



**SANGFOR**



# 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
1.1 Scenario .....	1
1.2 Environment .....	1
1.2.1 Network Environment .....	1
1.3 Precautions .....	1
Chapter 2 Configure .....	2
2.1 Configure IAM.....	2
2.2 Configure Cyber Command .....	5
2.3 Configure Endpoint Secure .....	6
Chapter 3 Correlation.....	9
3.1 Synchronize Logs to Cyber Command.....	9
3.2 Response in Cyber Command.....	12
3.2.1 Lockout the Account .....	12
3.2.2 Browsing Risk Notification.....	14

# Chapter 1 Scenario

## 1.1 Scenario

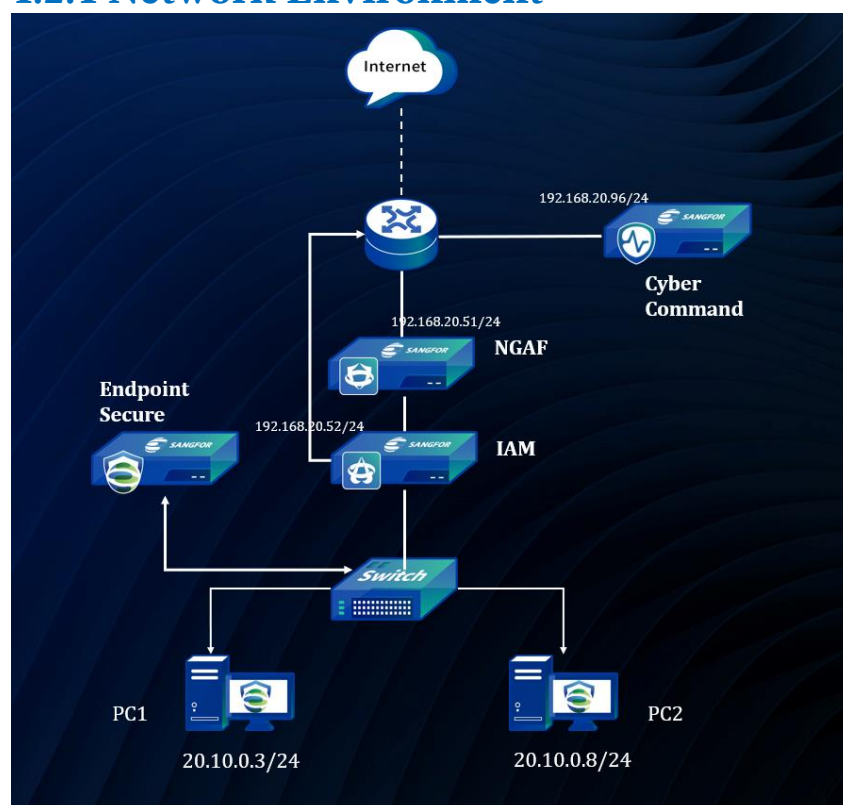
Cyber Command collects data from security detection probes of each intranet node, presents users with intranet business assets and attacks and potential threats against intranet key business assets in a visual form, and uses the platform to attack all security systems on the existing network Carry out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

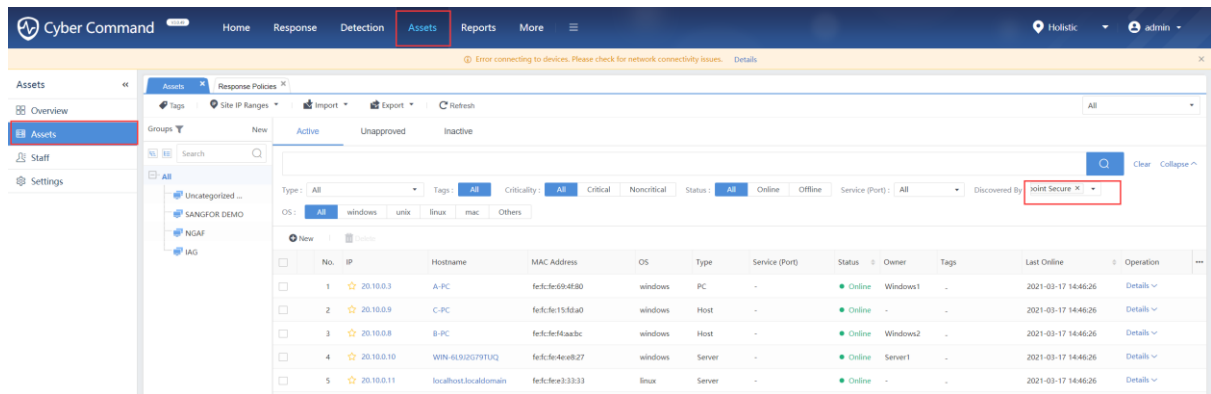
### 1.2.1 Network Environment



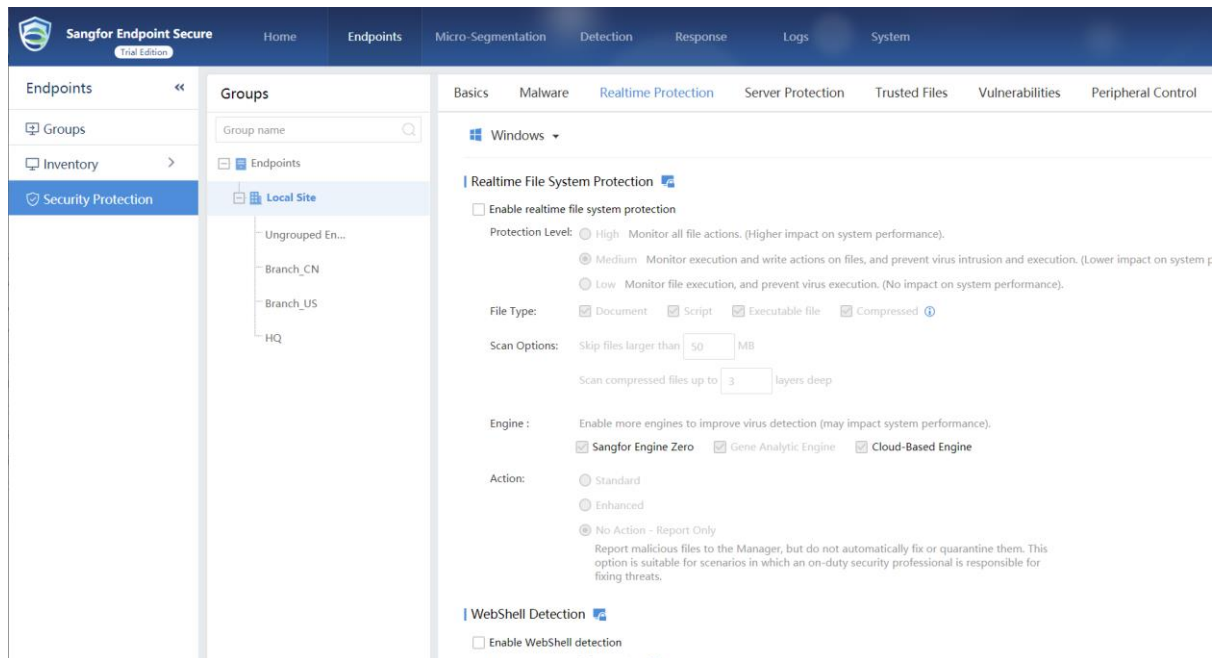
## 1.3 Precautions

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.

