Cyber Command

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

Version 3.0.49

Change Log

Date	Change Description
Mar 3, 2021	Document release.
May 17, 2021	Document update.

CONTENT

Chapter 1 Scenario

1.1 Scenario

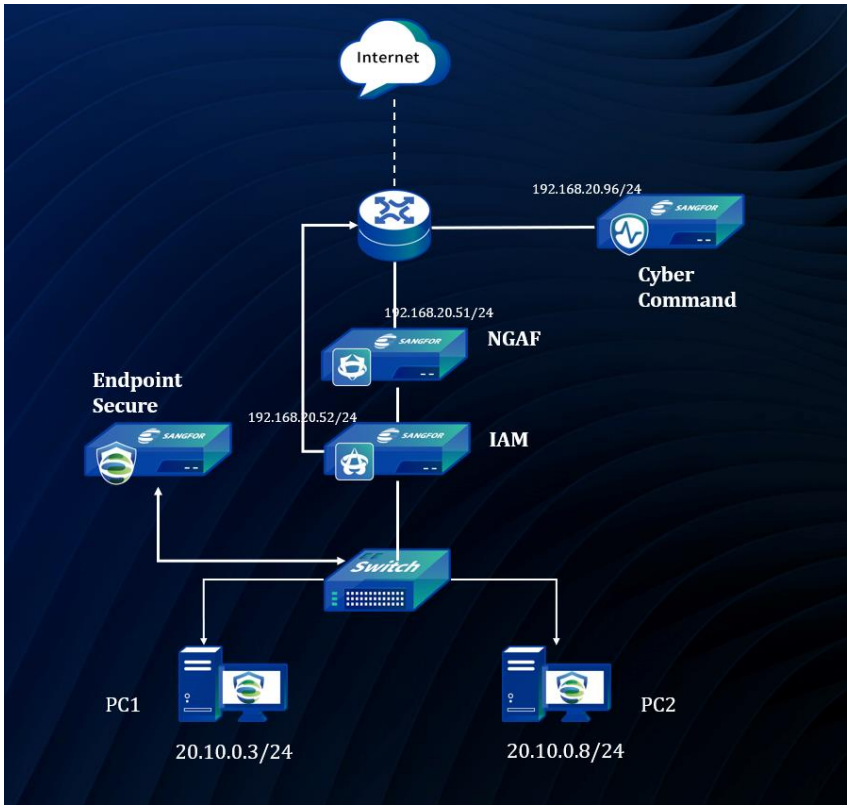
Cyber Command collects data from security detection probes of each intranet node, presents users with intranet business assets and attacks and potential threats against intranet key business assets in a visual form, and uses the platform to attack all security systems on the existing network Carry out unified management and policy issuance.

IAM supports the visual control of endpoints, applications, data, and traffic across the entire network, and intelligently senses internal risks such as endpoints' access violations, Internet violations, and sensitive data leakage, and realizes the integration of endpoints' access control, Internet access control, and data leakage control. Behavioral safety control.

In the Cyber Command and IAM Correlation, IAM synchronizes online users information to Cyber Command for unified summary and analysis, helping to quickly locate users with security risks, so as to realize accurate reminders and account blocking, and strengthen the control of online security.

1.2 Environment

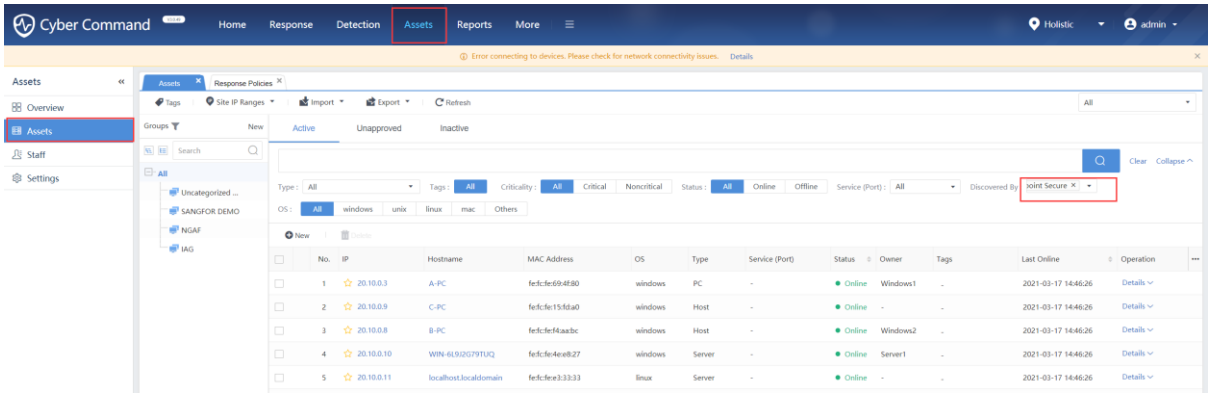
1.2.1 Network Environment



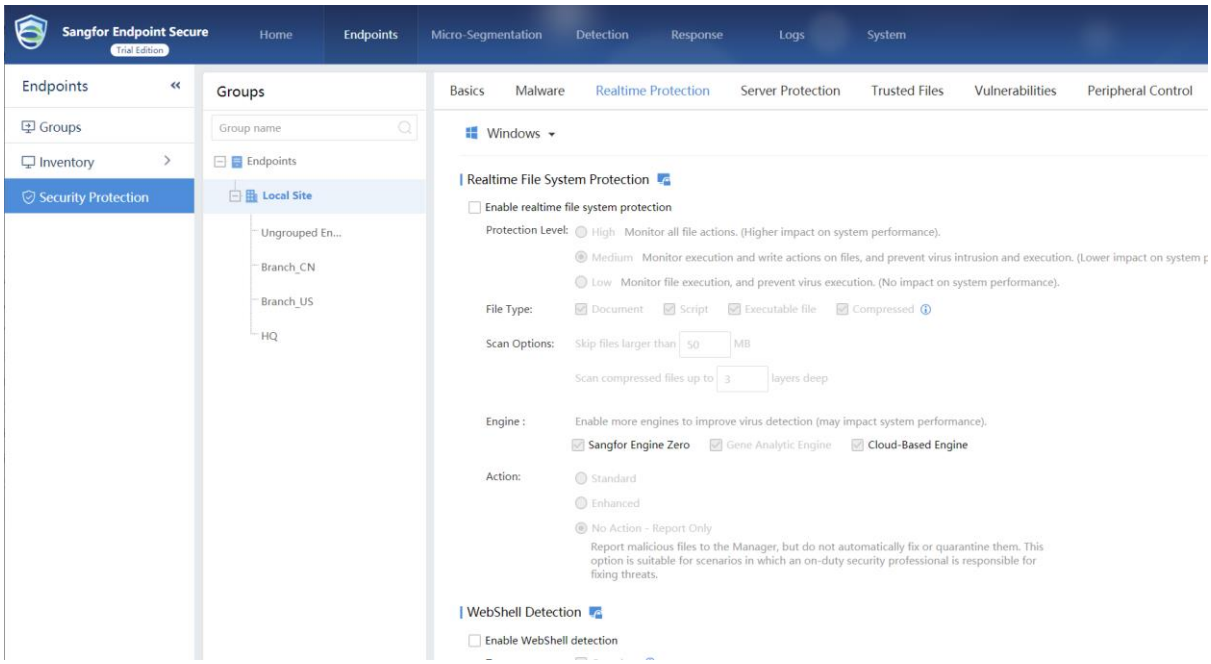
1.3 Precautions

1. IAM not support Synchronize security logs to Cyber Command and not support anti virus in endpoint, Cyber Command only support issue the lockout or reminder policy to IAM, so you need install the Endpoint Secure to let IAM to correlate to scan virus and synchronize the security logs to Cyber Command, then you can configure response policy in Cyber Command.

2. Please ensure that Endpoint Secure synchronized all assets to Cyber Command.



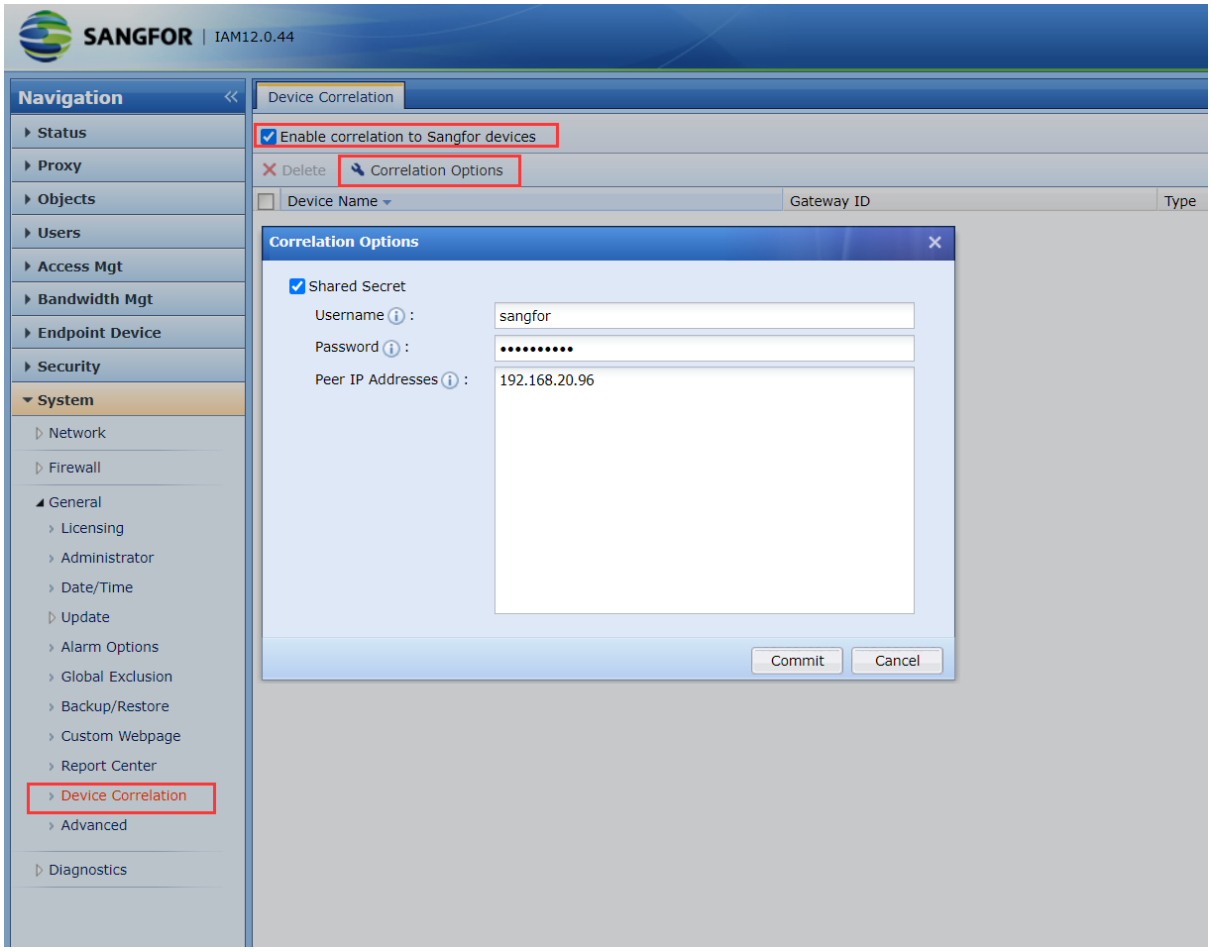
3. Disable the Realtime File System Protection and other Protection, for we should avoid Endpoint Secure kill virus directly, after disabled Realtime Protection of Endpoint Secure, then IAM can detect the traffic of Botnet. **The virus samples we use are only for internal testing of the correlation effect, and real-time detection needs to be enabled on when the correlation effect is tested or when the implement is completed.**



