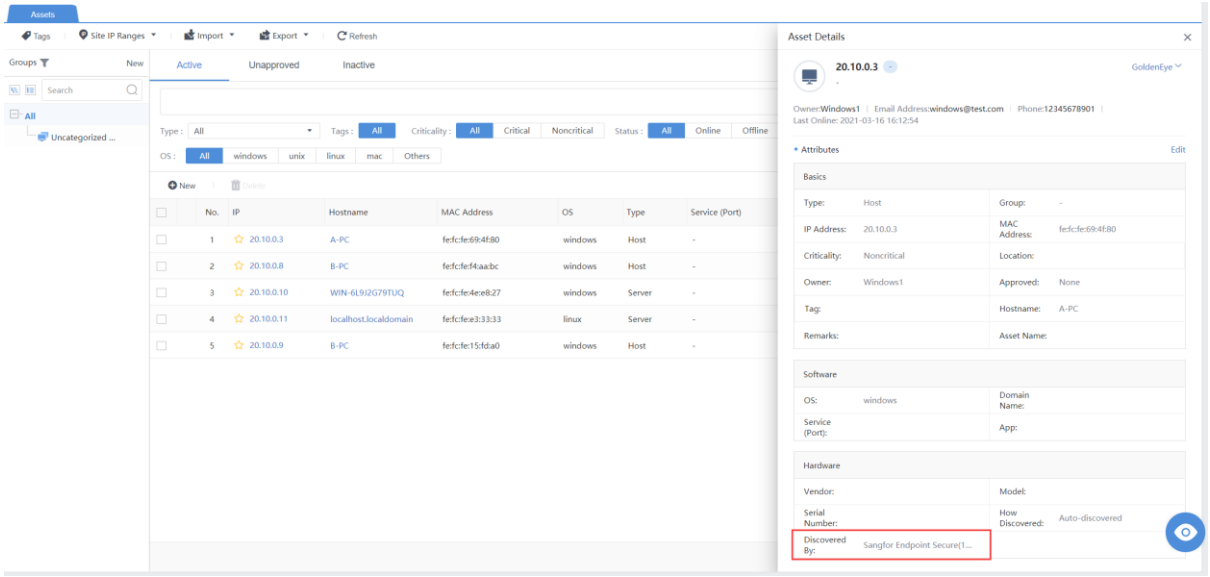
5. You can check whether there exists assets in Endpoint Secure.



6. If you there exists in Endpoint Secure, you Go to Assets->Assets in Cyber Command to check whether assts has been synchronized to Cybercommand.



7. You can view the details to see the assets source, such as following detail, you can see this asset discovered by Endpoint Secure.