## How to Correlate with IAM to Simply the Operation



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.**

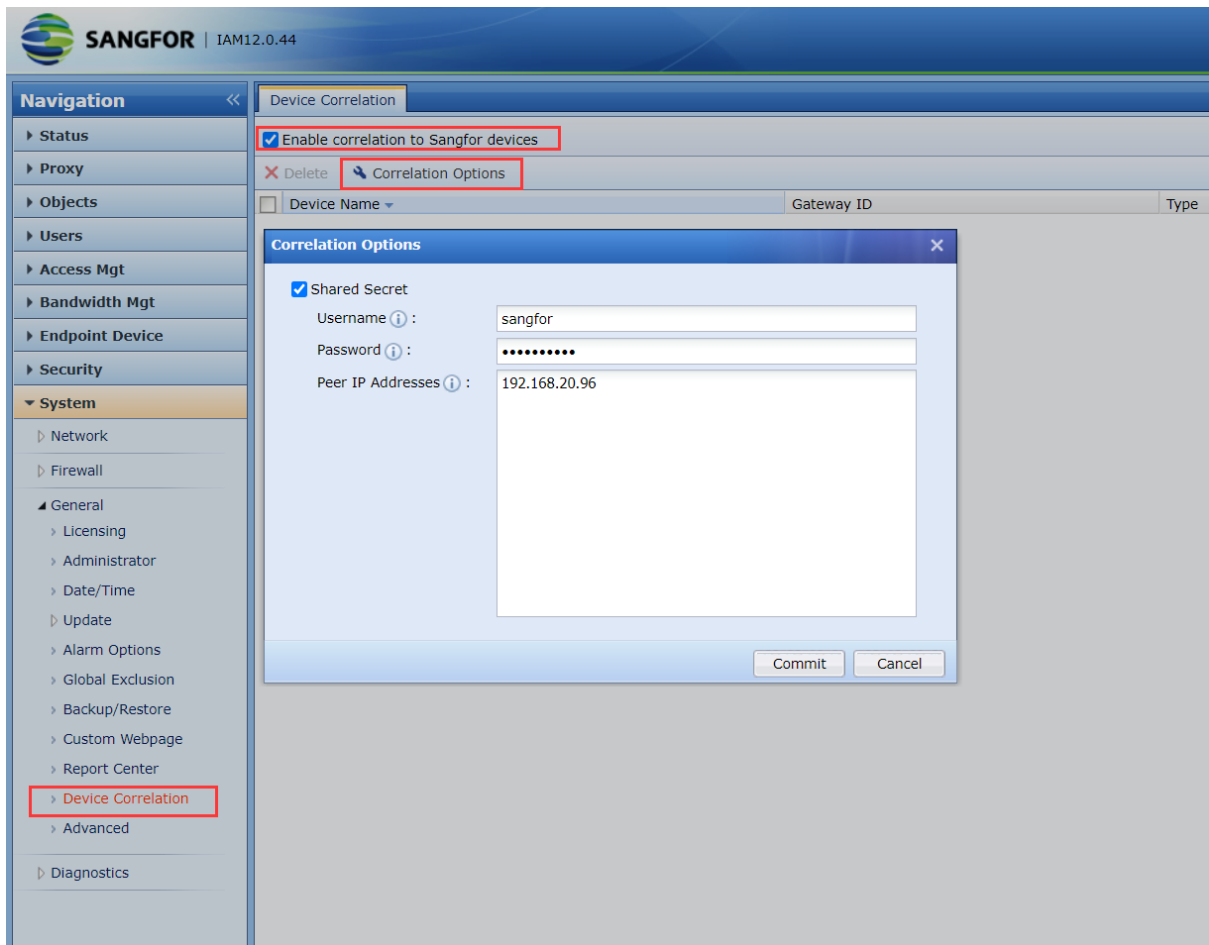


## Chapter 2 Configure

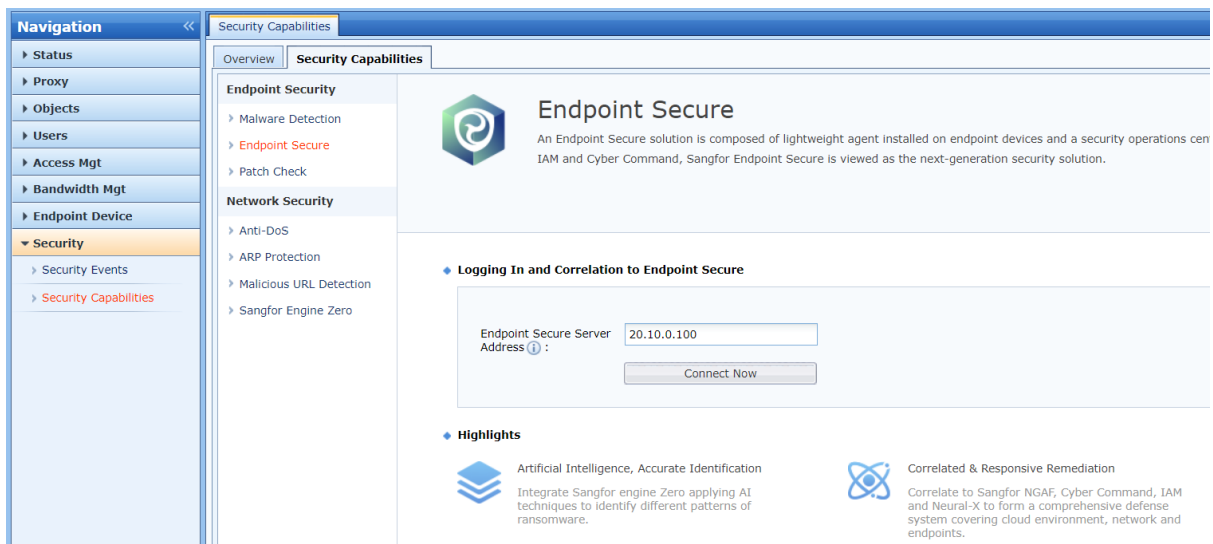
### 2.1 Configure IAM

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

## How to Correlate with IAM to Simply the Operation

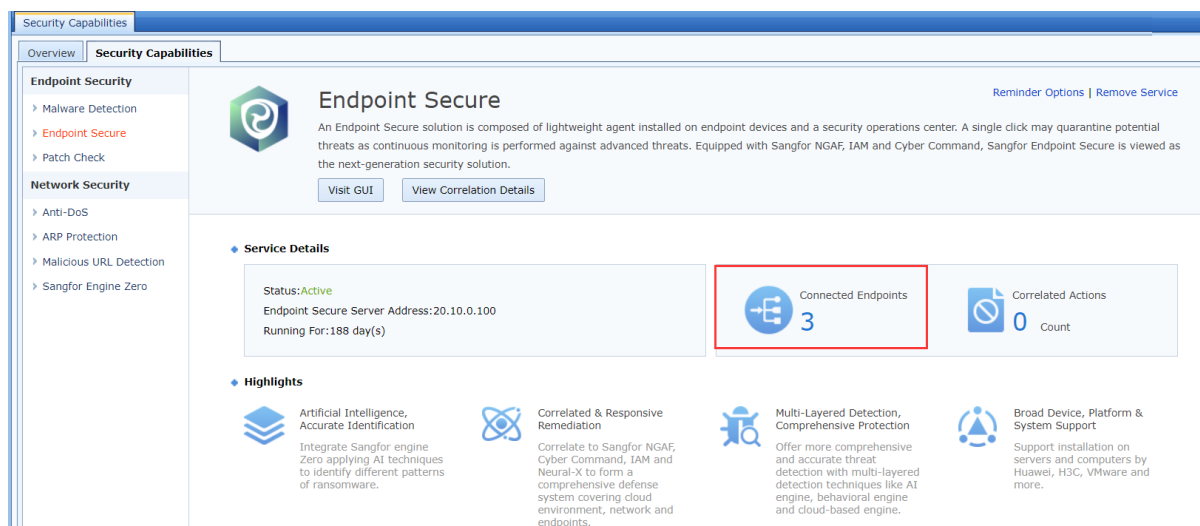


2. Go to Security-> Security Capabilities path. Input the IP address of Endpoint Secure.



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

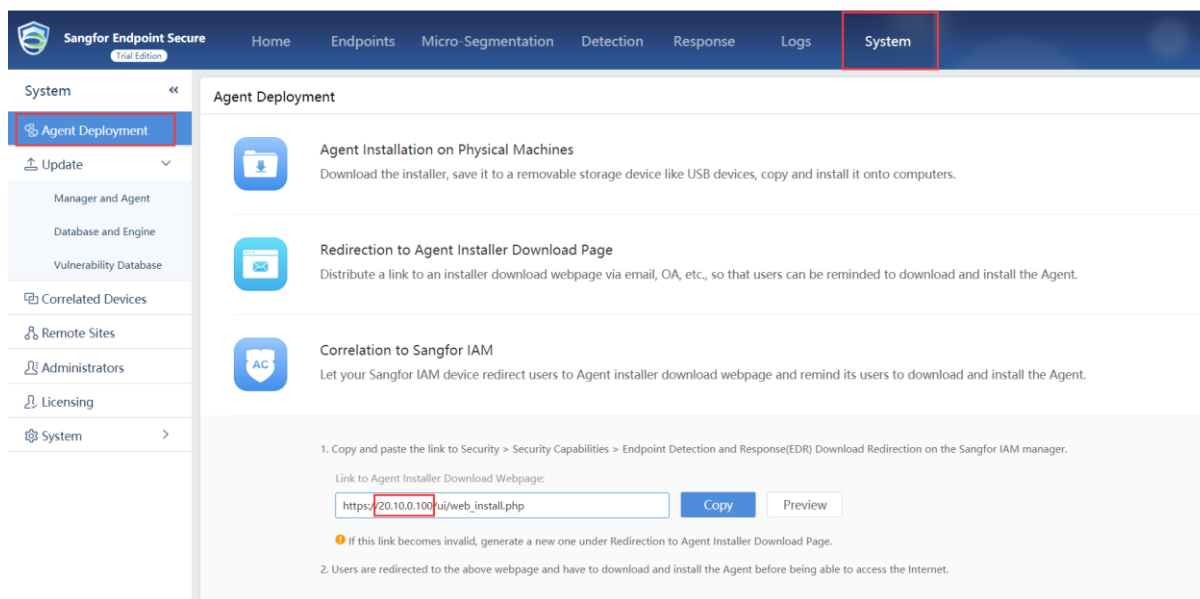
## How to Correlate with IAM to Simply the Operation