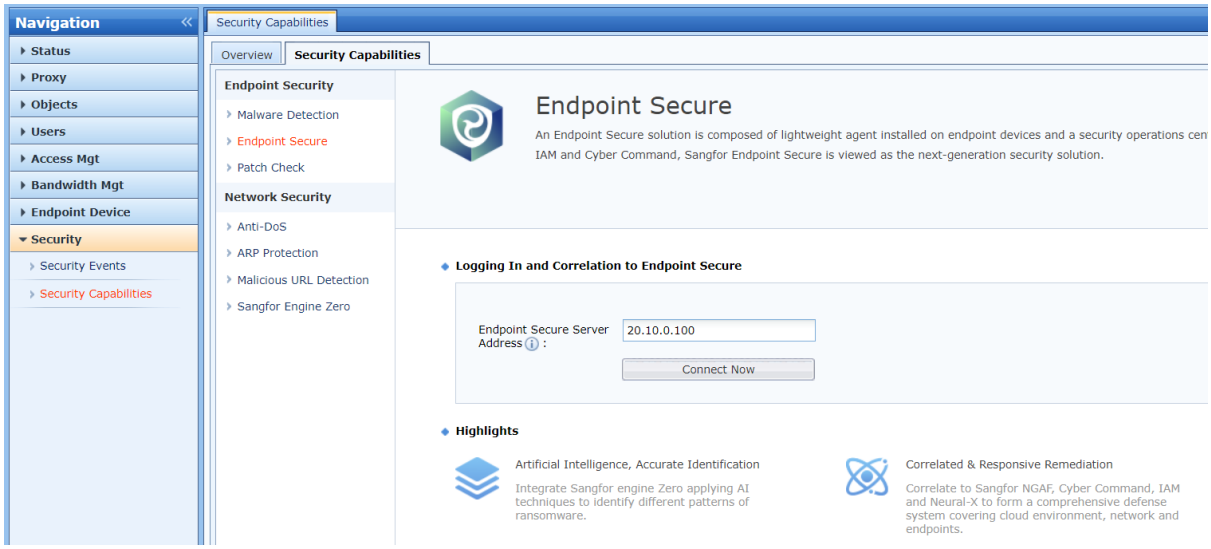
Chapter 2 Configure

2.1 Configure IAM

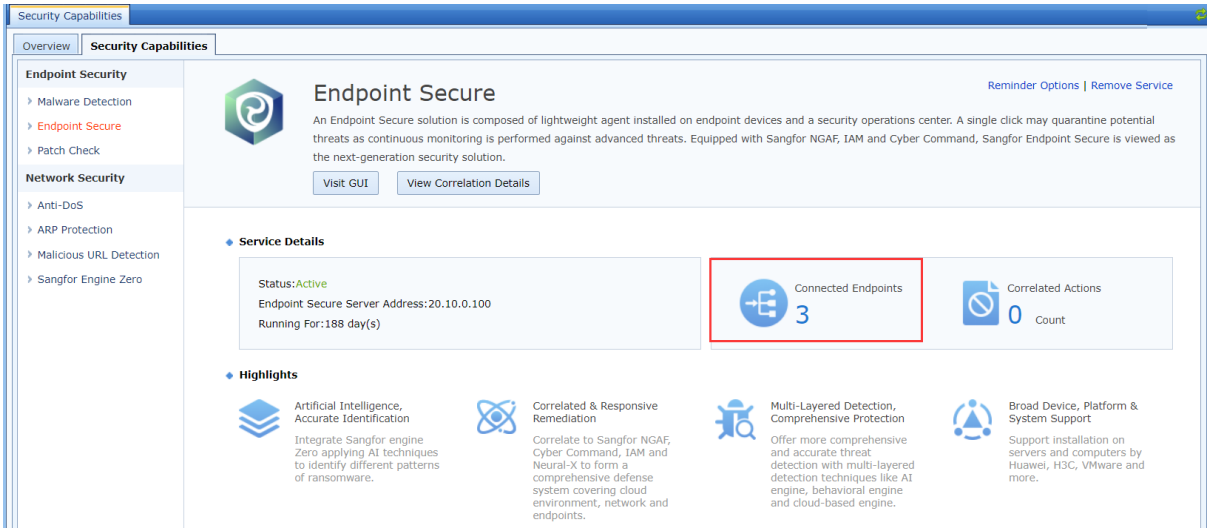
1.Go to System-> General->Device Correlation.



2. Go to Security-> Security Capabilities path. Input the IP address of Endpoint Secure.



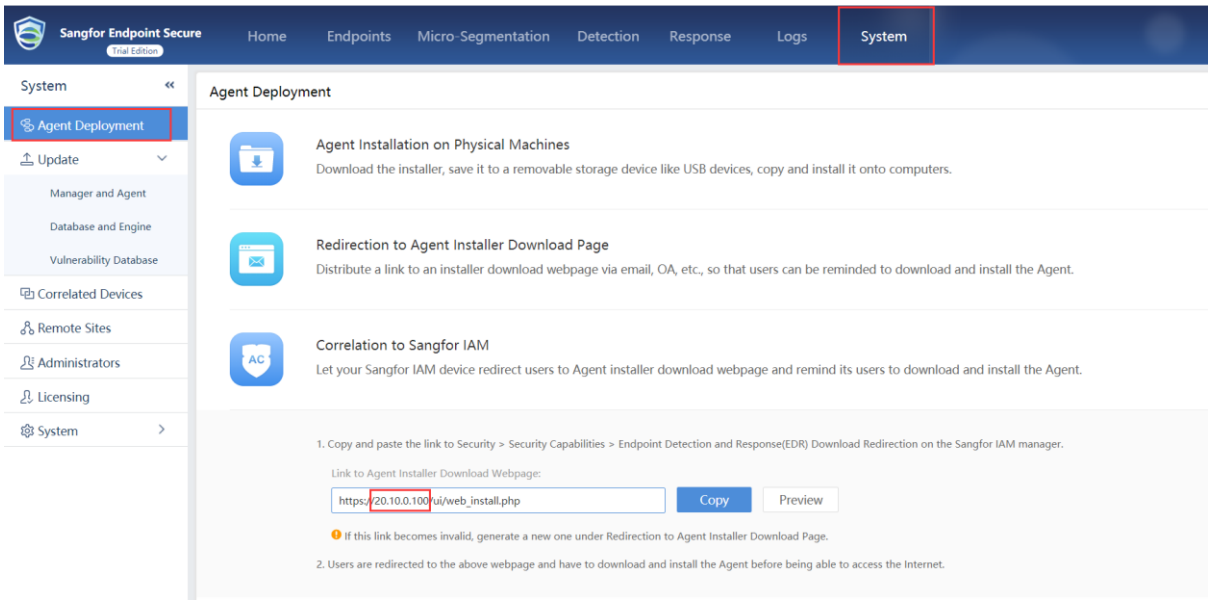
3. After IAM connected to Endpoint Secure, you can see the endpoint counts that how many endpoints already connected to MGR



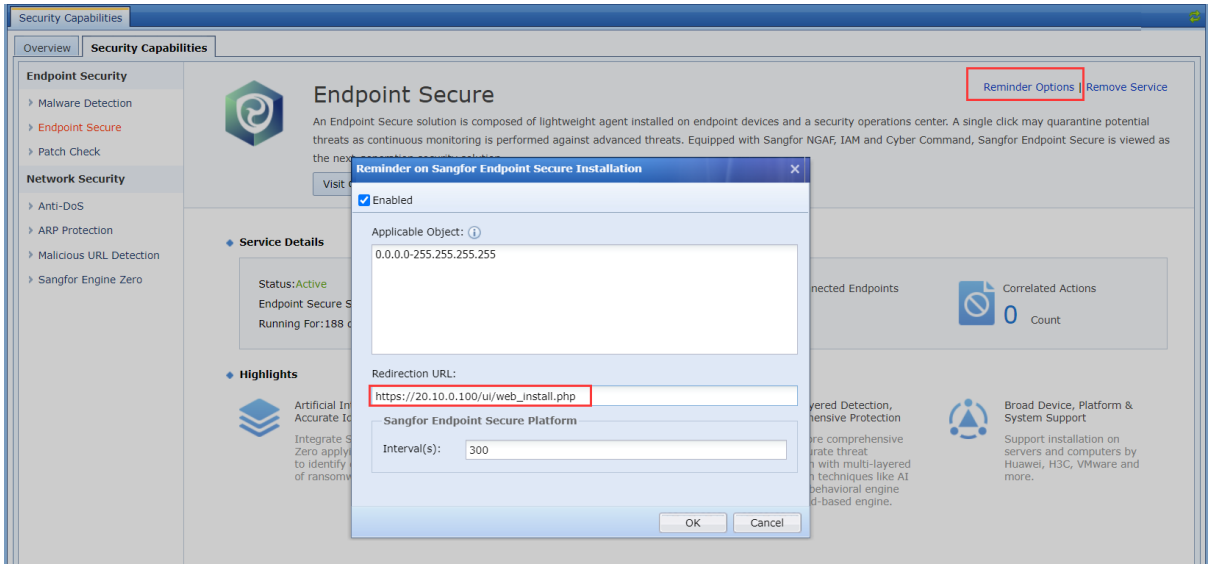
4.In order to IAM could redirect reminder page to risk endpoint, you must configure reminder policy in IAM.

First, configure risk reminder page address in Endpoint Secure, you can you System-> Agent Deployment-> Correlation to Sangfor IAM page and configure ES agent download address so that IAM can direct PC to ES agent download page.

Note: You must ensure that the internal endpoints are able to access the ES agent download address.