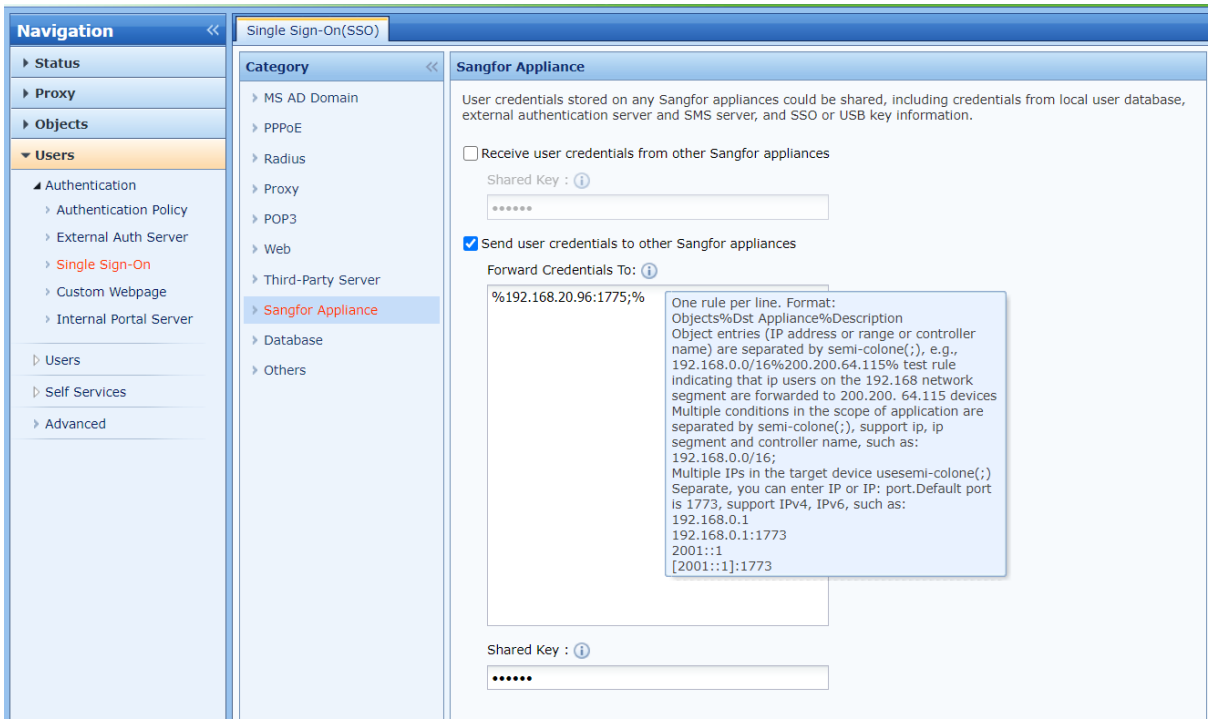


Chapter 3 Correlate with IAM to Manage Assets

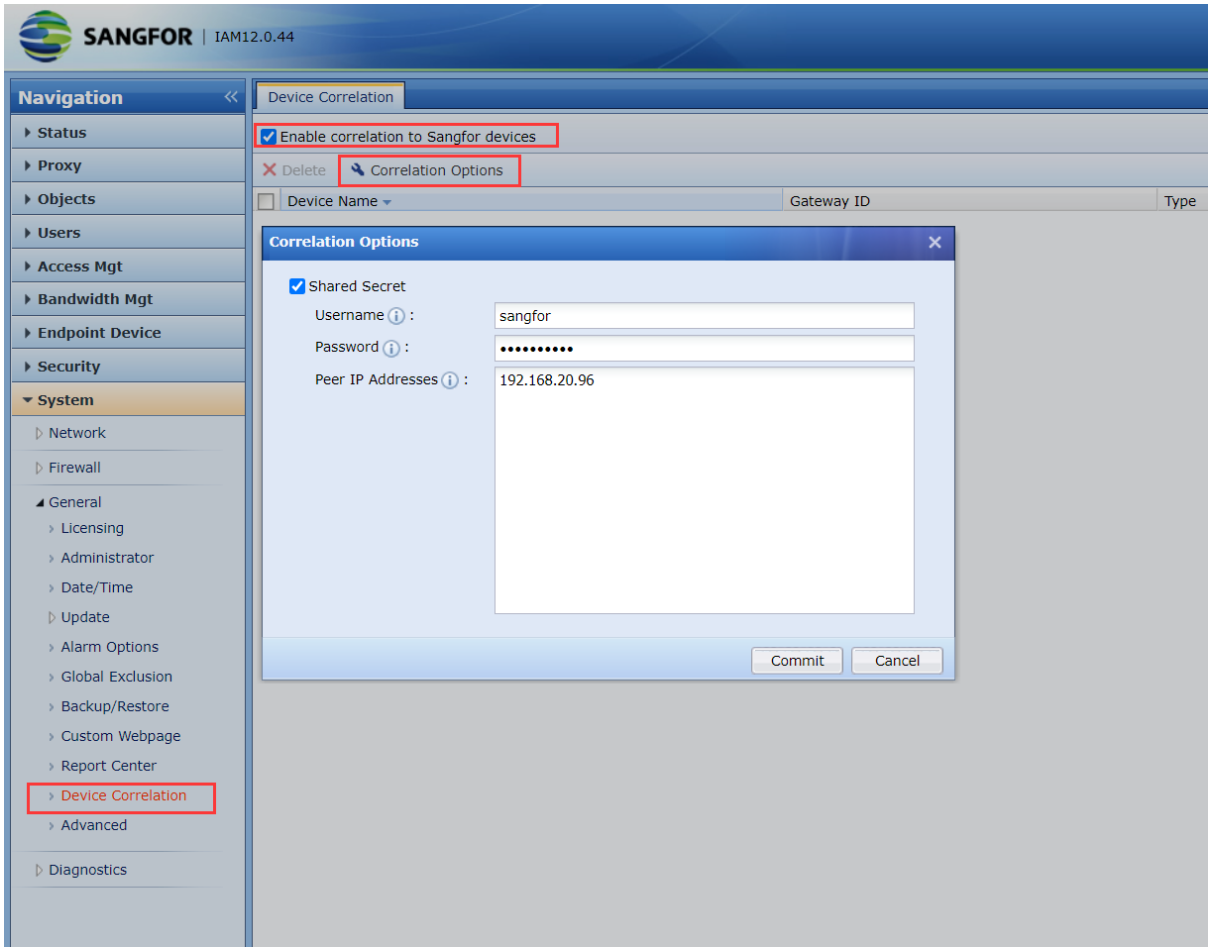
3.1 With IAM Before 13.0.15 version

3.1.1 Configure IAM

1. Go to Users->Single Sign On->Sangfor Appliance, then fill in the IP of Cyber Command and set the destination port as 1775, 1775 port is general port for authentication between two sangfor devices.