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

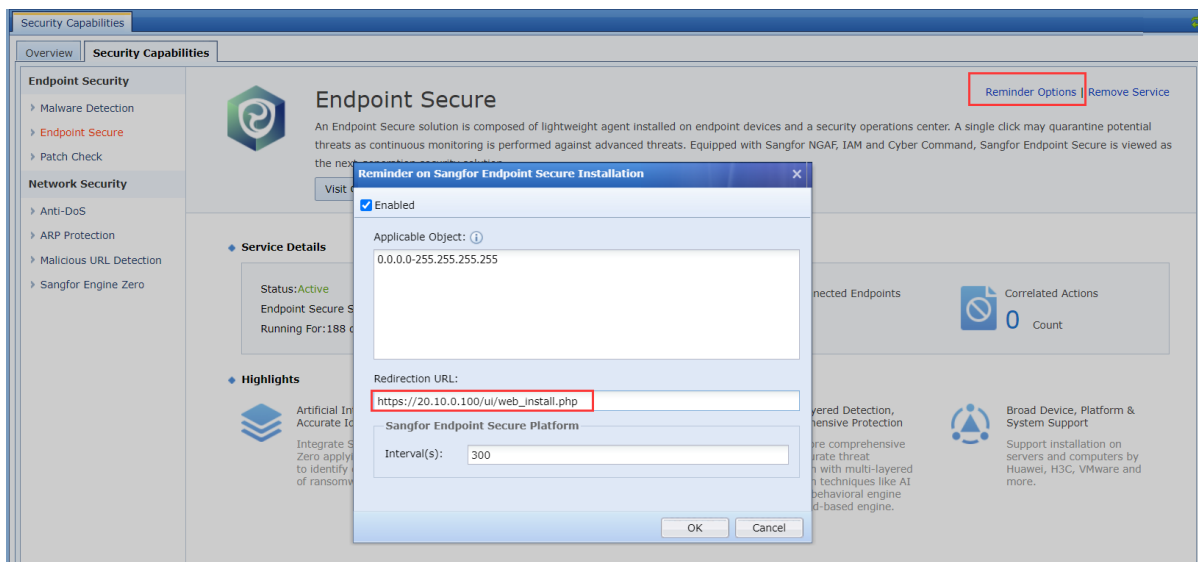
First, configure risk reminder page address in Endpoint Secure, you can you System-> Agent Deployment-> Correlation to Sangfor IAM page and configure ES agent download address so that IAM can direct PC to ES agent download page.

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



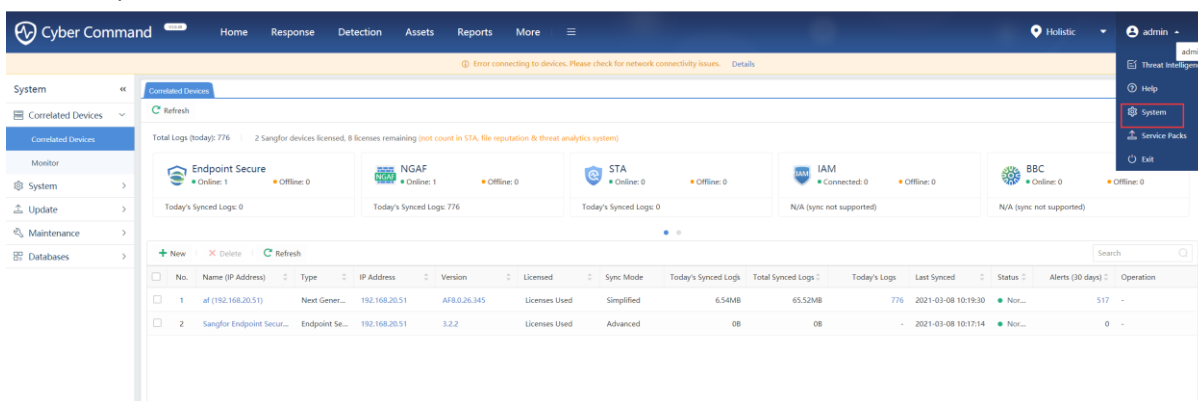
Second, configure reminder policy in IAM, please ensure the redirection URL is same as you configured in ES.

## How to Correlate with IAM to Simply the Operation

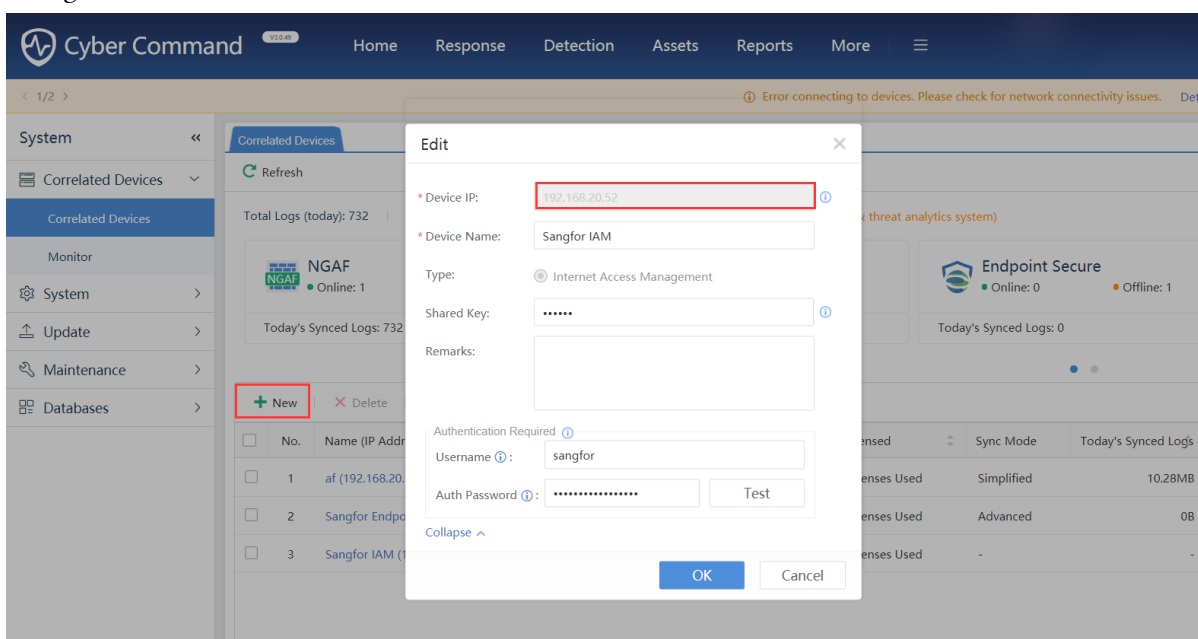


## 2.2 Configure Cyber Command

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.



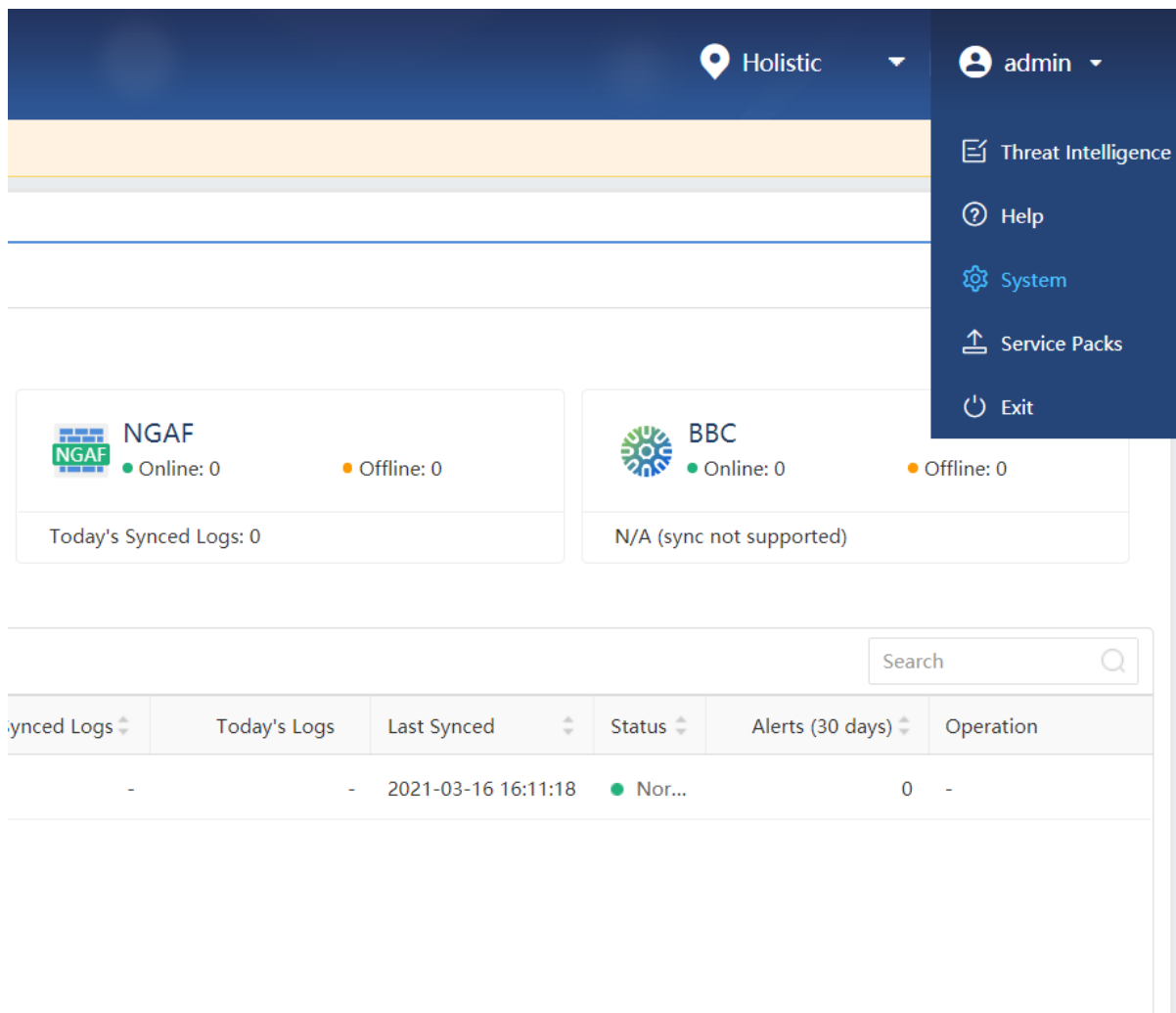
3. If you are not sure whether the username and password were correct, you can click Test to check the account validity.