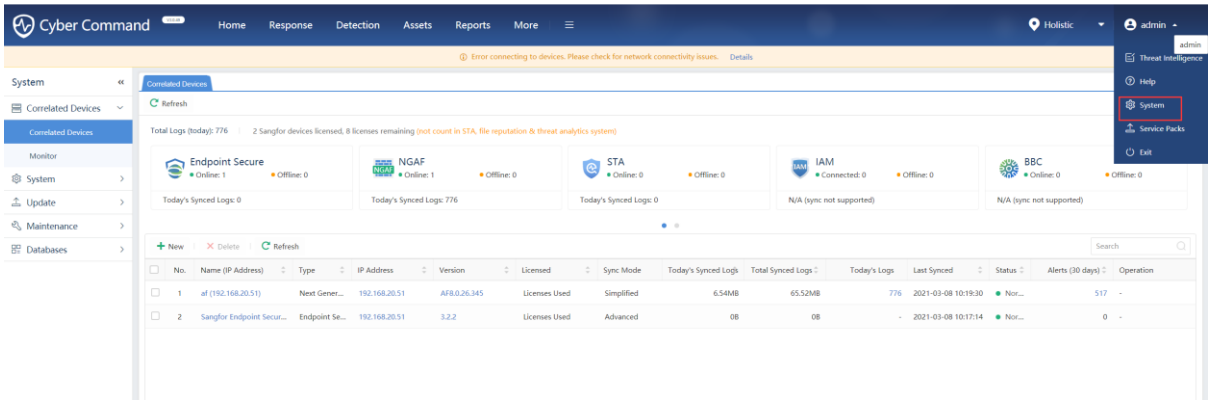


Second, configure reminder policy in IAM, please ensure the redirection URL is same as you configured in ES.

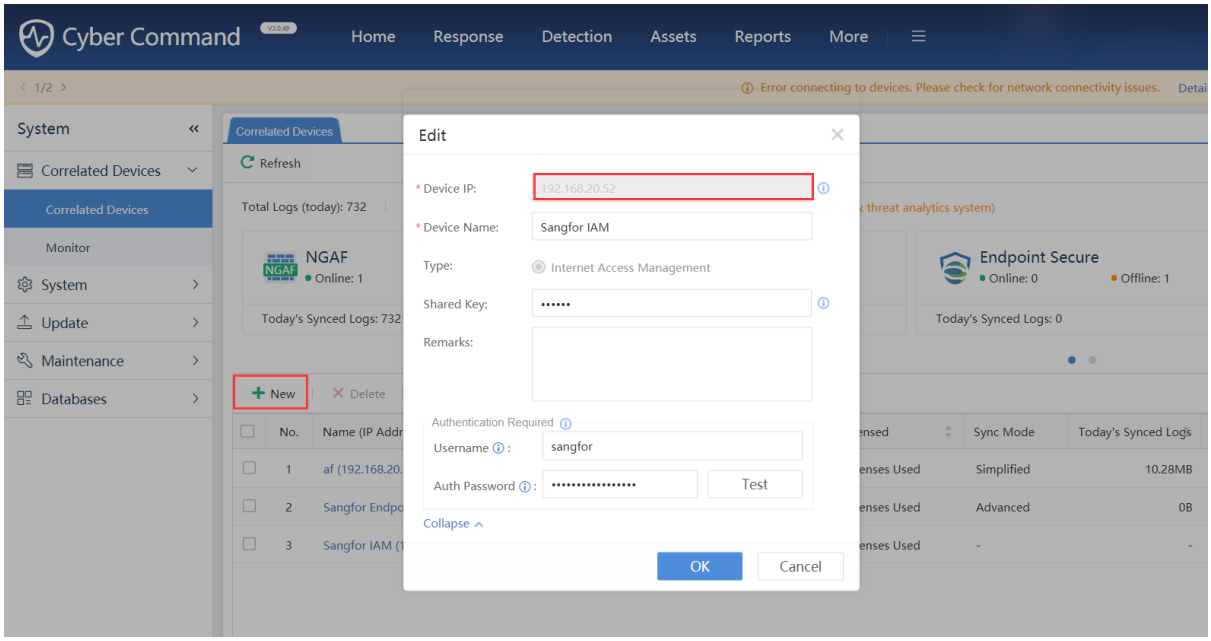


2.2 Configure Cyber Command

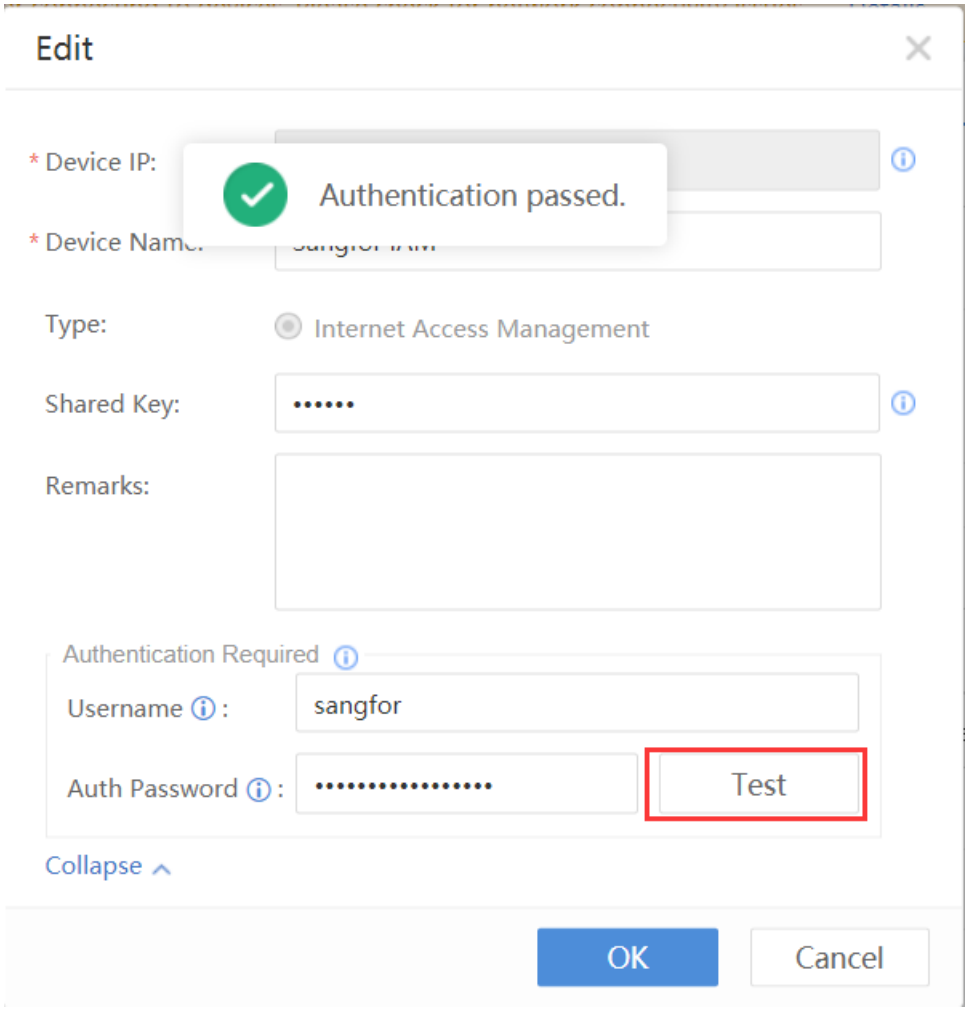
1. Go to System->Correlated Devices-> Correlated Devices.



2.Click New to create correlation, you must input the correct the username and password that you configured in IAM.