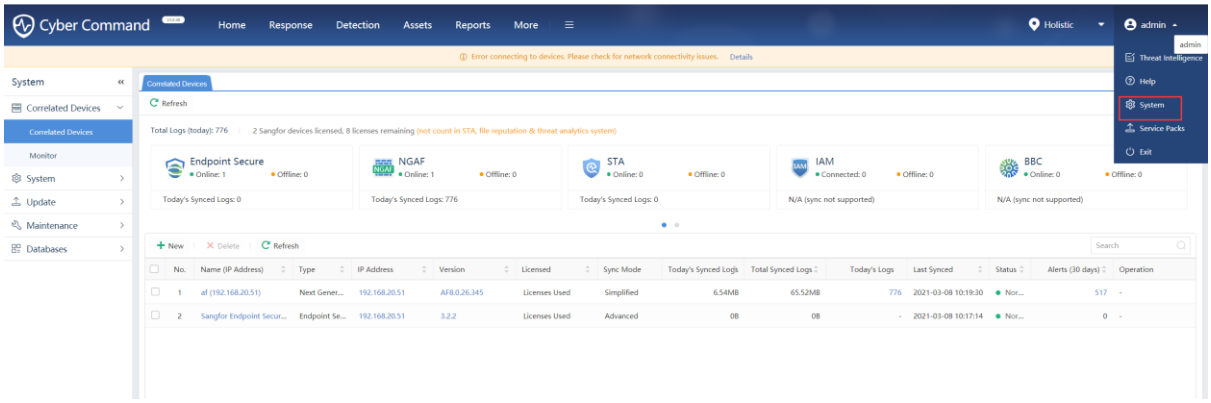


2.Go to System-> General->Device Correlation, input the IP of Cyber Command and you can set username and password.

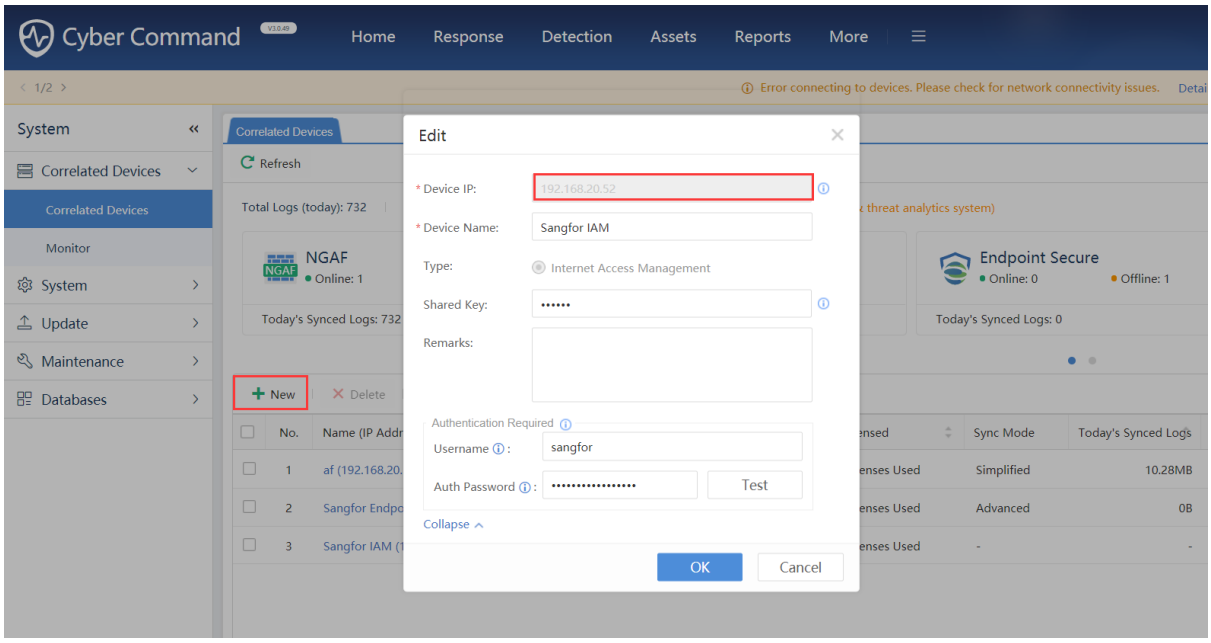


3.1.2 Configure Cyber Command

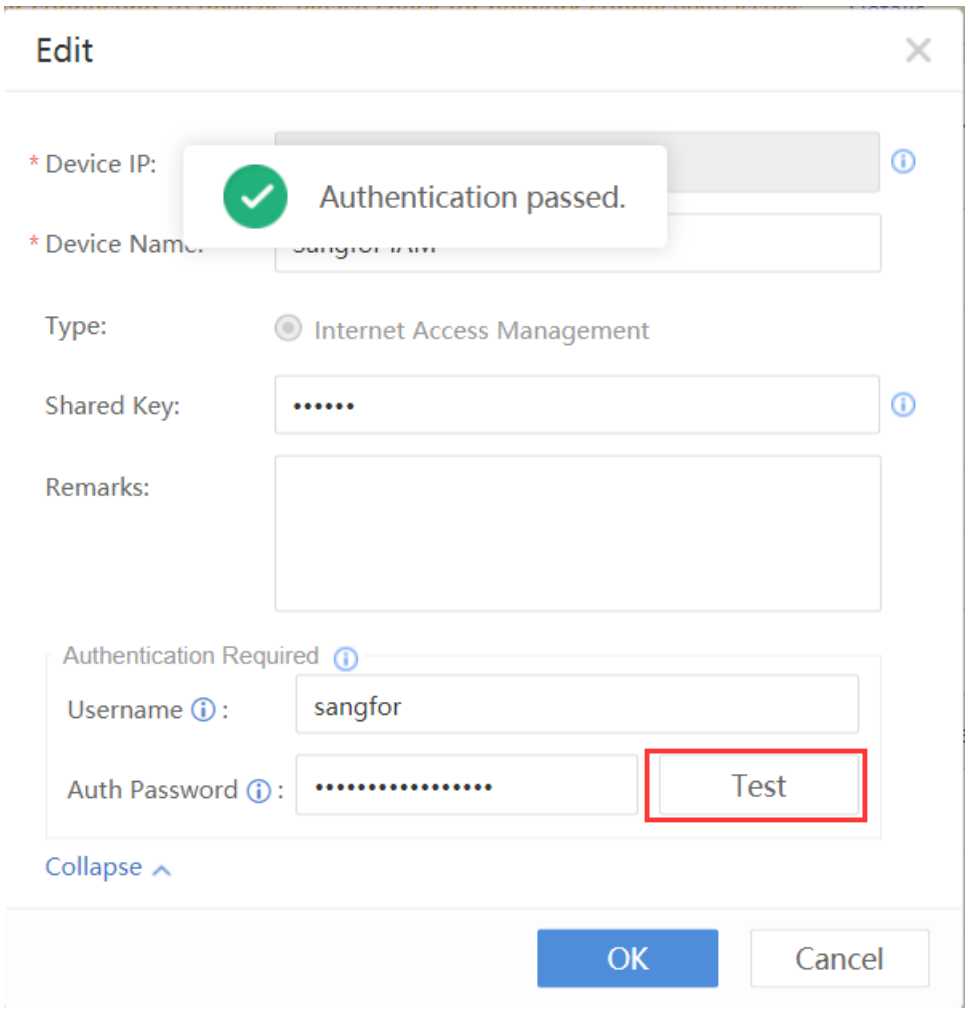
1. Go to System->Correlated Devices-> Correlated Devices.