The image shows a software interface for editing an endpoint configuration. The window is titled "Edit" and contains several fields: "Device IP" (with a green checkmark and "Authentication passed." message), "Device Name" (containing "sangfor"), "Type" (set to "Internet Access Management"), "Shared Key" (masked with dots), and "Remarks" (empty). Below these is an "Authentication Required" section with "Username" (containing "sangfor") and "Auth Password" (masked with dots). A "Test" button is highlighted with a red box. At the bottom are "OK" and "Cancel" buttons.

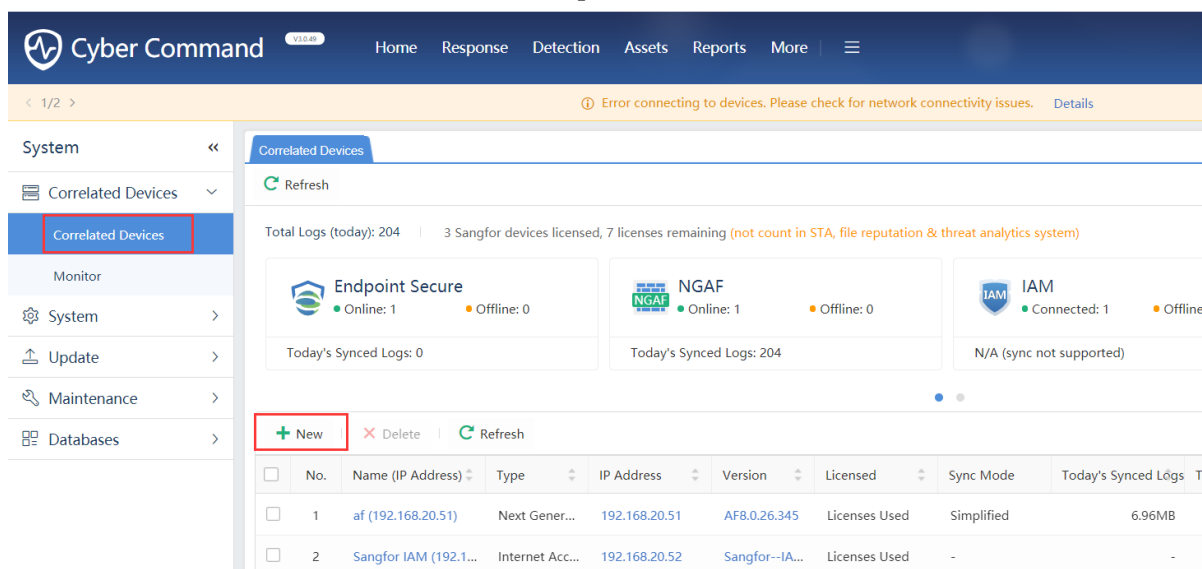
## 2.3 Configure Endpoint Secure

1. Go to System Path.

## How to Correlate with IAM to Simply the Operation

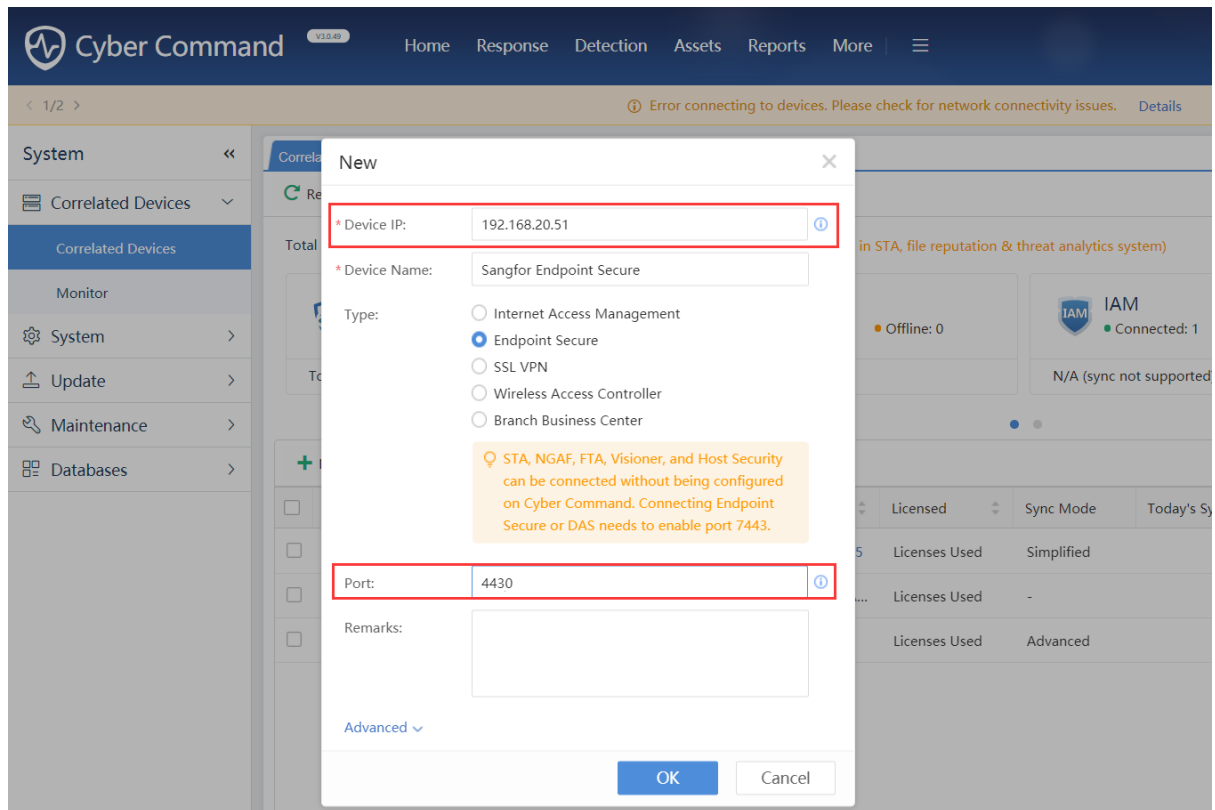


2. Go to Correlated Devices-> Correlated Devices path, and click New to create Correlation.

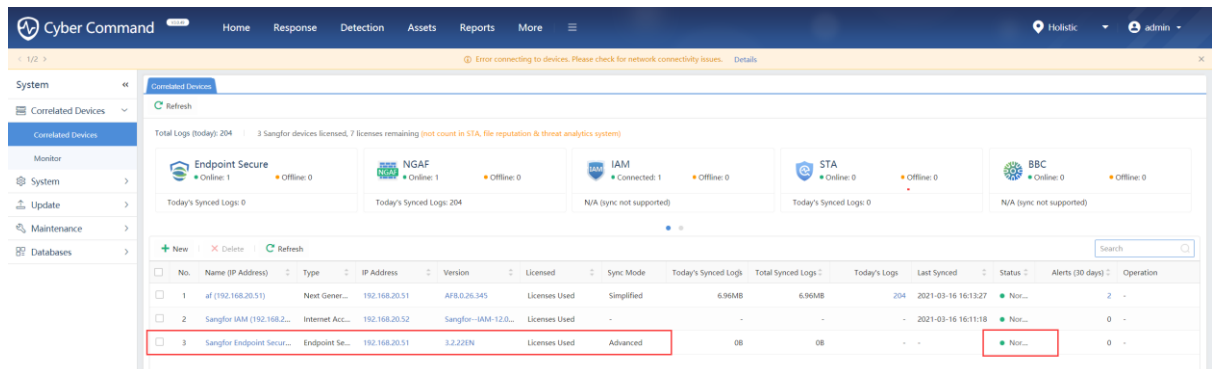


3. Input the IP of Endpoint Secure and the Port, if Endpoint Secure deployed after a NAT device, Please map the 443 port of Endpoint Secure to the NAT device. For example, here is the 4430 port mapped to the NAT device.