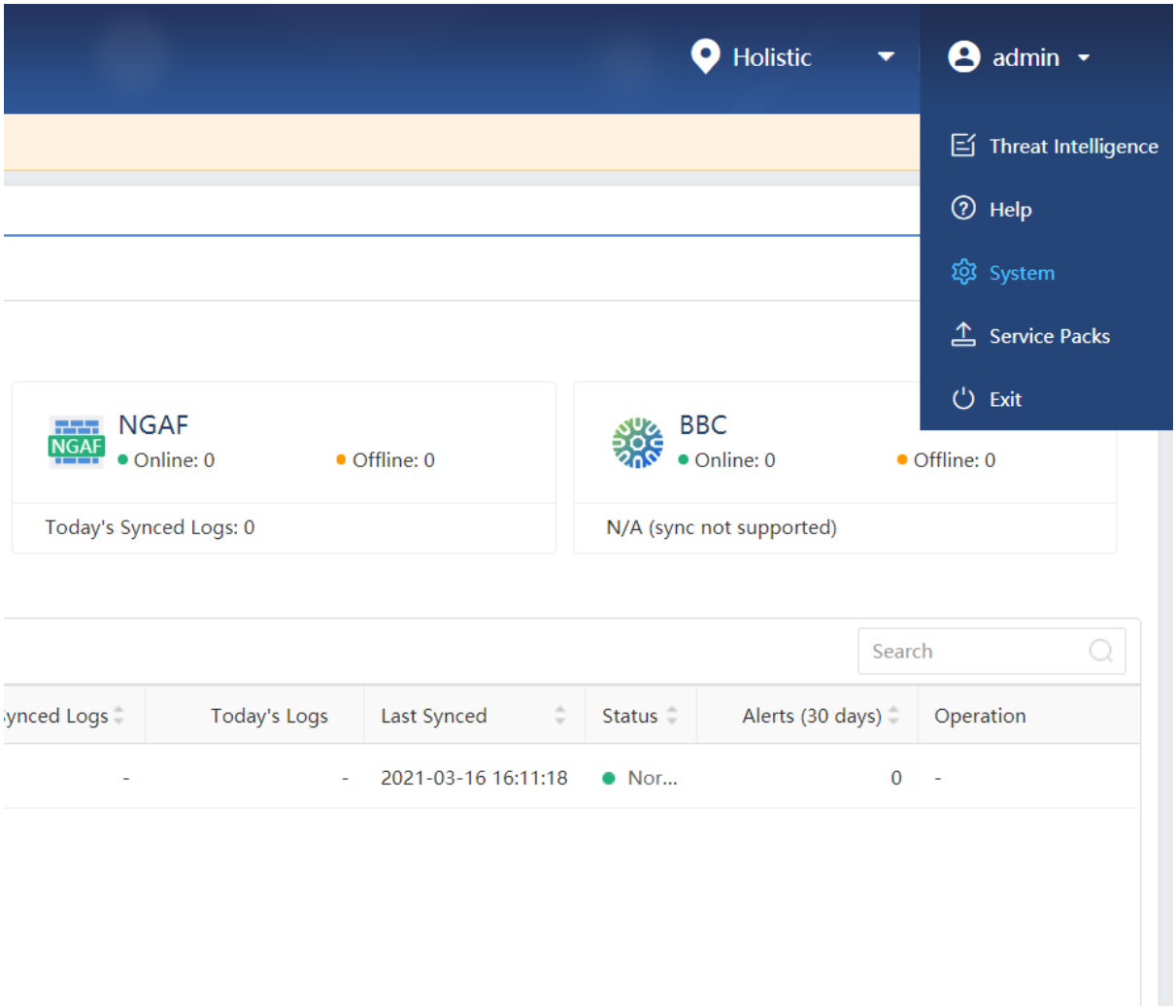


3. If you are not sure whether the username and password were corretc, you can click Test to check the account validity.

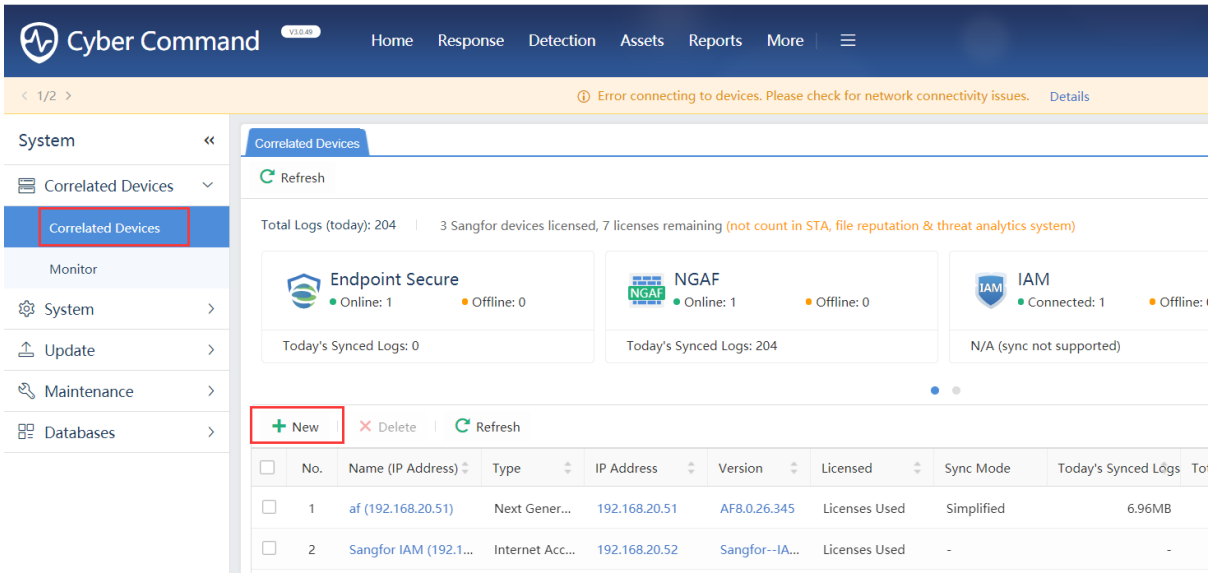


2.3 Configure Endpoint Secure

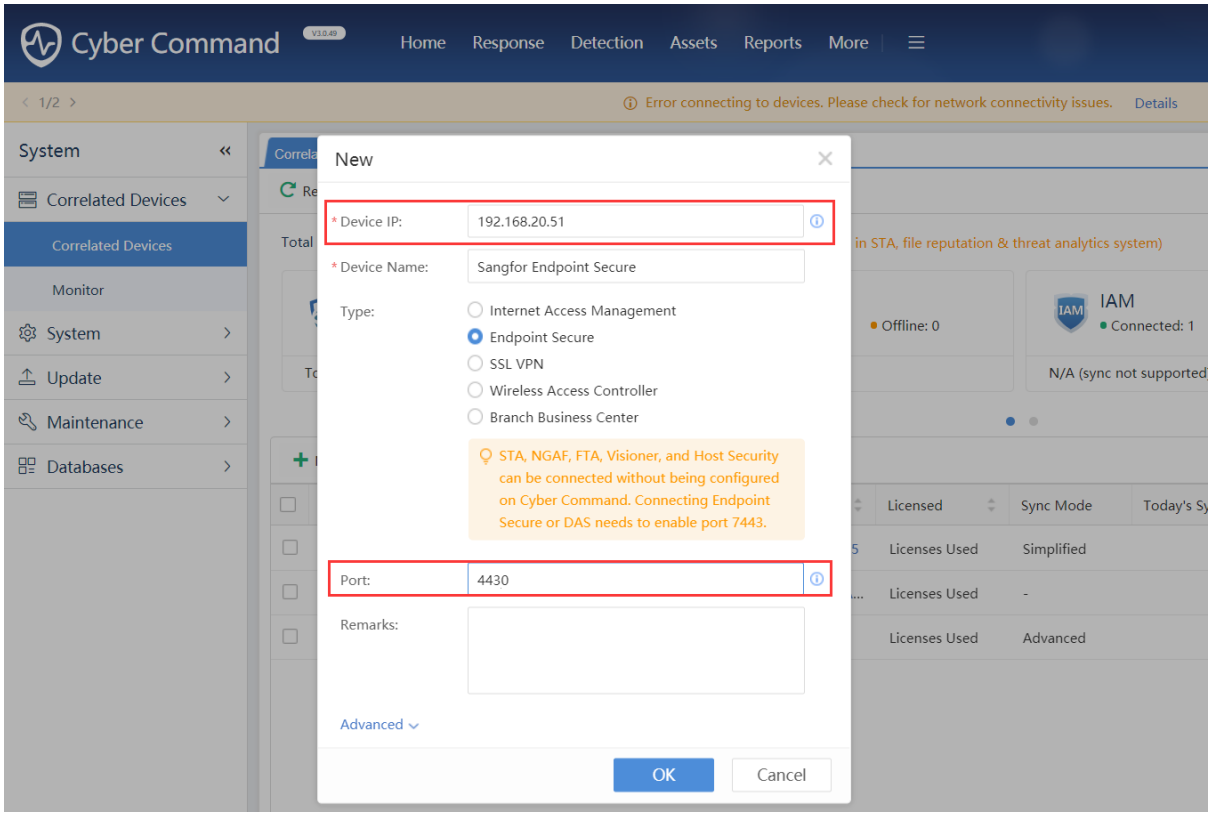
1. Go to System Path.



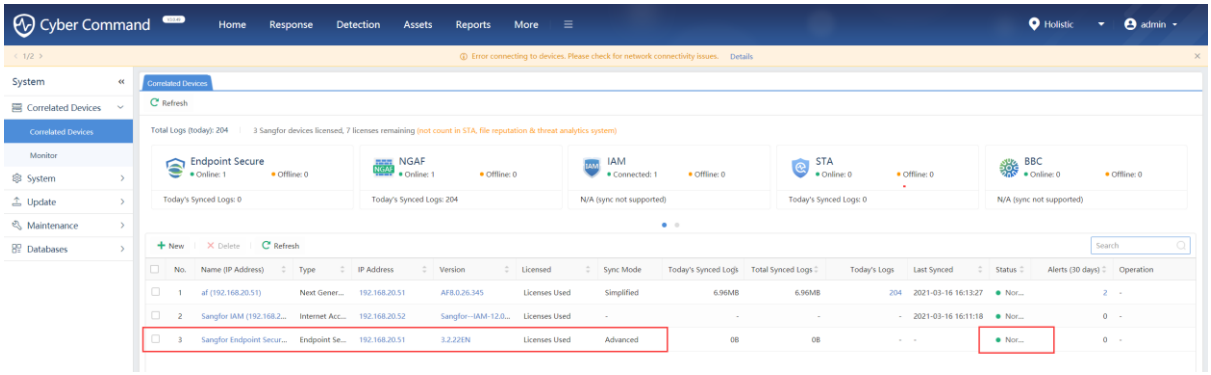
2. Go to Correlated Devices-> Correlated Devices path, and click New to create Correlation.



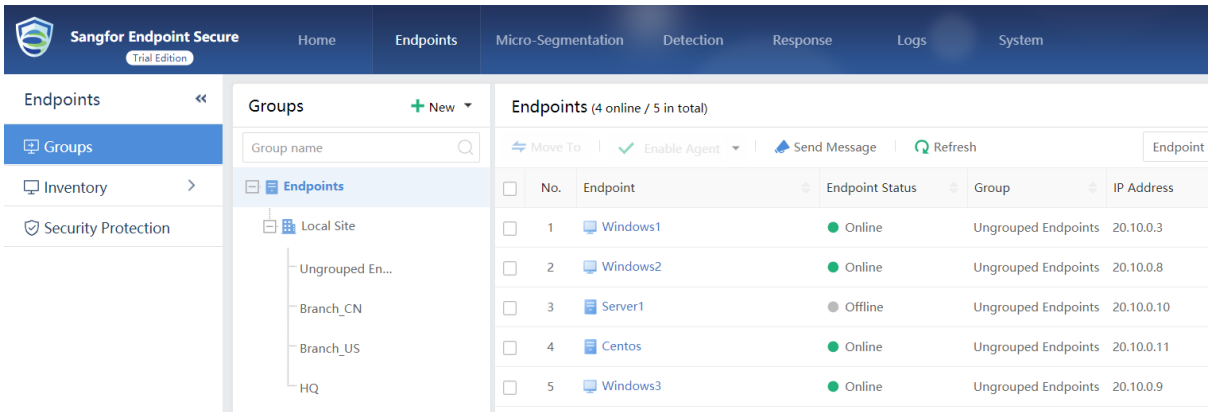
3. Input the IP of Endpoint Secure and the Port, if Endpoint Secure deployed after a NAT device, Please map the 443 port of Endpoint Secure to the NAT device. For example, here is the 4430 port mapped to the NAT device.



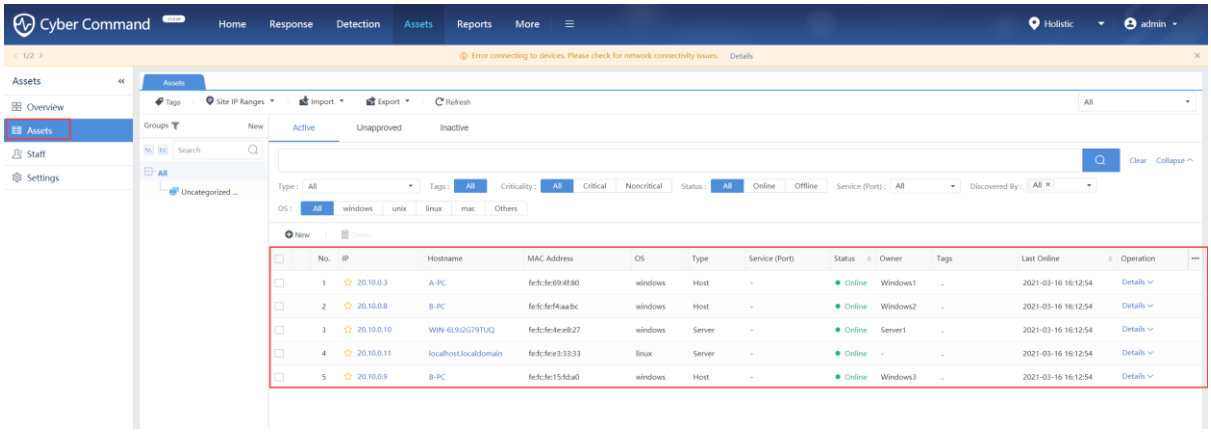
4. After click OK, you can see the correlation status in console.