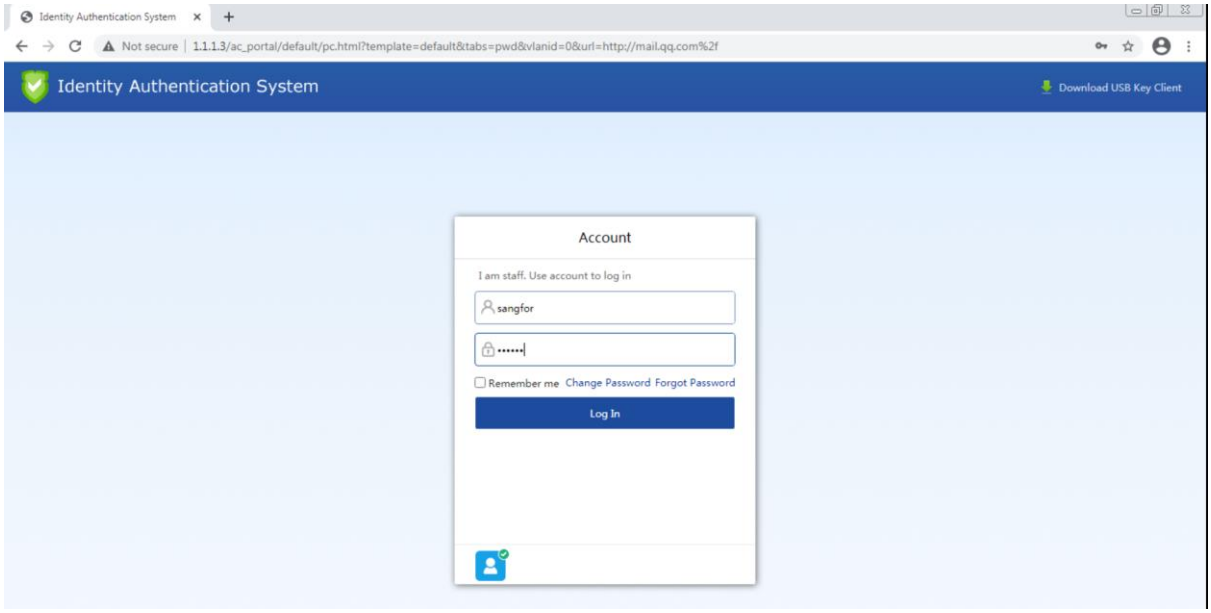
2. Click New to create correlation, you must input the correct the username and password that you configured in IAM, and if you need to synchronize online users of IAM to Cyber Command, you must input the Shared Key same as you configured in IAM SSO Options.