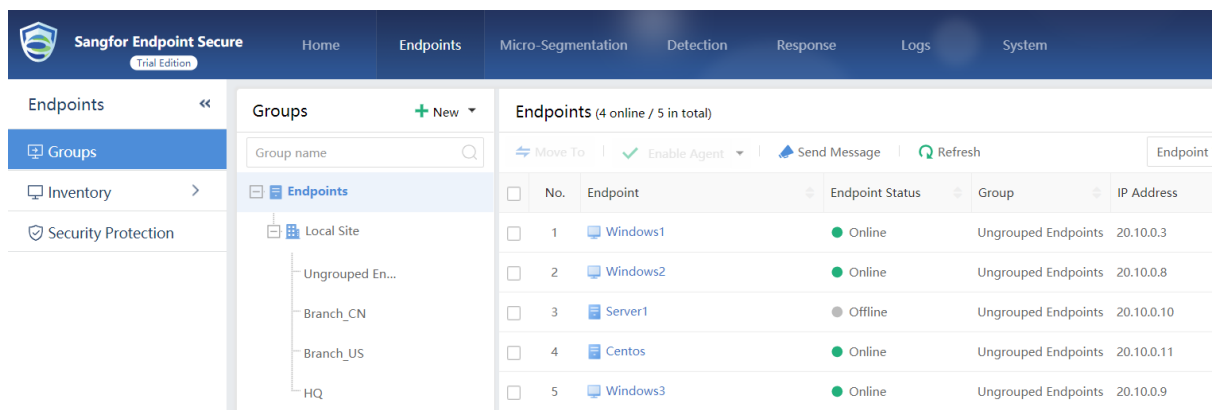
## How to Correlate with IAM to Simply the Operation



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

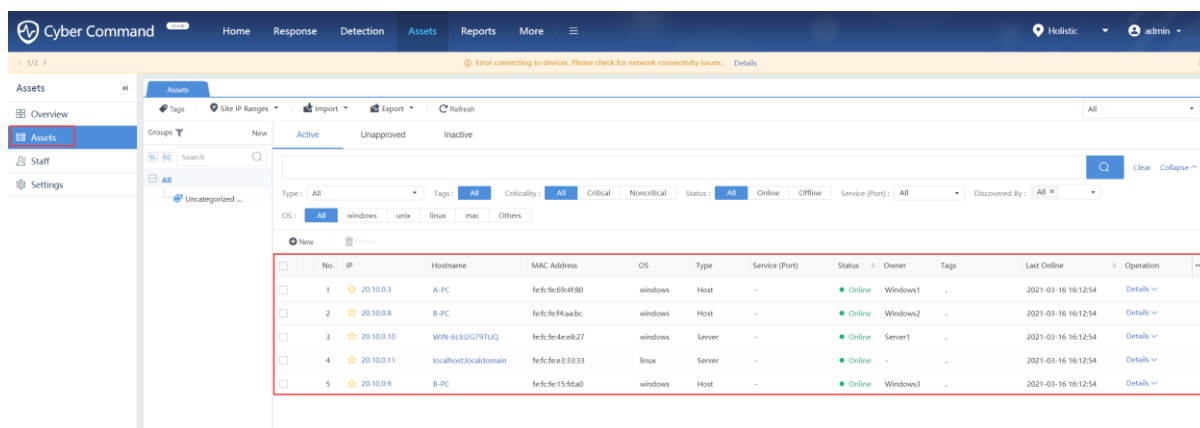


5. You can check whether there exists assets in Endpoint Secure.

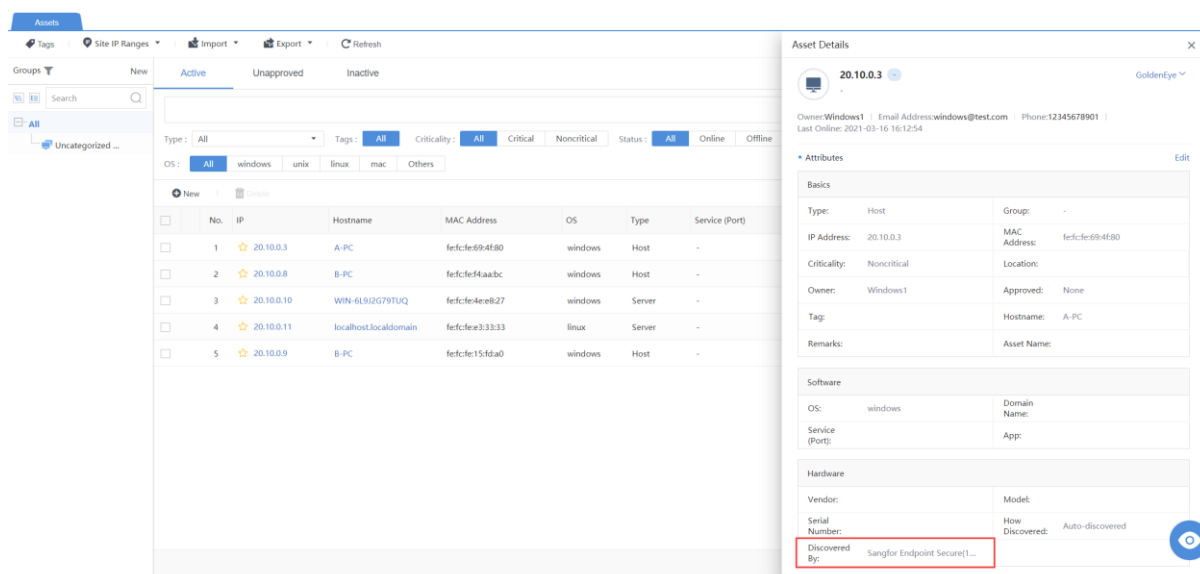


6. If you there exists in Endpoint Secure, you Go to Assets->Assets in Cyber Command to check whether assts has been synchronized to Cybercommand.

## How to Correlate with IAM to Simply the Operation



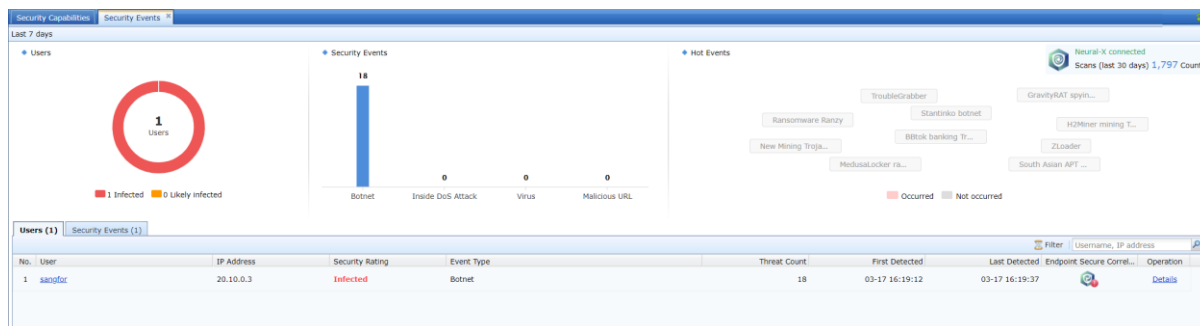
7. You can view the details to see the assets source, such as following detail, you can see this asset discovered by Endpoint Secure.



## 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.

## How to Correlate with IAM to Simply the Operation

**Solution**  
Correlate that host to Sangfor Endpoint Secure to fix this issue. [Analyze via Endpoint Secure](#)

Endpoint Secure detection and analytics found no victim hosts. Please log in to Endpoint Secure to perform full scan and fix the possible threats. Close