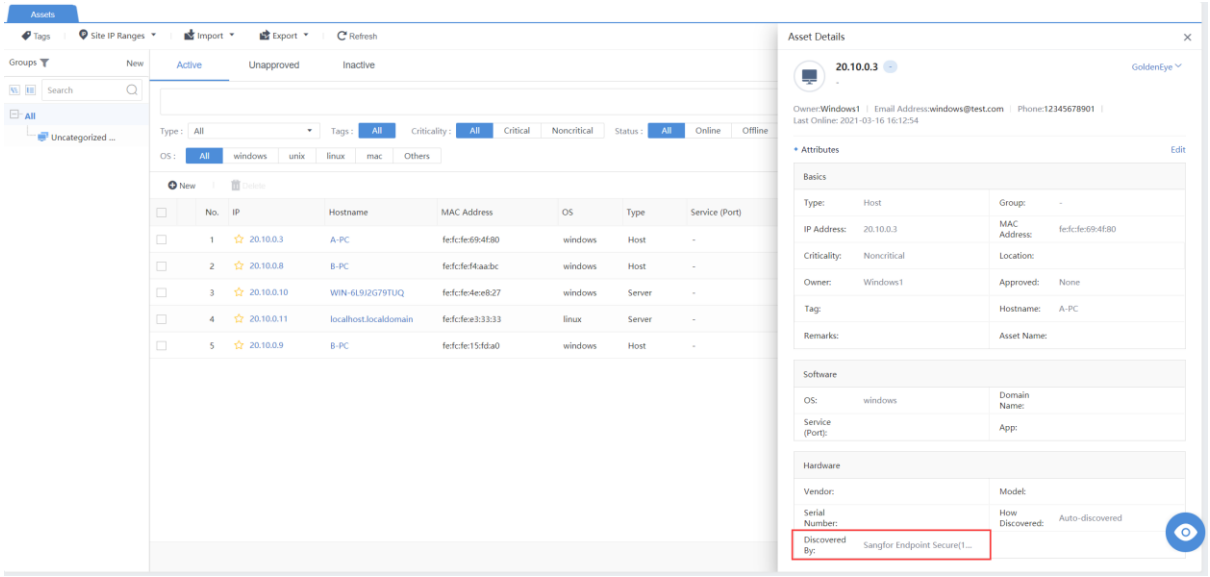
5. You can check whether there exists assets in Endpoint Secure.



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.



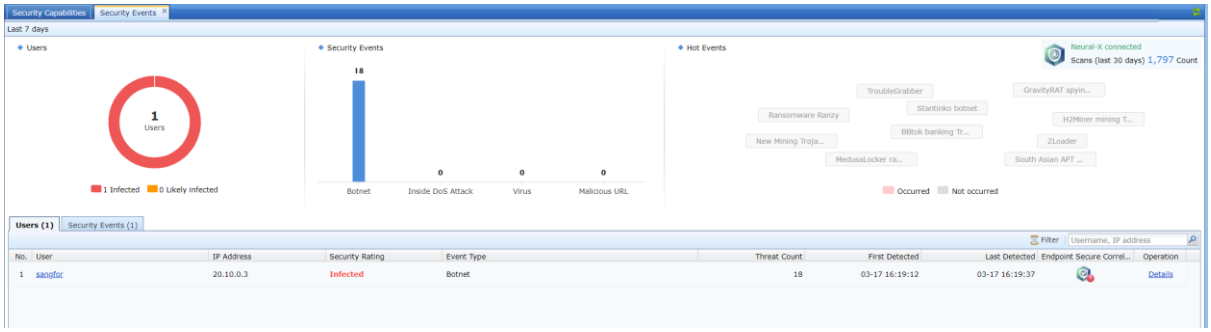
7. You can view the details to see the assets source, such as following detail, you can see this asset discovered by Endpoint Secure.



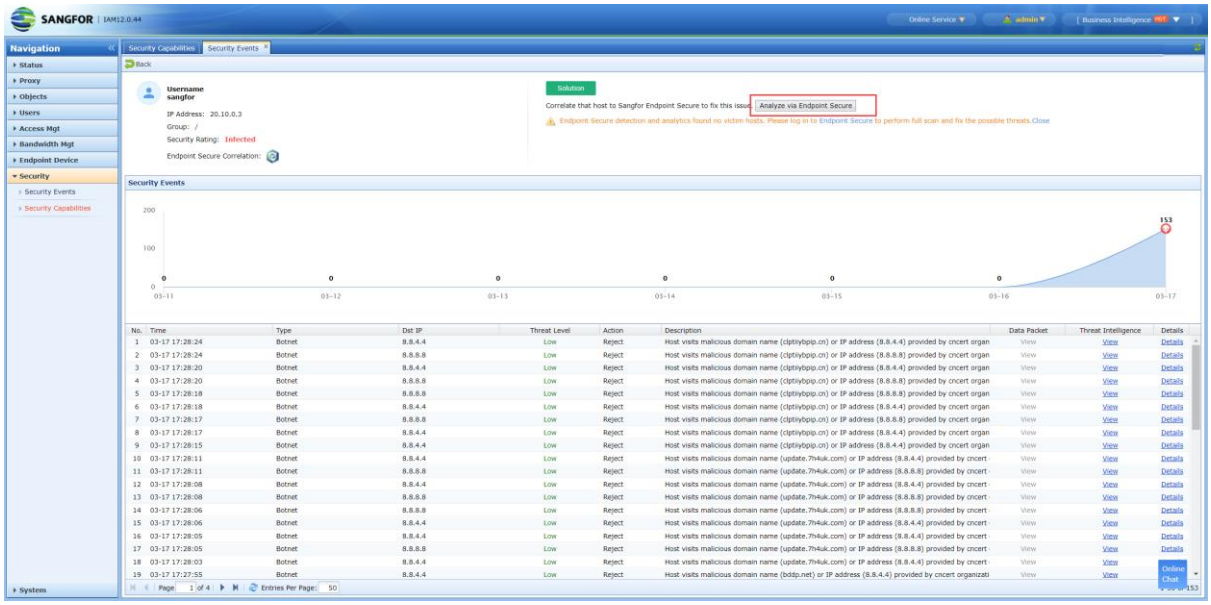
Chapter 3 Correlation

3.1 Synchronize Logs to Cyber Command

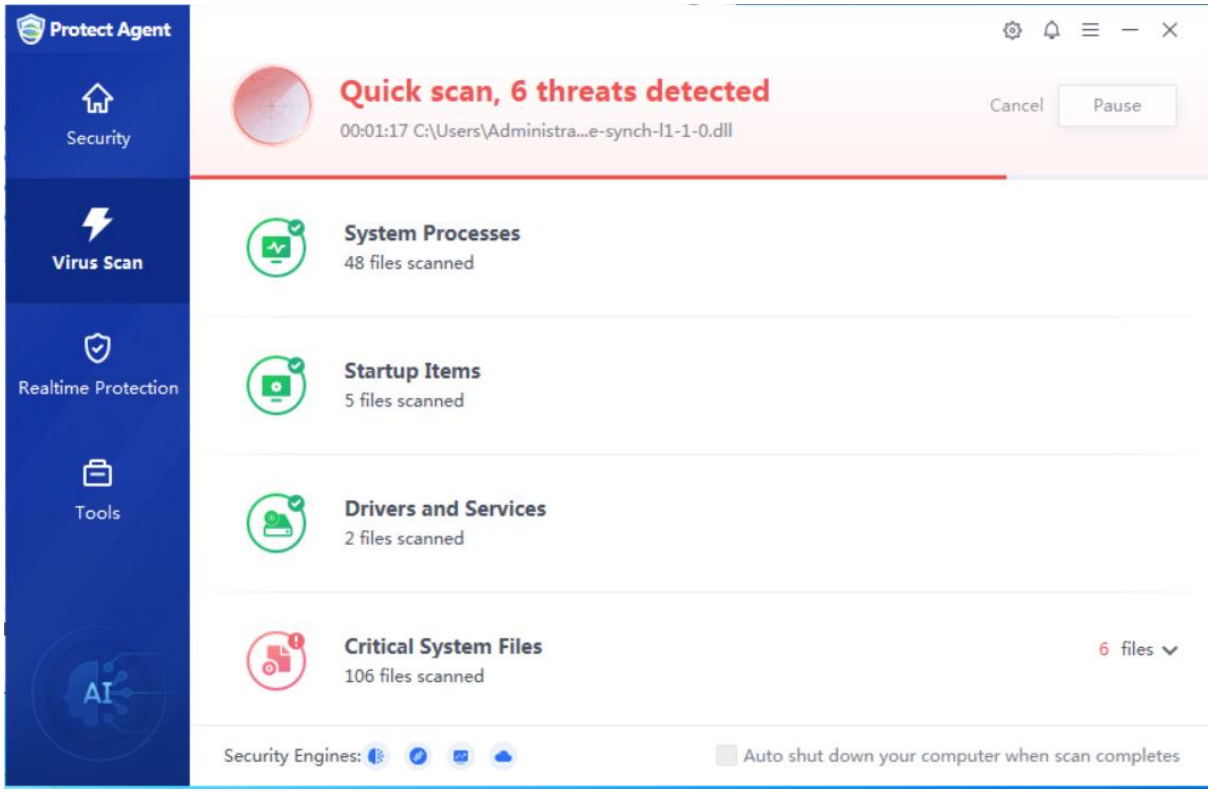
1. When IAM detected the Botnet traffic, you can see the logs in web console.