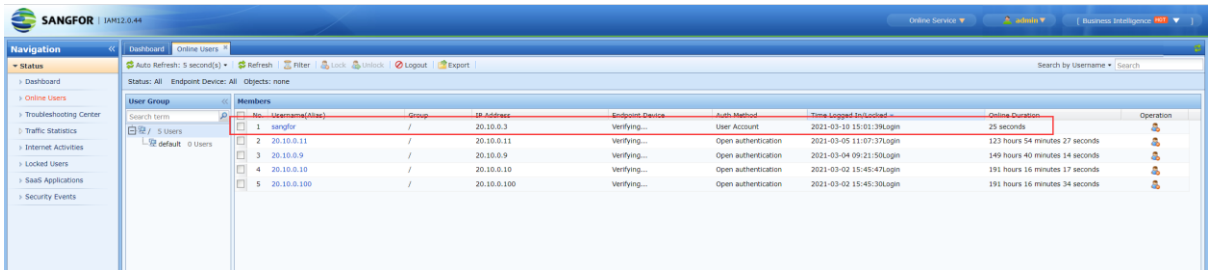


3. If you are not sure whether the username and password were correct, you can click Test to check the account validity.

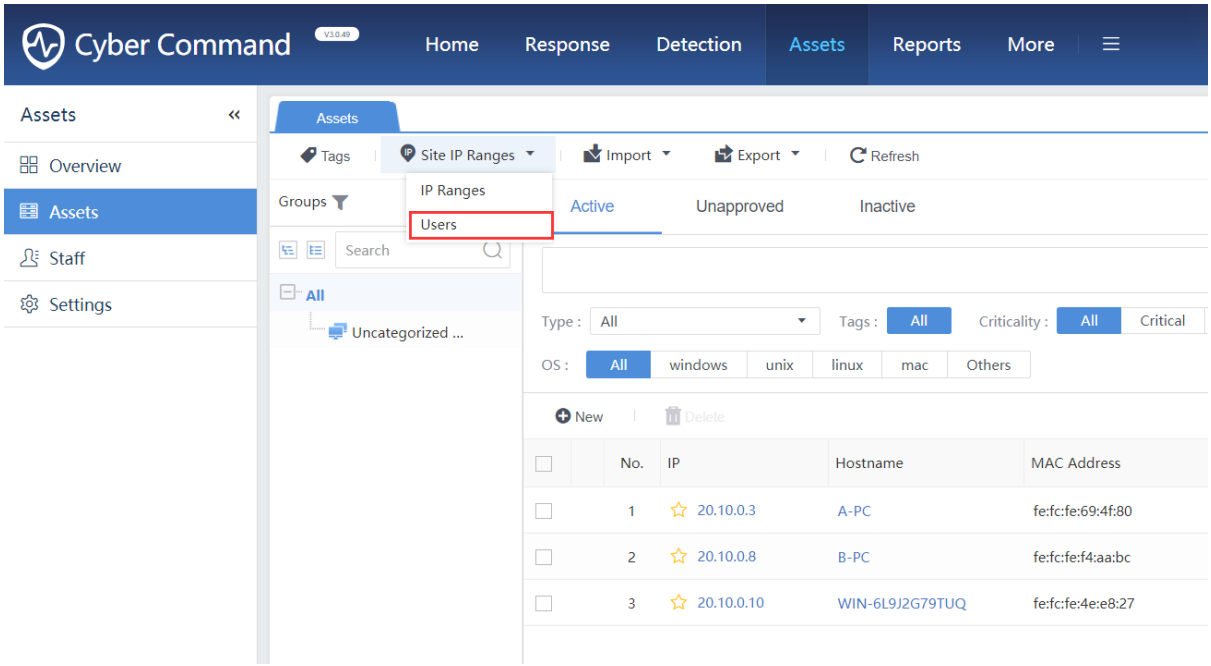


4. If you configure password based authentication policy in IAM, when PC try to access the internet, the IAM will direct the access page to authentication page, if user authenticates successfully, the username will be online in IAM and IAM will forward the authentication to Cyber Command.

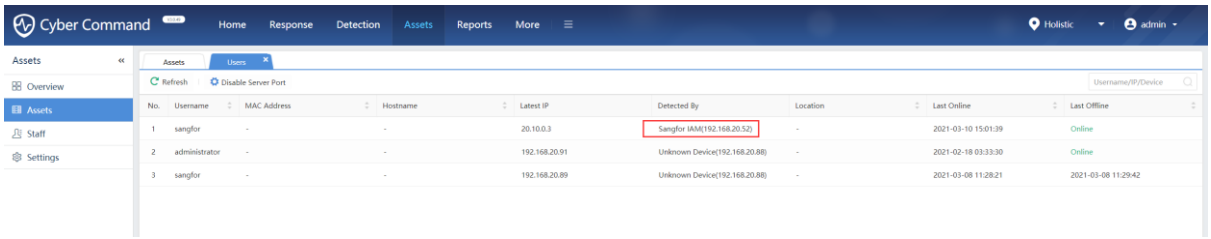




5. You can Go to Assets->Assets path and select the Users as following picture.



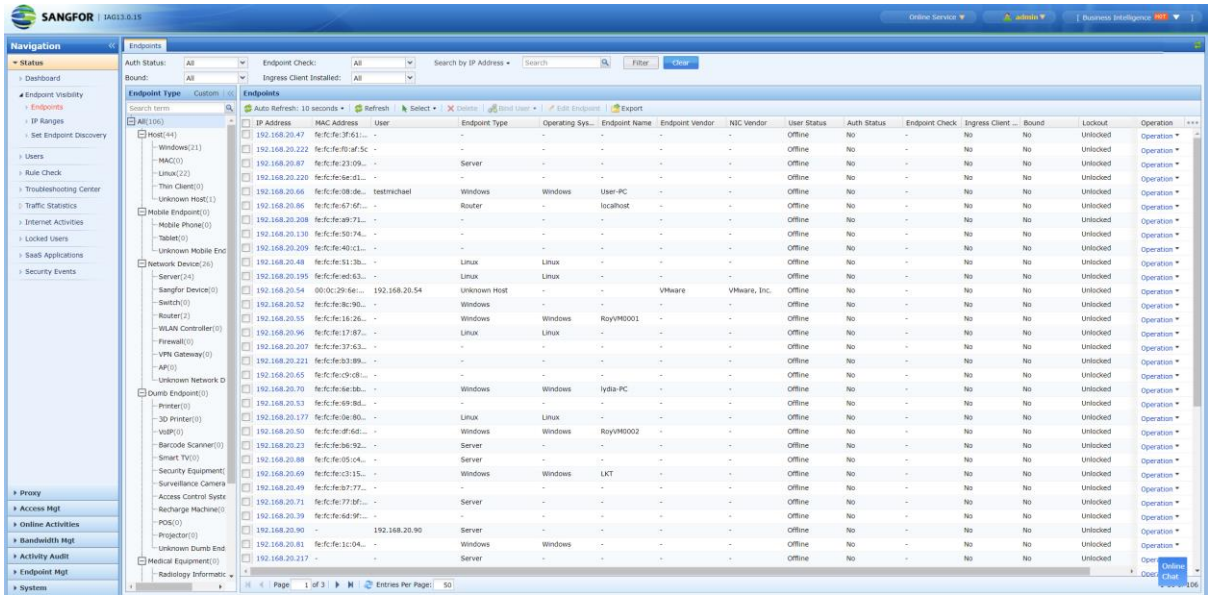
6. Then you can see the user information already synchronized to Cyber Command.