**Security Events**

No.	Time	Type	Dest IP	Threat Level	Action	Description	Data Packet	Threat Intelligence	Details
1	03-17 17:28:24	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (cptrivpopp.cn) or IP address (8.8.4.4) provided by cncret organ	View	View	Details
2	03-17 17:28:24	Botnet	8.8.8.8	Low	Reject	Host visits malicious domain name (cptrivpopp.cn) or IP address (8.8.8.8) provided by cncret organ	View	View	Details
3	03-17 17:28:20	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (cptrivpopp.cn) or IP address (8.8.4.4) provided by cncret organ	View	View	Details
4	03-17 17:28:20	Botnet	8.8.8.8	Low	Reject	Host visits malicious domain name (cptrivpopp.cn) or IP address (8.8.8.8) provided by cncret organ	View	View	Details
5	03-17 17:28:18	Botnet	8.8.8.8	Low	Reject	Host visits malicious domain name (cptrivpopp.cn) or IP address (8.8.8.8) provided by cncret organ	View	View	Details
6	03-17 17:28:18	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (cptrivpopp.cn) or IP address (8.8.4.4) provided by cncret organ	View	View	Details
7	03-17 17:28:17	Botnet	8.8.8.8	Low	Reject	Host visits malicious domain name (cptrivpopp.cn) or IP address (8.8.8.8) provided by cncret organ	View	View	Details
8	03-17 17:28:17	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (cptrivpopp.cn) or IP address (8.8.4.4) provided by cncret organ	View	View	Details
9	03-17 17:28:15	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (cptrivpopp.cn) or IP address (8.8.4.4) provided by cncret organ	View	View	Details
10	03-17 17:28:11	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (update.7h4uk.com) or IP address (8.8.4.4) provided by cncret	View	View	Details
11	03-17 17:28:11	Botnet	8.8.8.8	Low	Reject	Host visits malicious domain name (update.7h4uk.com) or IP address (8.8.8.8) provided by cncret	View	View	Details
12	03-17 17:28:08	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (update.7h4uk.com) or IP address (8.8.4.4) provided by cncret	View	View	Details
13	03-17 17:28:08	Botnet	8.8.8.8	Low	Reject	Host visits malicious domain name (update.7h4uk.com) or IP address (8.8.8.8) provided by cncret	View	View	Details
14	03-17 17:28:06	Botnet	8.8.8.8	Low	Reject	Host visits malicious domain name (update.7h4uk.com) or IP address (8.8.8.8) provided by cncret	View	View	Details
15	03-17 17:28:06	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (update.7h4uk.com) or IP address (8.8.4.4) provided by cncret	View	View	Details
16	03-17 17:28:05	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (update.7h4uk.com) or IP address (8.8.4.4) provided by cncret	View	View	Details
17	03-17 17:28:05	Botnet	8.8.8.8	Low	Reject	Host visits malicious domain name (update.7h4uk.com) or IP address (8.8.8.8) provided by cncret	View	View	Details
18	03-17 17:28:03	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (update.7h4uk.com) or IP address (8.8.4.4) provided by cncret	View	View	Details
19	03-17 17:27:55	Botnet	8.8.4.4	Low	Reject	Host visits malicious domain name (bddd.net) or IP address (8.8.4.4) provided by cncret organizati	View	View	Details

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

**Protect Agent**

**Security**

**Quick scan, 6 threats detected**  
00:01:17 C:\Users\Administra...e-synch-l1-1-0.dll

**Virus Scan**

**Realtime Protection**

**Tools**

**System Processes**  
48 files scanned

**Startup Items**  
5 files scanned

**Drivers and Services**  
2 files scanned

**Critical System Files**  
106 files scanned **6 files**

Security Engines: [Icons]

Auto shut down your computer when scan completes

# How to Correlate with IAM to Simply the Operation

The screenshot shows the Sangfor Endpoint Secure console. On the left, the 'Security Events' section displays a list of events with columns for No., Time, Type, and Severity. A line graph above the list shows event counts over time. The main area features an 'Analytics Results' window with a table of detected files and their status. The table includes columns for No., Host(s), Virus Type, Infected Files, Status, and Operation. A 'Data Packet' section on the right provides details for specific events, including IP addresses and threat intelligence.

No.	Host(s)	Virus Type	Infected Files	Status	Operation
1	20.10.0.3	Ransom virus	Malicious Files: c:\user\administrator\desktop File Hash: 008D67CF7141C9F86C22442E	Waiting	Isolate, Trust, Ignore Big Data Analytics
2	20.10.0.3	Other viruses	Malicious Files: c:\user\administrator\desktop File Hash: 002A4888564779316774318906	Waiting	Isolate, Trust, Ignore Big Data Analytics
3	20.10.0.3	Other viruses	Malicious Files: c:\user\administrator\desktop File Hash: 016AC05898A3170782C02028A12	Waiting	Isolate, Trust, Ignore Big Data Analytics
4	20.10.0.3	Other viruses	Malicious Files: c:\user\administrator\desktop File Hash: 00888783175436A2E11C18812	Waiting	Isolate, Trust, Ignore Big Data Analytics
5	20.10.0.3	Other viruses	Malicious Files: c:\user\administrator\desktop File Hash: 00888783175436A2E11C18812	Waiting	Isolate, Trust, Ignore Big Data Analytics
6	20.10.0.3	Ransom virus	Malicious Files: c:\user\administrator\desktop File Hash: 0014081AC3D654D5DC9A9768CD	Waiting	Isolate, Trust, Ignore Big Data Analytics
7	20.10.0.3	Ransom virus	Malicious Files: c:\user\administrator\desktop File Hash: 8028502707CA1294EC33002591	Waiting	Isolate, Trust, Ignore Big Data Analytics
8	20.10.0.3	Other viruses	Malicious Files: c:\user\administrator\desktop File Hash: 0272047F8531880C23F4649624	Waiting	Isolate, Trust, Ignore Big Data Analytics

This screenshot displays the 'Threat Response' section of the Sangfor Endpoint Secure console. It features a summary dashboard with four metrics: 1 Victim Endpoints, 3 Compromised, 0 Critical, and 0 Suspicious. Below the dashboard is a table of endpoints with columns for No., Endpoint, Group, Severity, Security Events, Pending/Total Threats, Last Detected, and Operation. The table shows one endpoint, 'Windows1 (20.10.0.3)', which is 'Ungrouped Endpoints' and 'Compromised'.

No.	Endpoint	Group	Severity	Security Events	Pending/Total Threats	Last Detected	Operation
1	Windows1 (20.10.0.3)	Ungrouped Endpoints	Compromised	Ransomware, Trojan, Others	41/139	2021-03-17 18:11:39	Fix, Isolate

The screenshot shows the 'Risky Hosts' section of the Cyber Command console. It includes a summary dashboard with 2/56 Hosts (Risky/All), 2 Compromised, 0 High, 0 Medium, and 0 Low risk levels. A table below lists the hosts with columns for No., Hostname, Risk Level, Tags, Last Detected, and Status. Two hosts are listed: 'A-PC' and 'B-PC', both with a 'Compromised' risk level and 'Fixed' status.

No.	Hostname	Risk Level	Tags	Last Detected	Status
1	A-PC	Compromised	EDR, Virus	2021-03-17	Fixed (Correlated)
2	B-PC	Compromised	EDR, Virus	2021-03-17	Fixed

This screenshot provides a detailed view of a 'Risky Host' (A-PC) in the Cyber Command console. It shows the host's risk level as 'Compromised' and its status as 'Fixed'. The 'Summary' section includes a 'Stages of Attack' diagram showing the progression from 'Vuln Detected' to 'Data Theft'. The 'Impact Scope' section displays metrics for LAN and WAN impacted servers, hosts, and victims. The 'Risk Levels' section shows a bar chart of risk levels over time, with 9 Compromised, 6 High, and 3 Low risk levels.

**Stages of Attack:** Vuln Detected → Ever Attacked → CBC Comm → Scan Intranet → Laterally Propagate → Data Theft

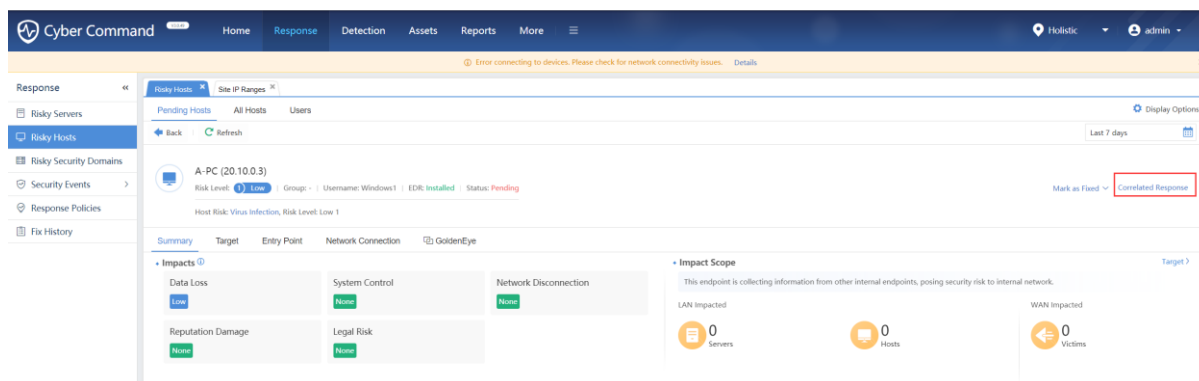
**Impact Scope:** LAN Impacted: 0 Servers, 0 Hosts, 0 Victims; WAN Impacted: 0 Servers, 0 Hosts, 0 Victims