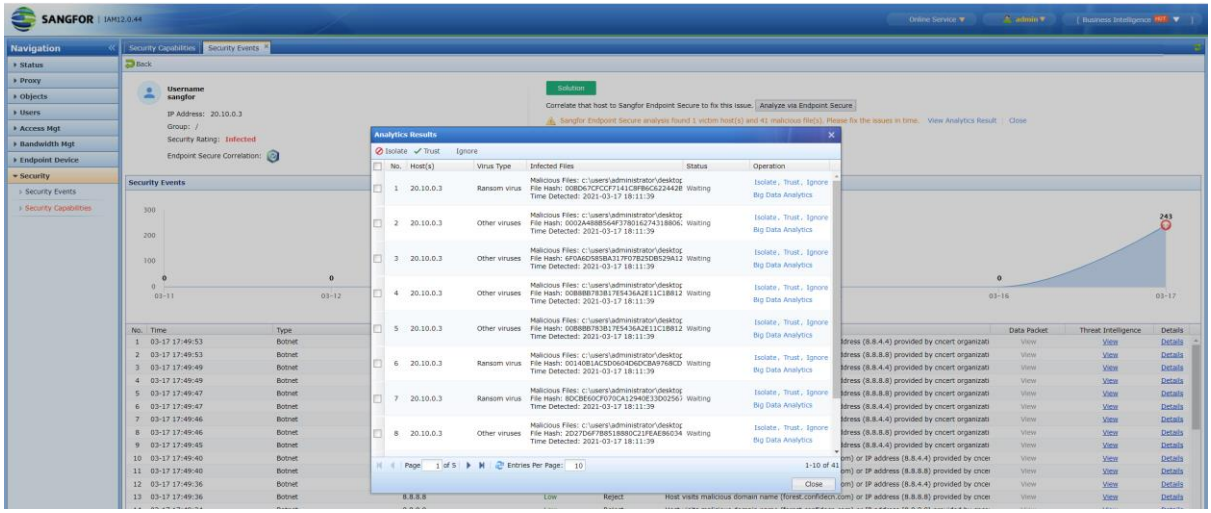


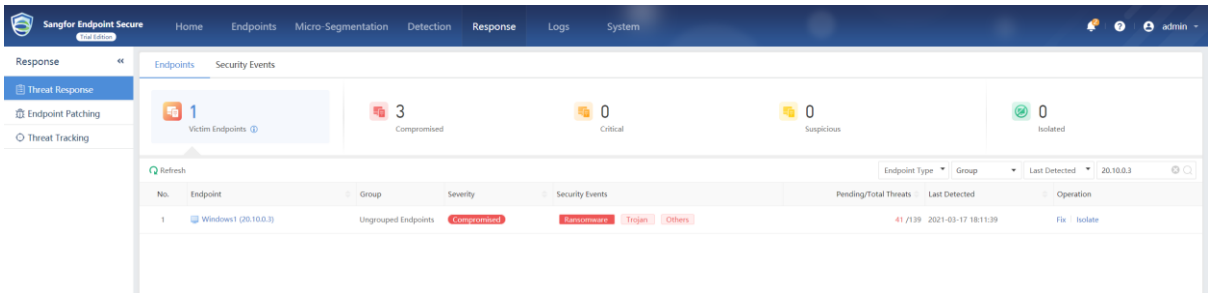
2. Click Analyze via Endpoint Secure to issue scan task.

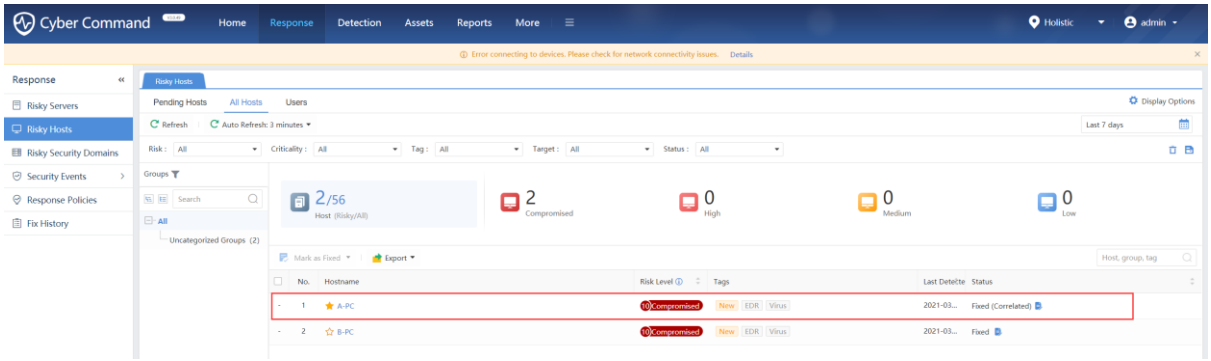


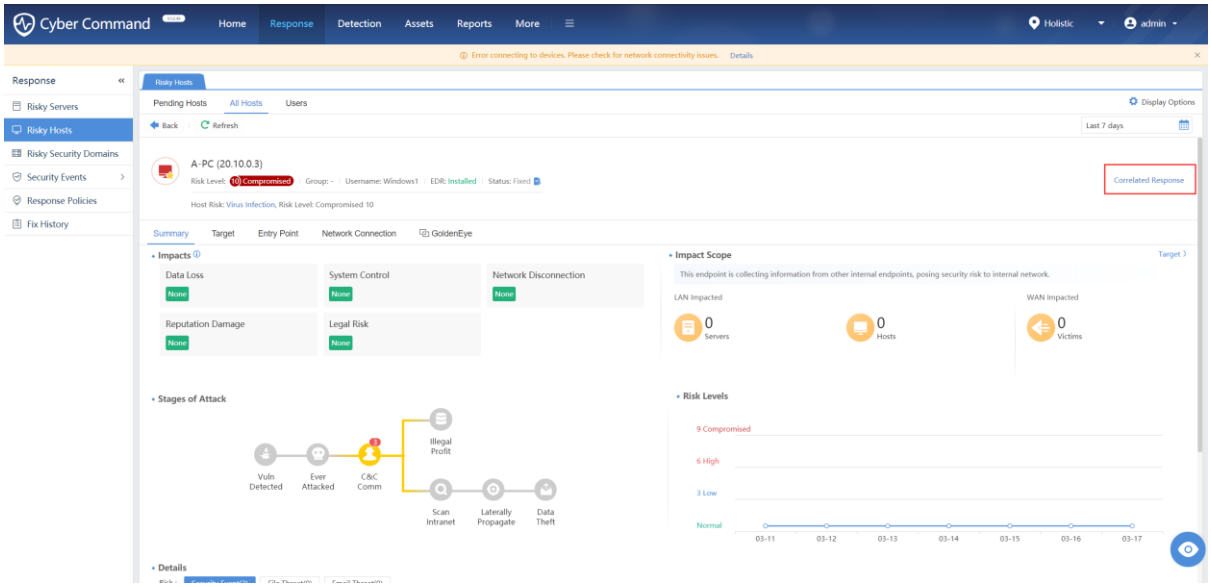
Then, you can see the scan task running in endpoint.




SANGFOR
Navigation
Security Events
Analytics Results


Sangfor Endpoint Secure
Home
Endpoints
Micro-Segmentation
Detection
Response
Logs
System
admin
Response
Threat Response
Endpoint Patching
Threat Tracking
Endpoints
Security Events
1
Victim Endpoints
3
Compromised
0
Critical
0
Suspicious
0
Isolated

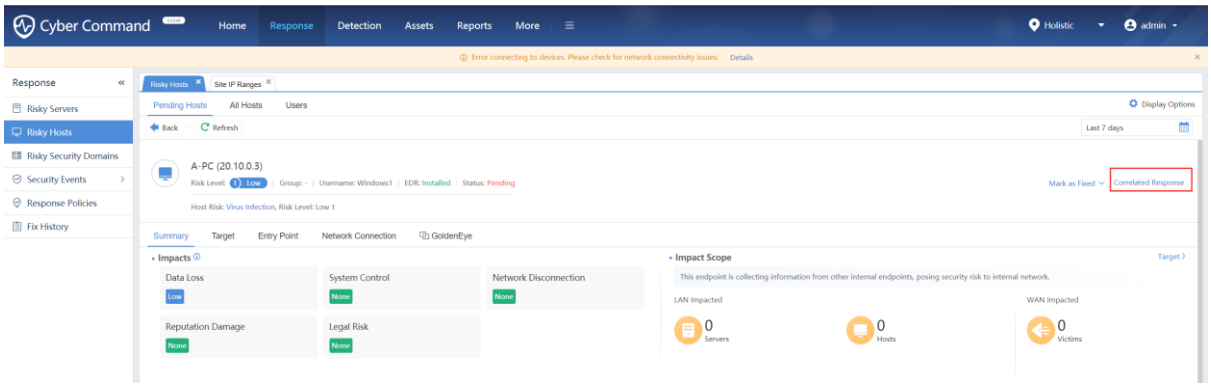

Cyber Command
Home
Response
Detection
Assets
Reports
More
Holistic
admin
Response
Risky Servers
Risky Hosts
Risky Security Domains
Security Events
Response Policies
Fix History
Pending Hosts
All Hosts
Users
2/56
Host (Risky/All)
2
Compromised
0
High
0
Medium
0
Low
A-PC
B-PC


Cyber Command
Home
Response
Detection
Assets
Reports
More
Holistic
admin
A-PC (20.10.0.3)
Correlated Response
Summary
Target
Entry Point
Network Connection
GoldenEye
Impacts
Data Loss
System Control
Network Disconnection
Reputation Damage
Legal Risk
Impact Scope
Stages of Attack
Risk Levels
Details