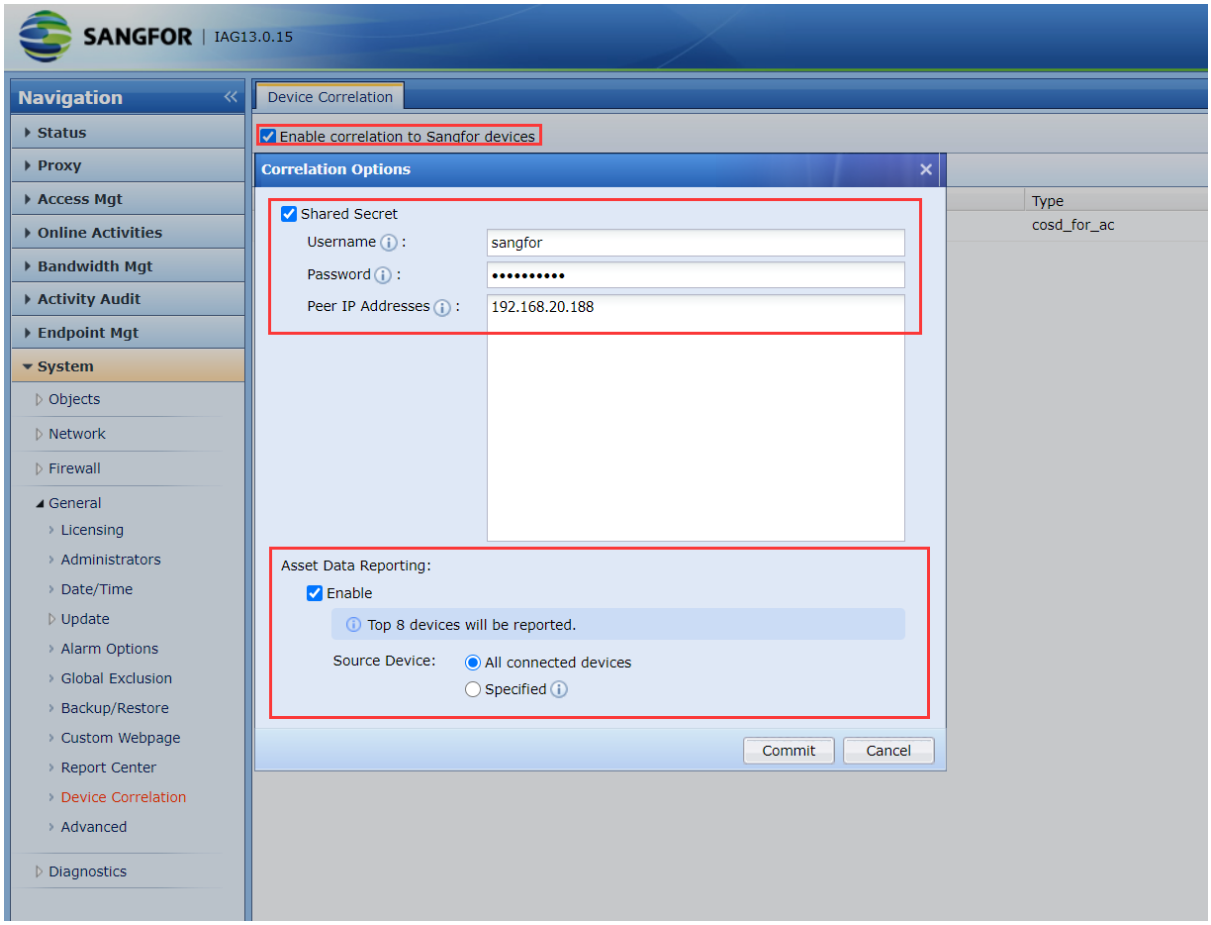
3.2 With IAG After 13.0.15 version

3.2.1 Configure IAG

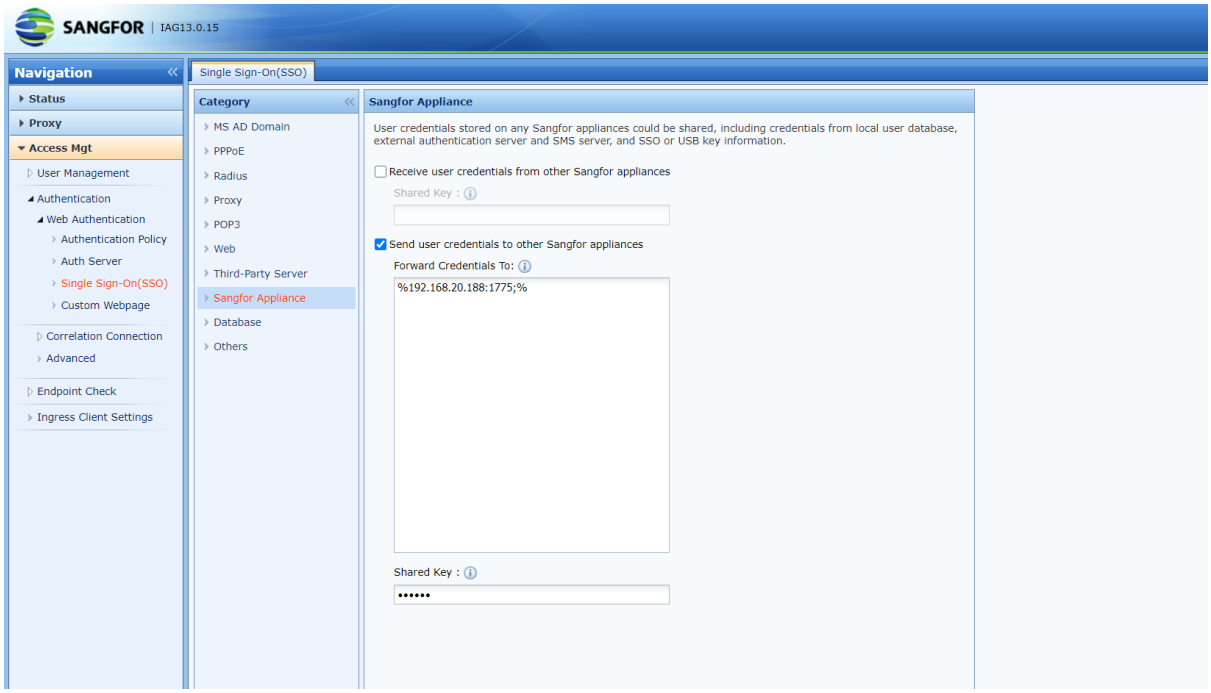
1.Check whether there exists assets in IAG, you can go to Status->Endpoint Visibility> Endpoints to check.



2. Go to System-> General->Device Correlation, input the IP of Cyber Command and you can set username and password. If you want to Synchronize the assets to Cyber Command, please check the Asset Data Reporting.