**Risk Levels:** 9 Compromised, 6 High, 3 Low

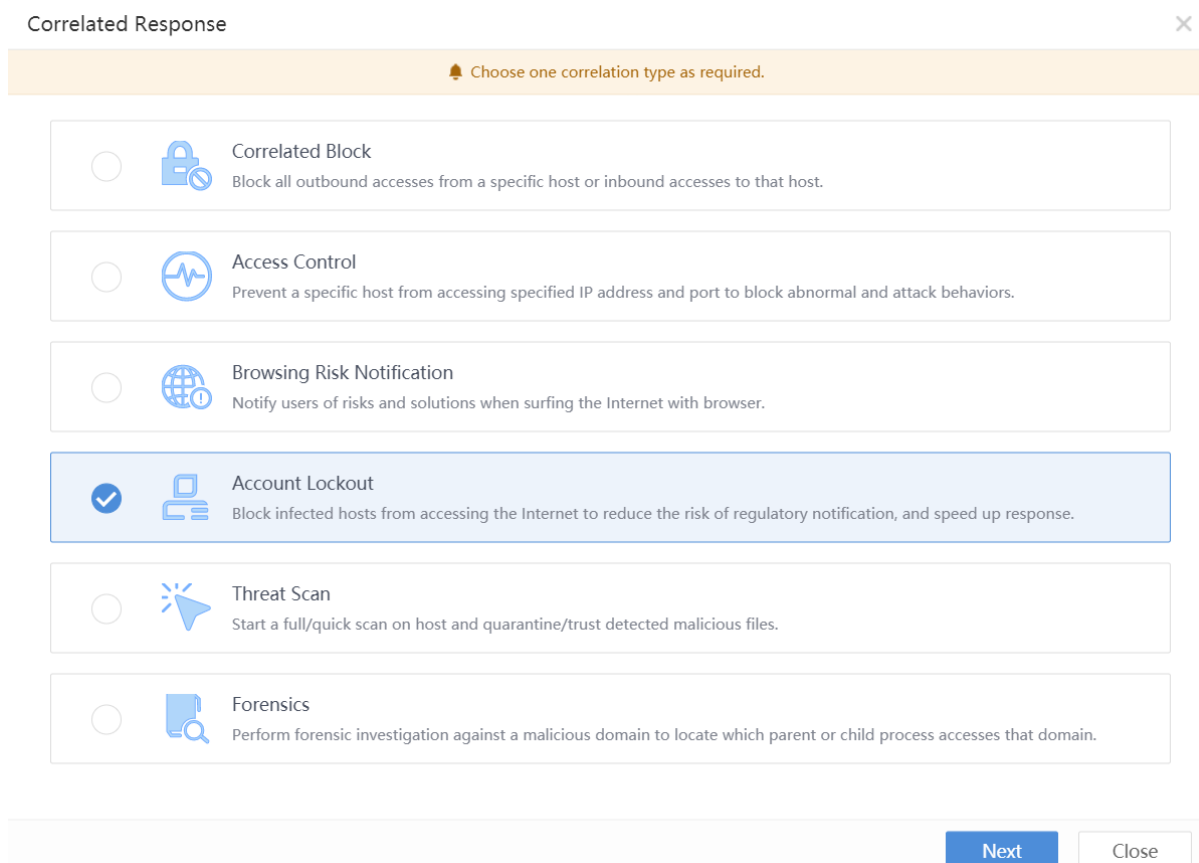
## 3.2 Response in Cyber Command

### 3.2.1 Lockout the Account

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

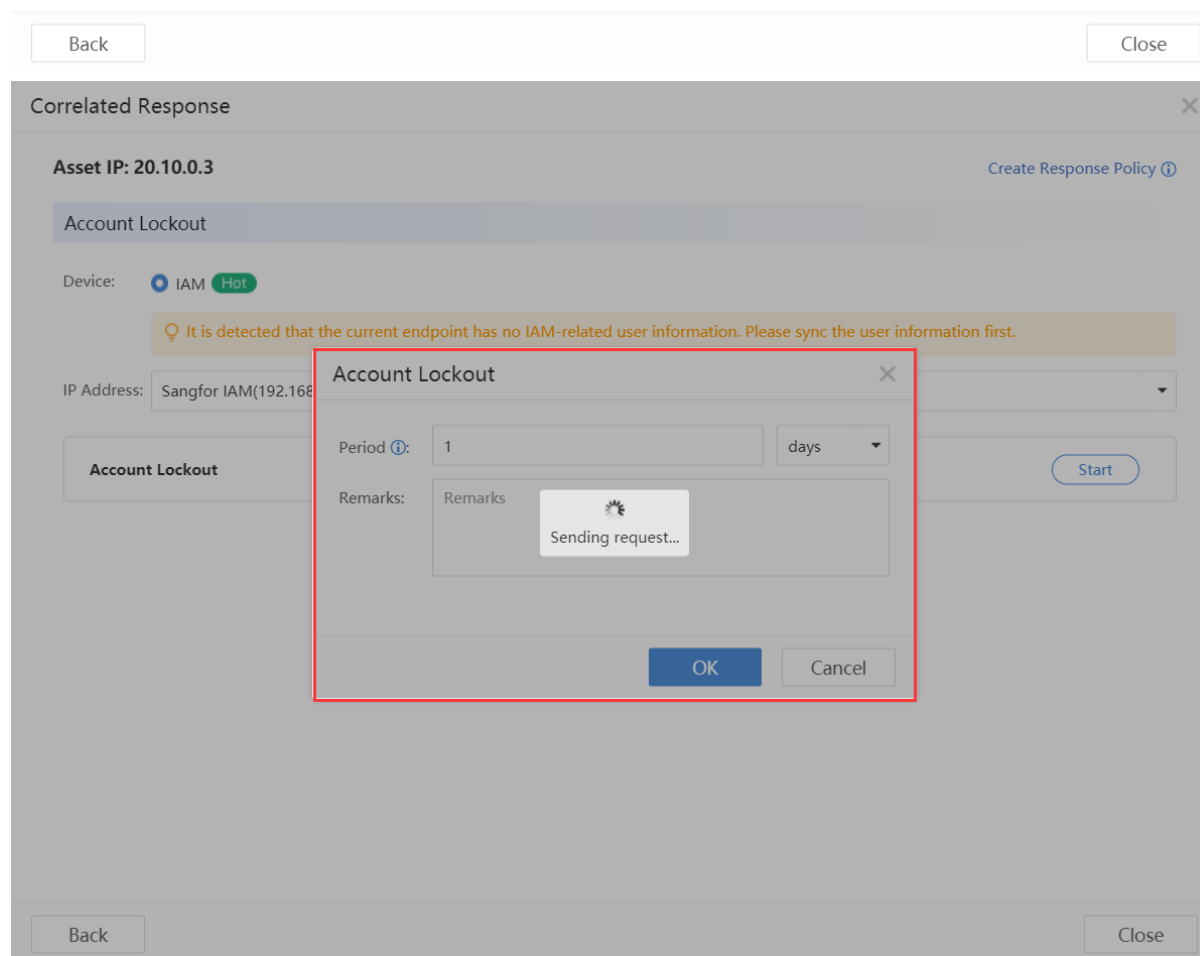
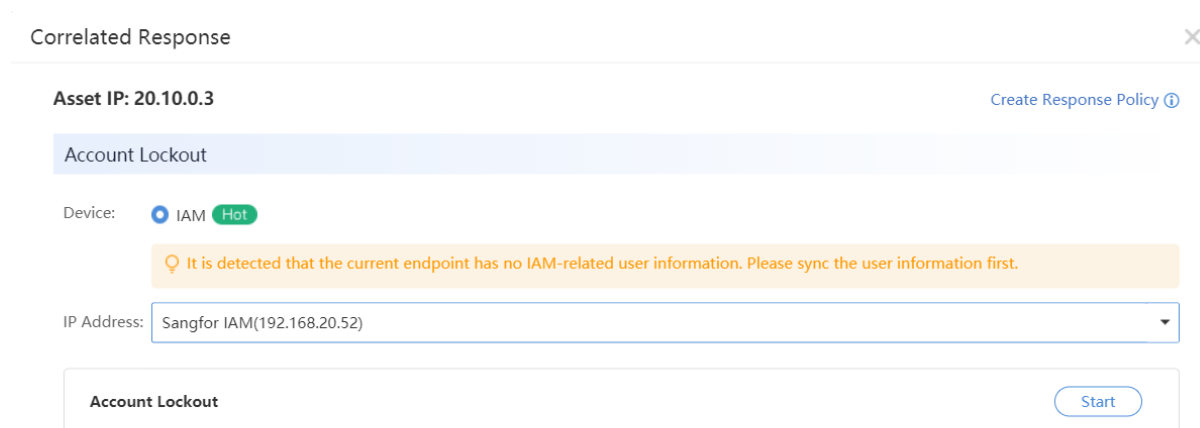


2. Select Account Lockout.



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

## How to Correlate with IAM to Simply the Operation



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

## How to Correlate with IAM to Simply the Operation

Correlated Response ✕

Asset IP: 20.10.0.3

[Create Response Policy](#)

Account Lockout

Device:  IAM Hot

🔔 It is detected that the current endpoint has no IAM-related user information. Please sync the user information first.

IP Address: Sangfor IAM(192.168.20.52)

**Account Lockout** 🔔 Locked (1 days 0 hours 00 mins)

[Edit](#) | [Cancel](#) |

Period: 1 days

Remarks: Manually correlate is a correlate policy that be pushed do...