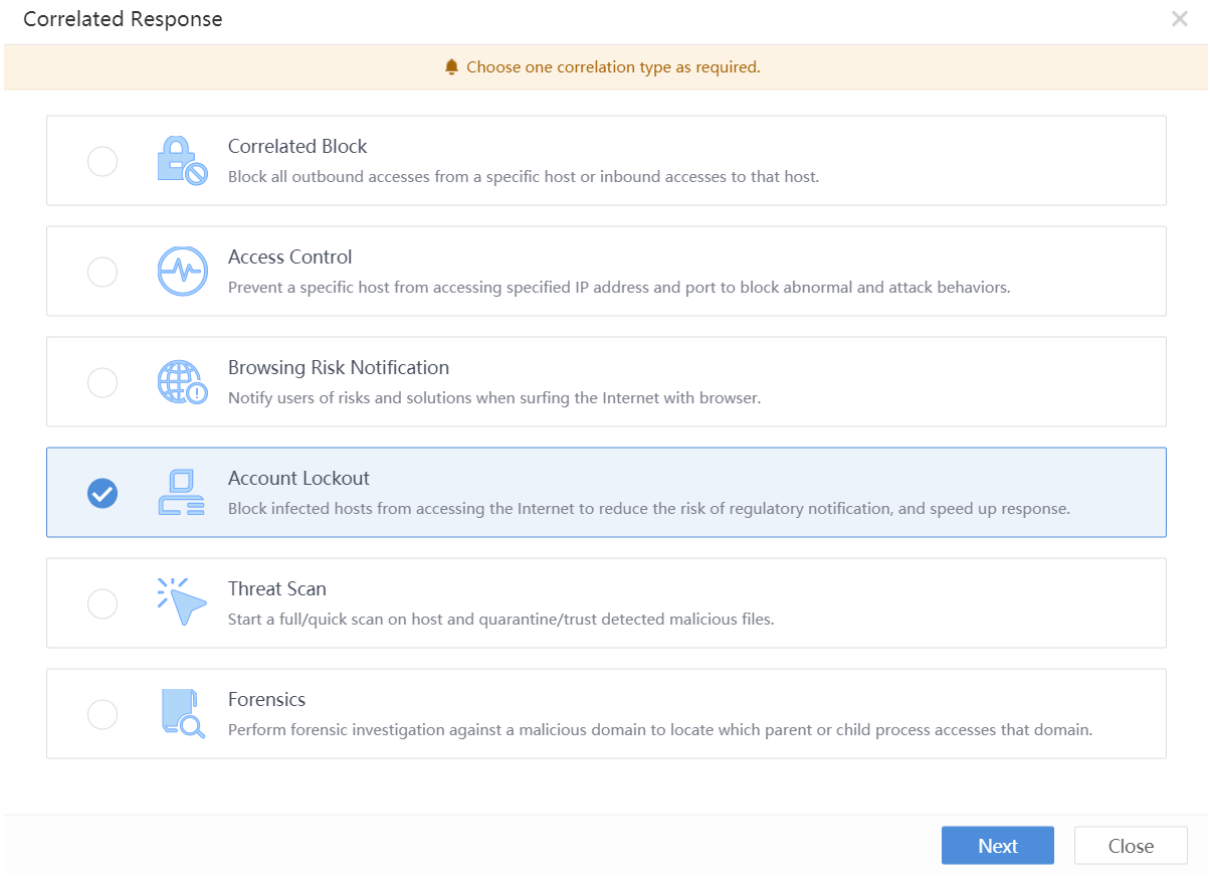
3.2 Response in Cyber Command

3.2.1 Lockout the Account

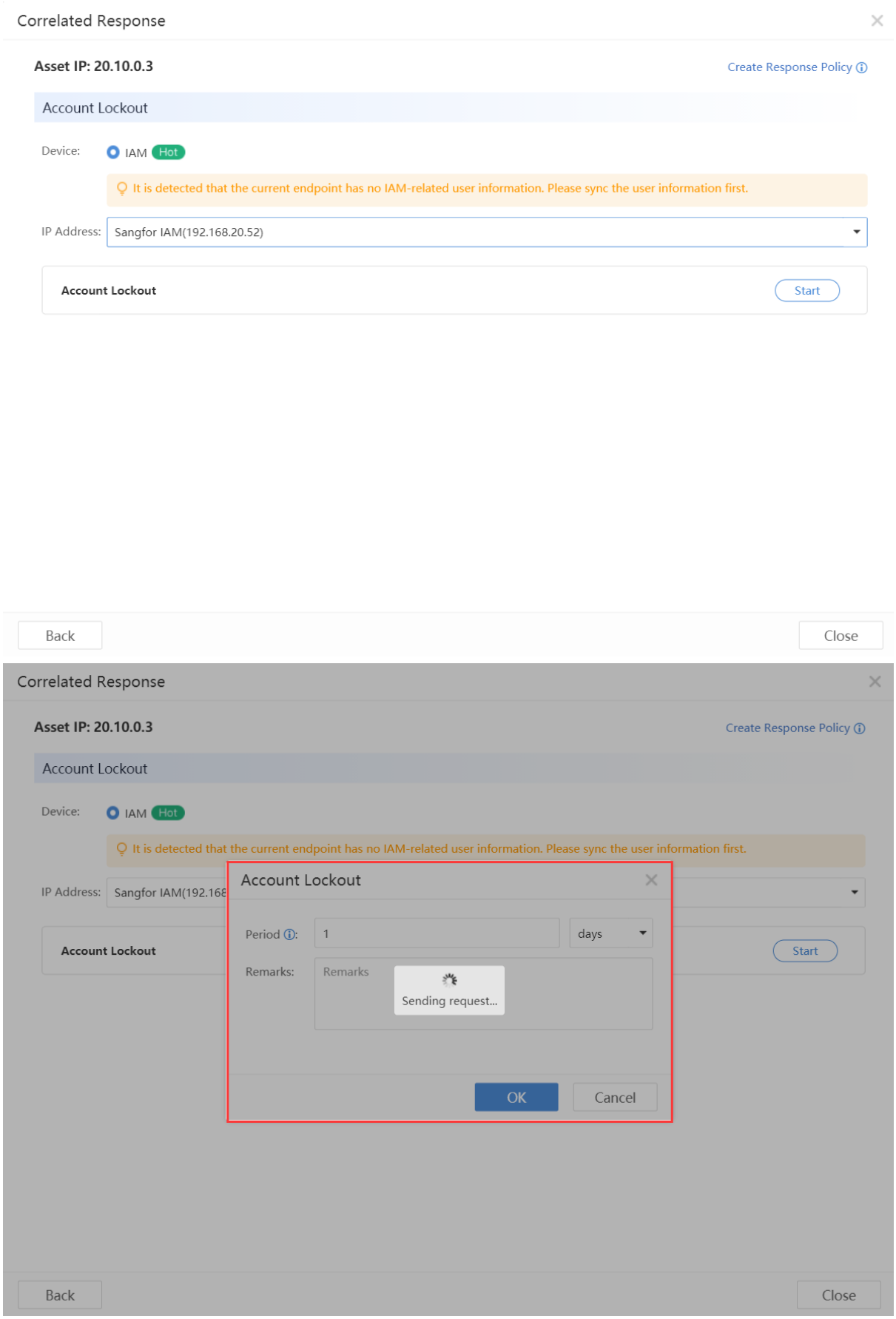
1. If you want to block the botnet host, you can click Correlated Response.



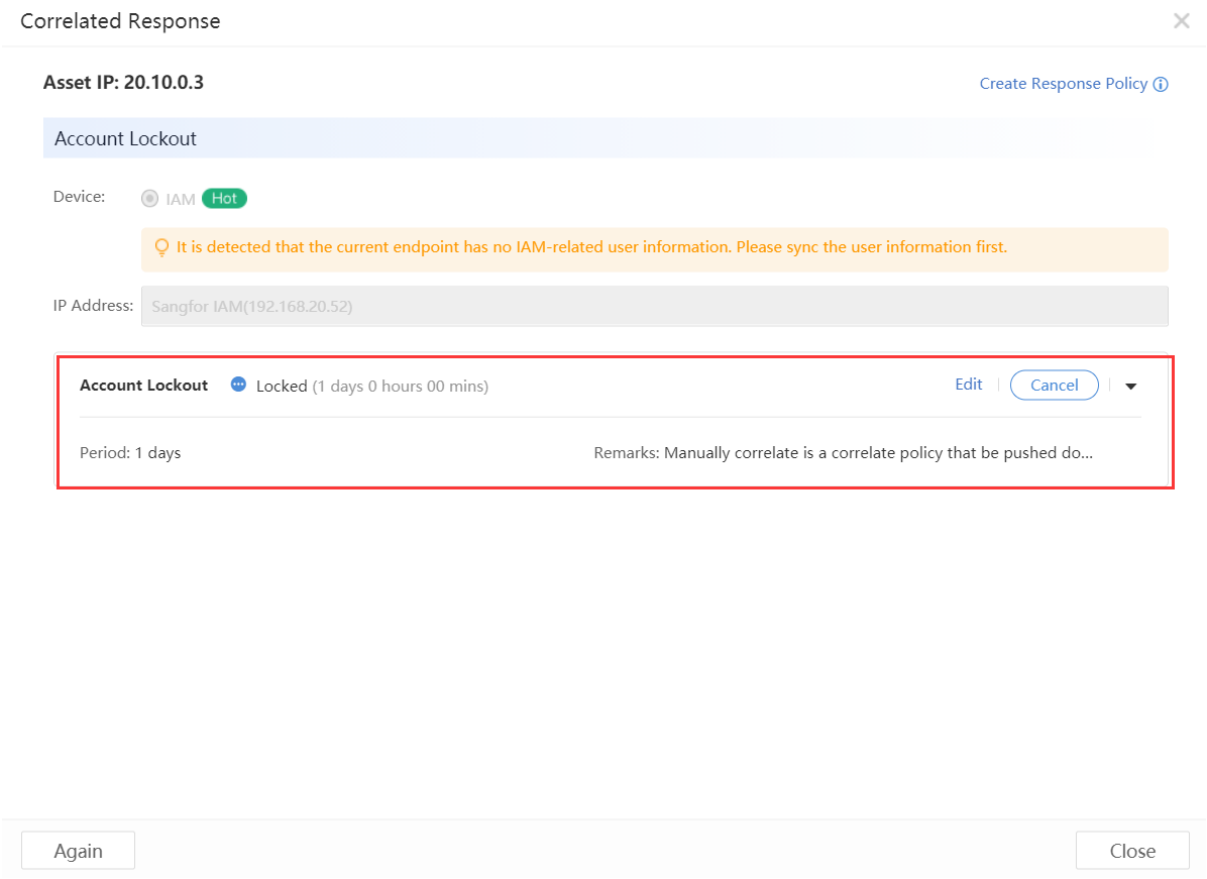
2. Select Account Lockout.



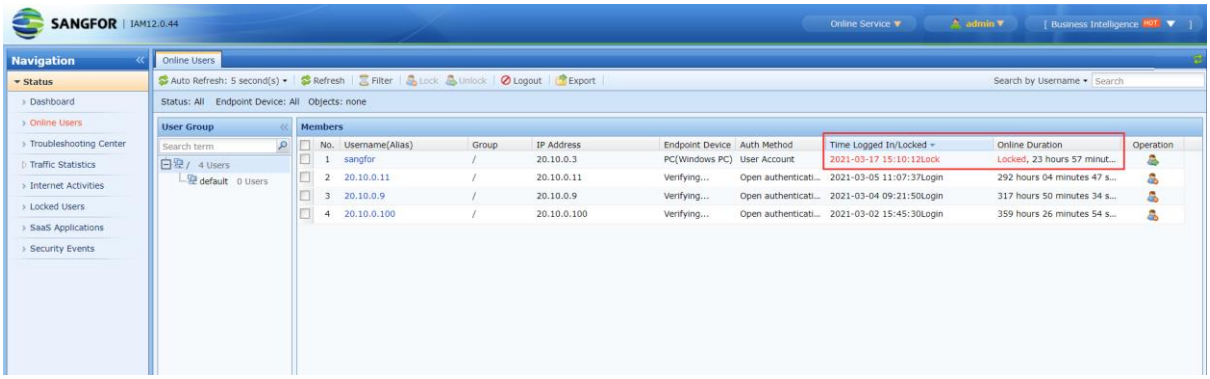
3. Select related IAM and click Start to set lockout time.