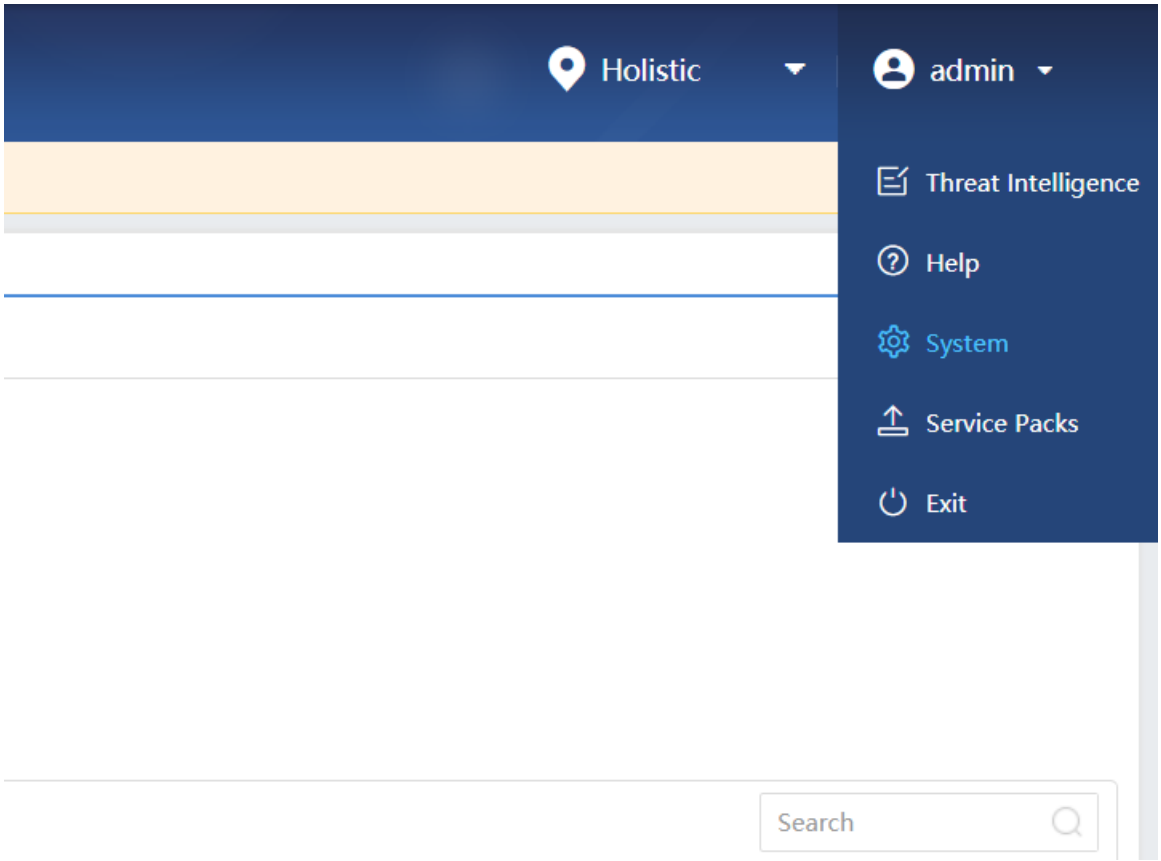


3. Go to Access Mgt->Web Authentication->Single Sign On->Sangfor Appliance, then fill in the IP of Cyber Command and set the destination port as 1775, 1775 port is general port for authentication between two sangfor devices.

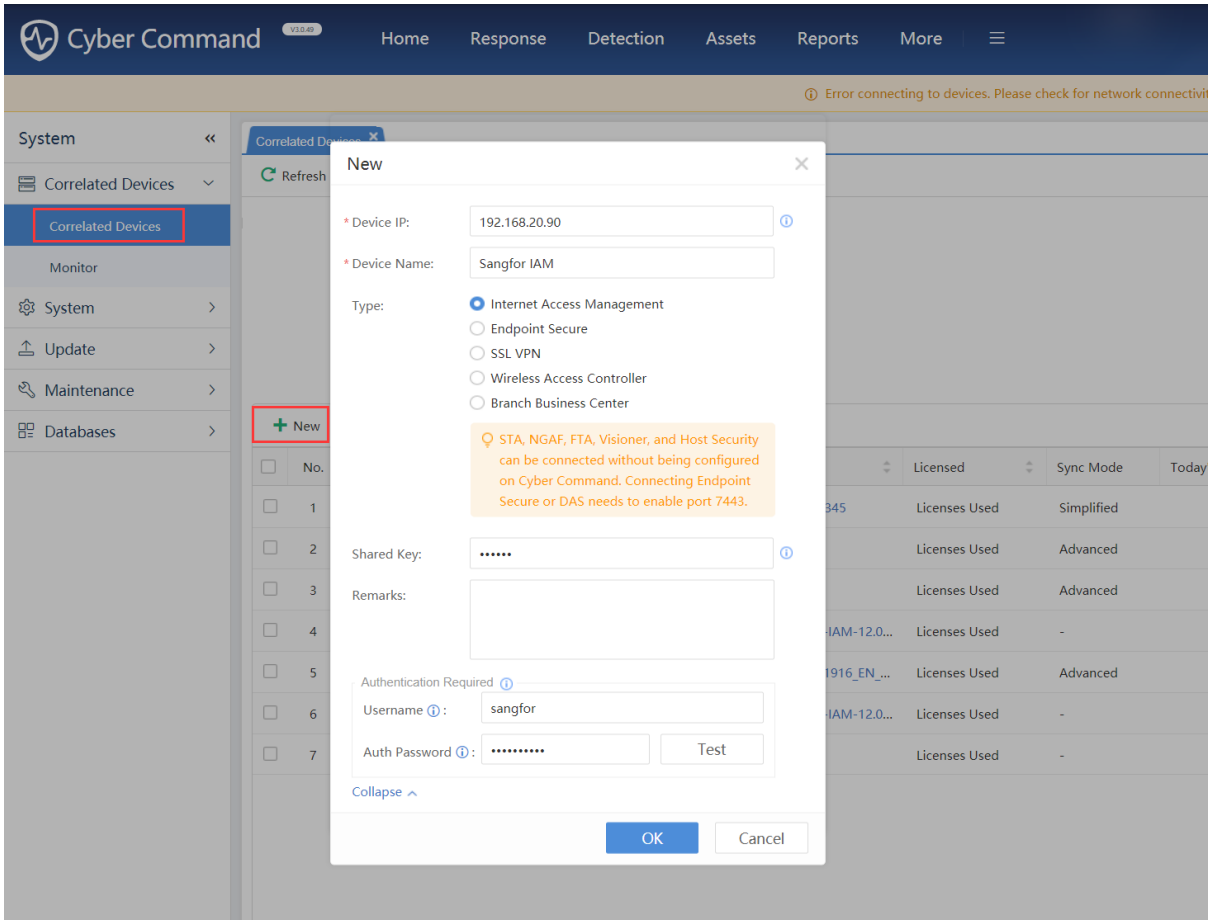


3.2.2 Configure Cyber Command

1. Go to System->Correlated Devices-> Correlated Devices.



2. Click New to create correlation, you must input the correct the username and password that you configured in IAG, and if you need to synchronize online users of IAG to Cyber Command, you must input the Shared Key same as you configured in IAG SSO Options.



3. If you are not sure whether the username and password were correct, you can click Test to check the account validity.

4. After Correlation configured successfully, you can see the assets already synchronized Cyber Command.

5. If you want to check the online user information of IAG in Cyber Command, just configure password based authentication policy in IAG same as Chapter 3.1.2.