Again

Close

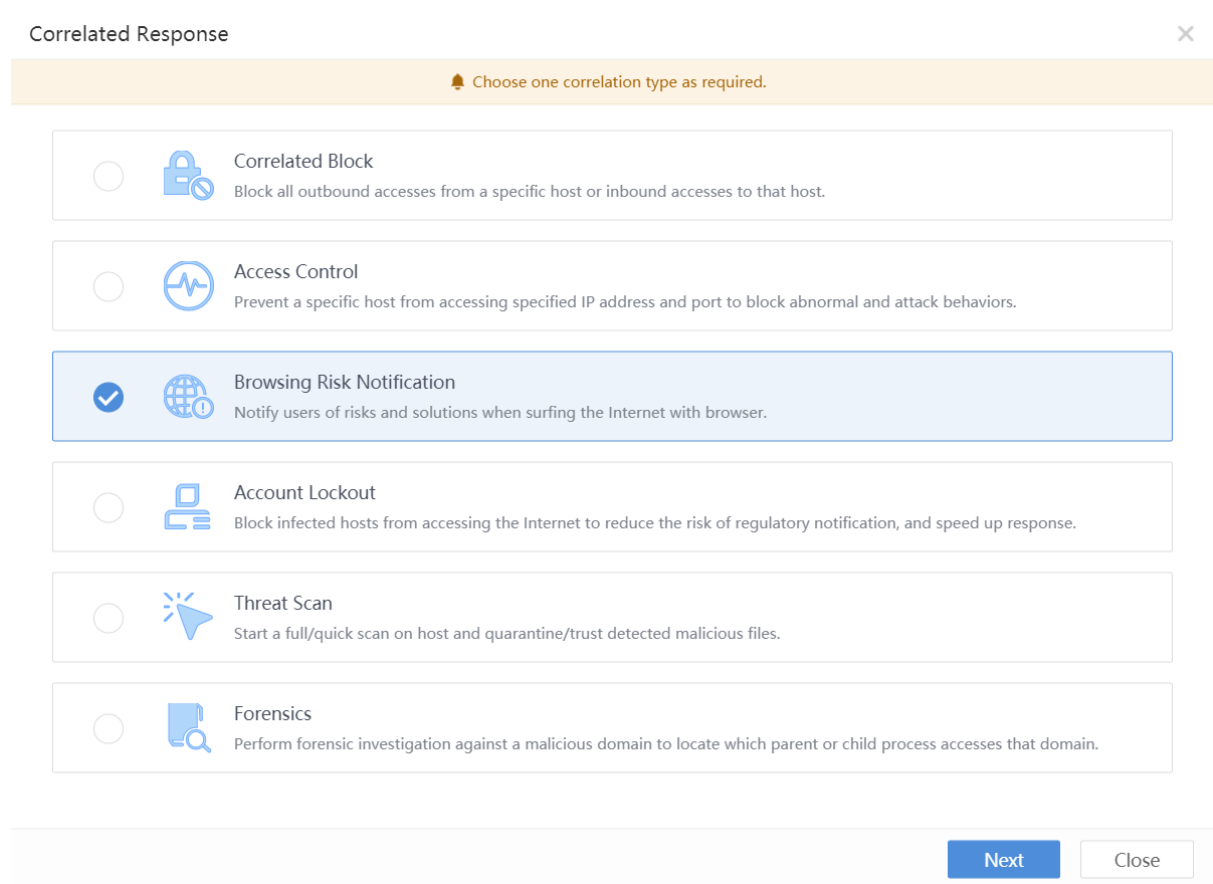
5. Log in IAM web console and go to Status-> Online Users path, you can see the user already locked by IAM.

No.	Username(Alias)	Group	IP Address	Endpoint Device	Auth Method	Time Logged In/Locked	Online Duration	Operation
1	sangfor	/	20.10.0.3	PC(Windows PC)	User Account	2021-03-17 15:10:12Lock	Locked, 23 hours 57 minut...	
2	20.10.0.11	/	20.10.0.11	Verifying...	Open authenticati...	2021-03-05 11:07:37Login	292 hours 04 minutes 47 s...	
3	20.10.0.9	/	20.10.0.9	Verifying...	Open authenticati...	2021-03-04 09:21:50Login	317 hours 50 minutes 34 s...	
4	20.10.0.100	/	20.10.0.100	Verifying...	Open authenticati...	2021-03-02 15:45:30Login	359 hours 26 minutes 54 s...	

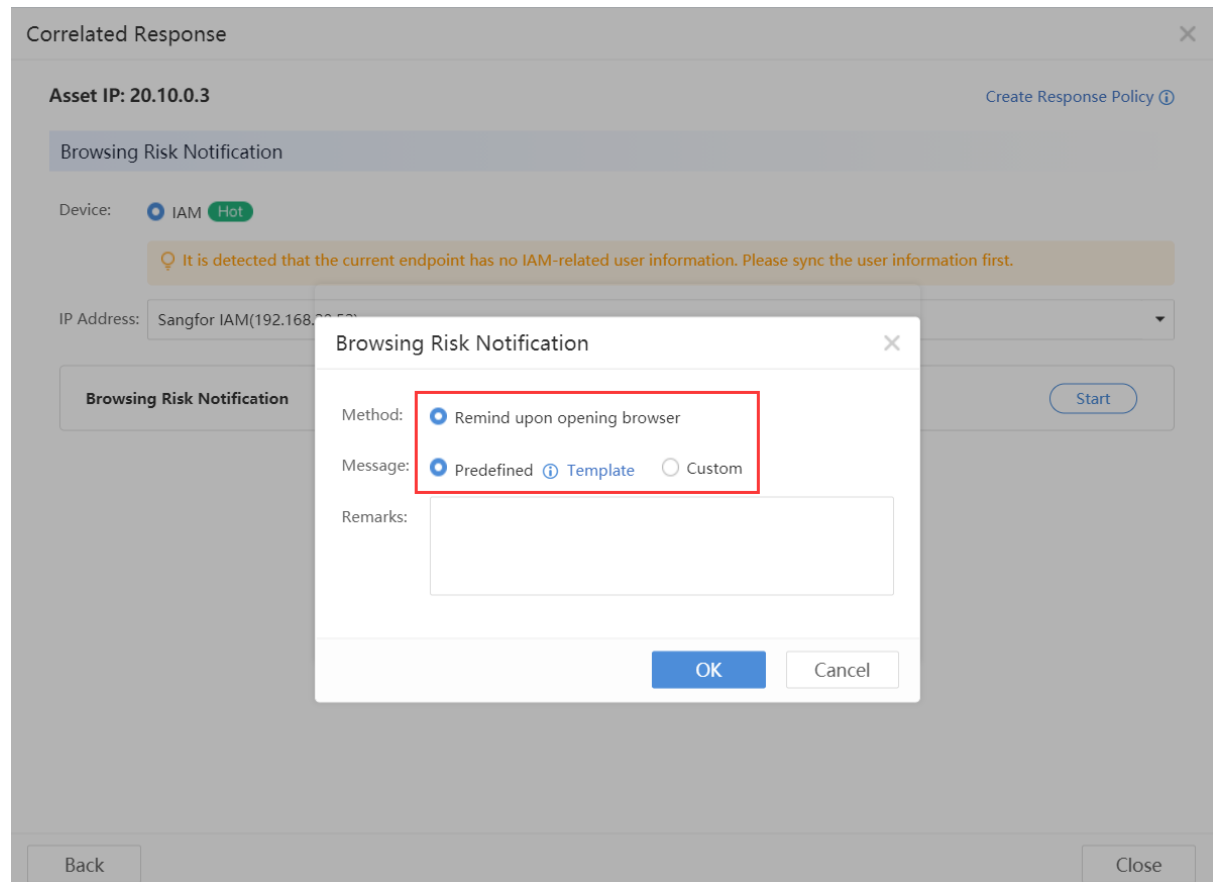
### 3.2.2 Browsing Risk Notification

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

## How to Correlate with IAM to Simply the Operation



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.

## How to Correlate with IAM to Simply the Operation

Correlated Response ✕

**Asset IP: 20.10.0.3** Create Response Policy ⓘ

**Browsing Risk Notification**

Device:  IAM Hot

⚠ It is detected that the current endpoint has no IAM-related user information. Please sync the user information first.

IP Address: Sangfor IAM(192.168.20.52)

**Browsing Risk Notification** ✔ Reminded Edit | Cancel | ▼

---

Method: Notify in browser Contents: Predefined

Remarks: Manually correlate is a correlate policy that be pushed do...

Again Close

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

1113/freeze\_user/notice\_user.htm

Not secure | 1113/freeze\_user/notice\_user.htm

**Reminder**

You received a new message on Internet access. If you have any doubt, contact network administrator.

**The host is infected with virus.**

**Suggestions**

1. The log is reported by Sangfor Endpoint Secure Client. It is recommended to log into Sangfor Endpoint Secure Web admin console to isolate the host.
2. In addition, you can download Sangfor Endpoint Secure Client for virus scan and removal: [https://www.sangfor.com/product/sxf-network-security-endpoint\\_secure.html](https://www.sangfor.com/product/sxf-network-security-endpoint_secure.html)

OK



**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