4. Wait for a while, you can see the Cyber Command shows that policy issued successfully.

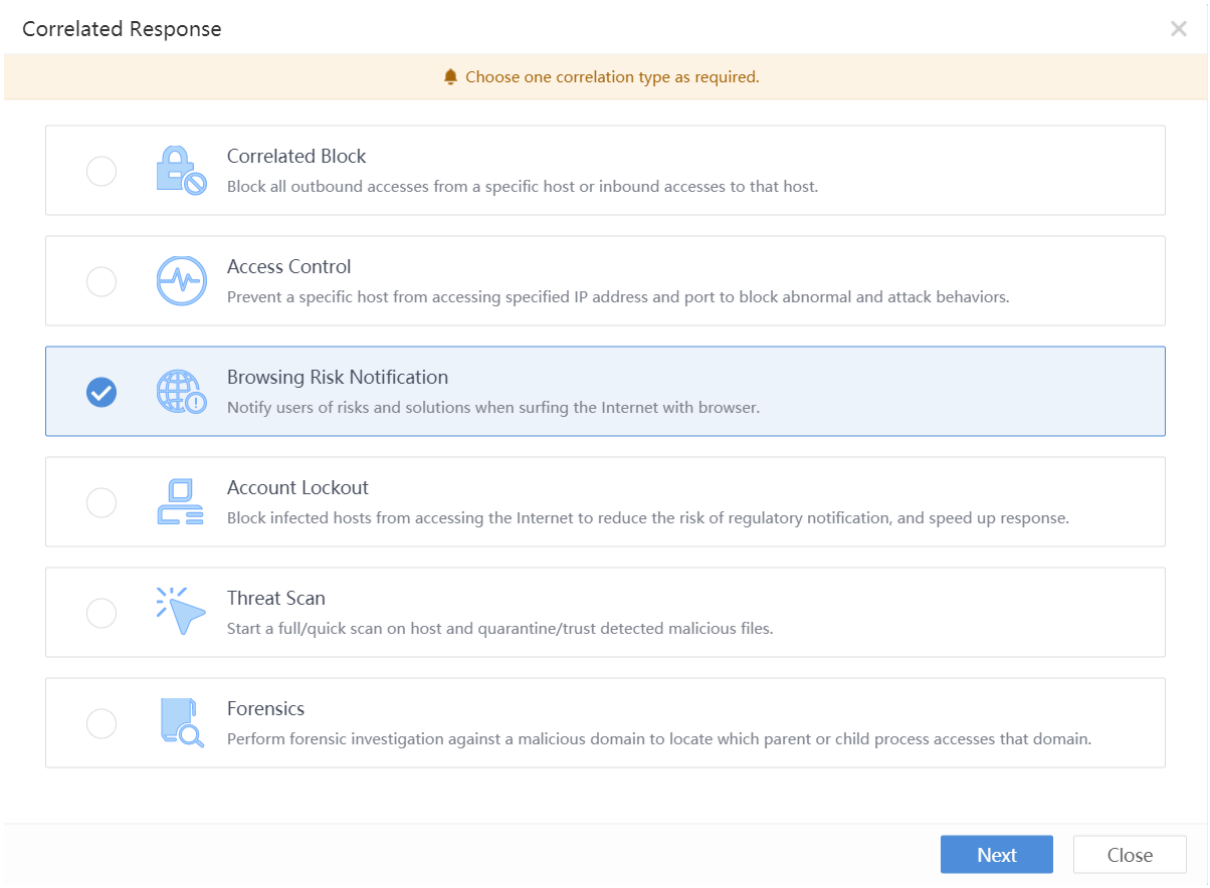


5. Log in IAM web console and go to Status-> Online Users path, you can see the user already locked by IAM.

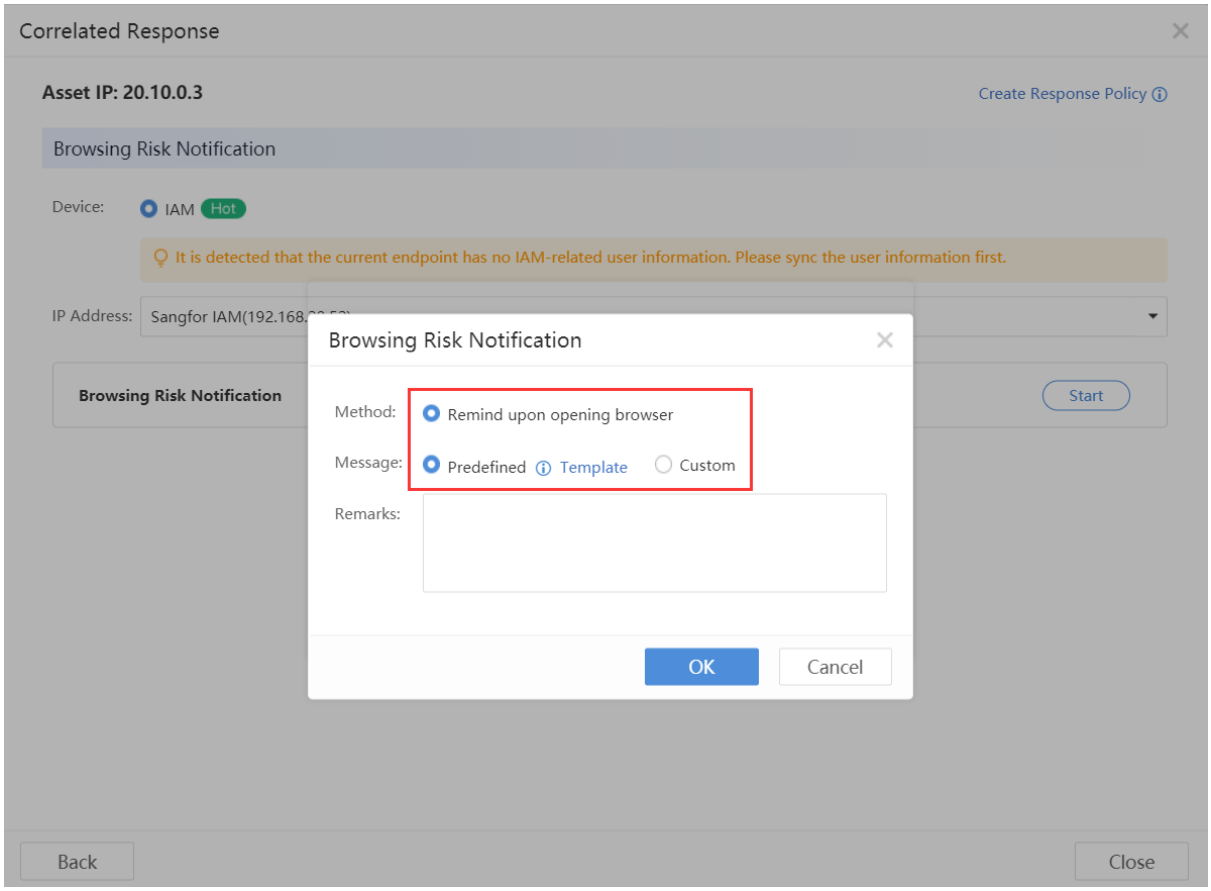


3.2.2 Browsing Risk Notification

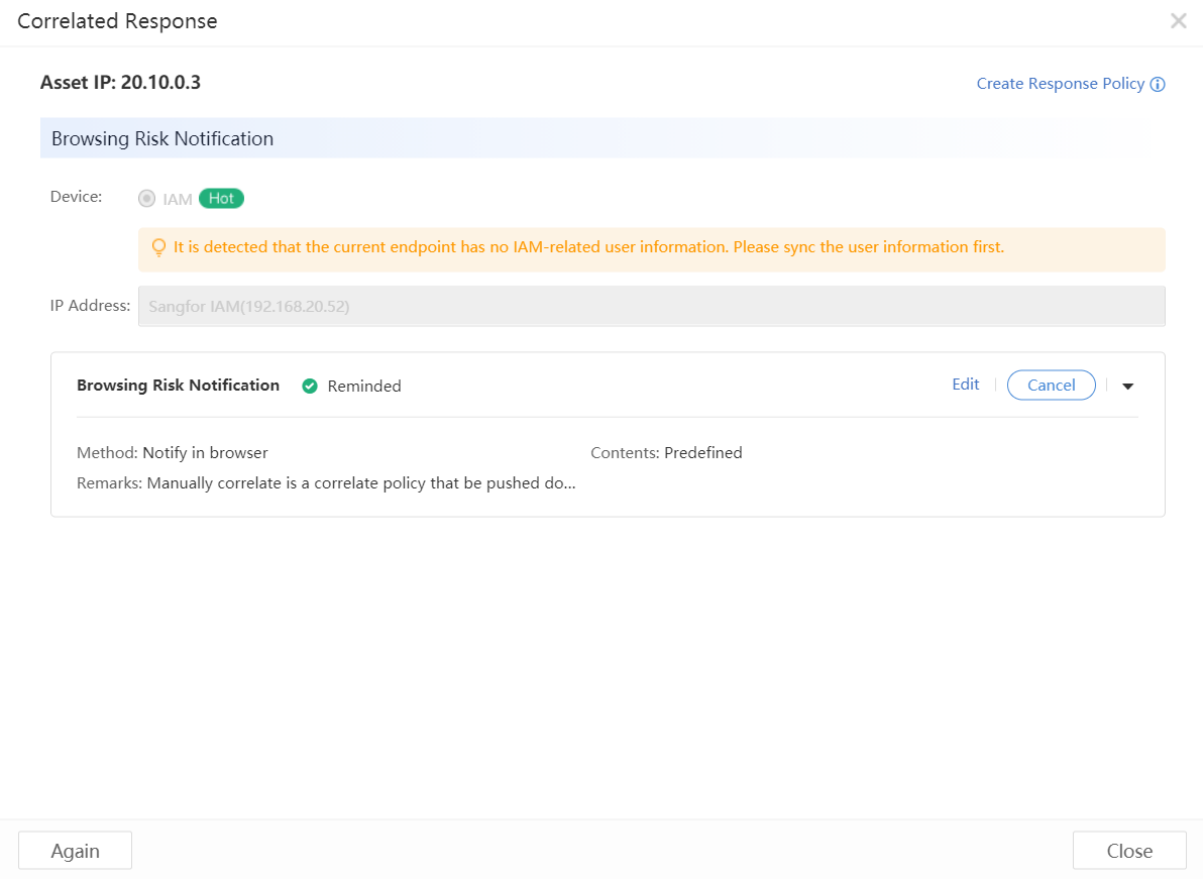
1. If you just want to notify the endpoint user to know the security issue, you can click Correlated Response.



2. Select predefined notification page or you can custom page by yourself.



3. Click OK and wait for a minute, you can see the policy issued successfully.



4. When endpoint user try to access the internet, IAM will direct the access page to notification page.