SANGFOR

IAG 13.0.15 Beta Guidance

Applicable Version: IAG 13.0.15 and above

13.0.15 Update Note

- IAM name changing, changed from IAM to IAG.
- License mode changes, all IAG License mode will be delivered by subscription.
- New Asset Identification Capabilities:

1) Built-in identification technology, fast and accurate identification of assets. Can identify PC, mobile Endpoint, dumb Endpoint, medical equipment and other categories of dozens of small categories. The homepage can see the asset overview of the intranet at a glance.
2) Support assets list delete, change, check operation, display Endpoint assets compliance status, can quickly batch approval into the network, reduce Endpoint perception. For the problem Endpoint write-off, support freeze control.
3) Support custom Endpoint type. For unidentified assets, the Endpoint type can be set according to fingerprint characteristics.
4) Can set access rights policy and other control policies according to the identified small class Endpoint types to solve the problem of permissions of different Endpoint types.
5) IP management effect optimization. Perform clustering and segmentation viewing of the IP segments of interest.

- Endpoint security check capability update:

1) New Endpoint access detection rules, including Anti-Virus Software Based Rule,Login Domain Based Rule,Access Check,Access Control,External Device Control,Windows Account Based Rule and Anti-Defacement Rule.
2) New no-client detection ability. Based on the traffic, the Endpoint anti-virus installation situation can be detected and repair instructions can be carried out.

1.Product Name Change Statement (BETA)

Dear Customer:

In order to better provide you with high-quality services and experience, and to improve our product positioning and value, SANGFOR IAM will officially change the product name from the original IAM (Internet Access Management) to IAG (Internet Access Gateway) since version 13.0.15. After the name change, we will focus more on improving the network management experience and security assurance for your organization. At the same time, we will also bring cloud-based or hybrid deployment management features, so stay tuned.

IAG 13.0.15 GA will be officially released at 24:00 (Hong Kong time) on April 30, 2021. From the time the name is changed, all subsequent software and hardware delivery, technical support, after-sales service and other related businesses will be changed. Please note that this will not affect your current product experience and services. On the contrary, we will continue to work hard and continue to bring you a better experience.

If you have any questions or suggestions about our name change, please do not hesitate to contact our product manager Eugene (eugene.yew@sangfor.com) , or contact your local Sangfor office, we will be happy to provide you with services.

SANGFOR IAG TEAM

2.License Mode Change Statement (BETA)

Dear Customer:

In order to better provide you with high-quality services, and to enhance your experience when purchasing SANGFOR IAG products, we will change the product license model to a subscription model since the release of IAG 13.0.15. If you are a customer applying for a trial for the first time, this will not affect your trial. But if you are using SANGFOR IAG device and plan to participate in this BETA process to experience new features, please pay attention to the following points:

1. This BETA process adopts the form of upgrading the firmware package. You will need to upgrade your device to the IAG13.0.15 (beta) version. Please note that after the upgrade is completed, you will not be able to downgrade or revert to the lower version.

*2. If your device software version is lower than 12.0.41 (not included), and the **Software update license** is within the valid period, you will be able to upgrade. After the upgrade, you will get a free **Device License** and **Multi-function License** for up to **3 years** from the date of the upgrade. For example, if you purchased a device on January 1, 2020, but upgraded to version 13.0.15 on January 1, 2021, the expiration time of the **Device License** and **Multi-function License** will change to January 1, 2024 after the upgrade. The license status and expiration time of the remaining modules remain unchanged.*

*3. If your device software version is equal to or greater than 12.0.41, and the **Software update license** is within the valid period, you will be able to upgrade. After the upgrade, you will get a free **Device License, Multi-function License** and **Endpoint Security License (if you are using 13.0.8 have purchased an official Endpoint Security License)**for up to **5 years** from the date of product activation. For example, if you purchased a device on January 1, 2020, but you upgraded to version 13.0.15 on January 1, 2021, the expiration time of the **Device License** and **Multi-function License** will change to January 1, 2025 after the upgrade. The license status and expiration time of the remaining modules remain unchanged.*

*4. Please note that in IAG 13.0.15 version, we have brought a brand new **Endopoint Security** feature, which requires a separate purchase license to use. However, we will give each customer participating in the Beta process a **30-days trial license for free**. You can contact our technical support or your local SANGFOR office to obtain a trial license after the upgrade is completed, and experience the new features. We look forward to your feedback!*

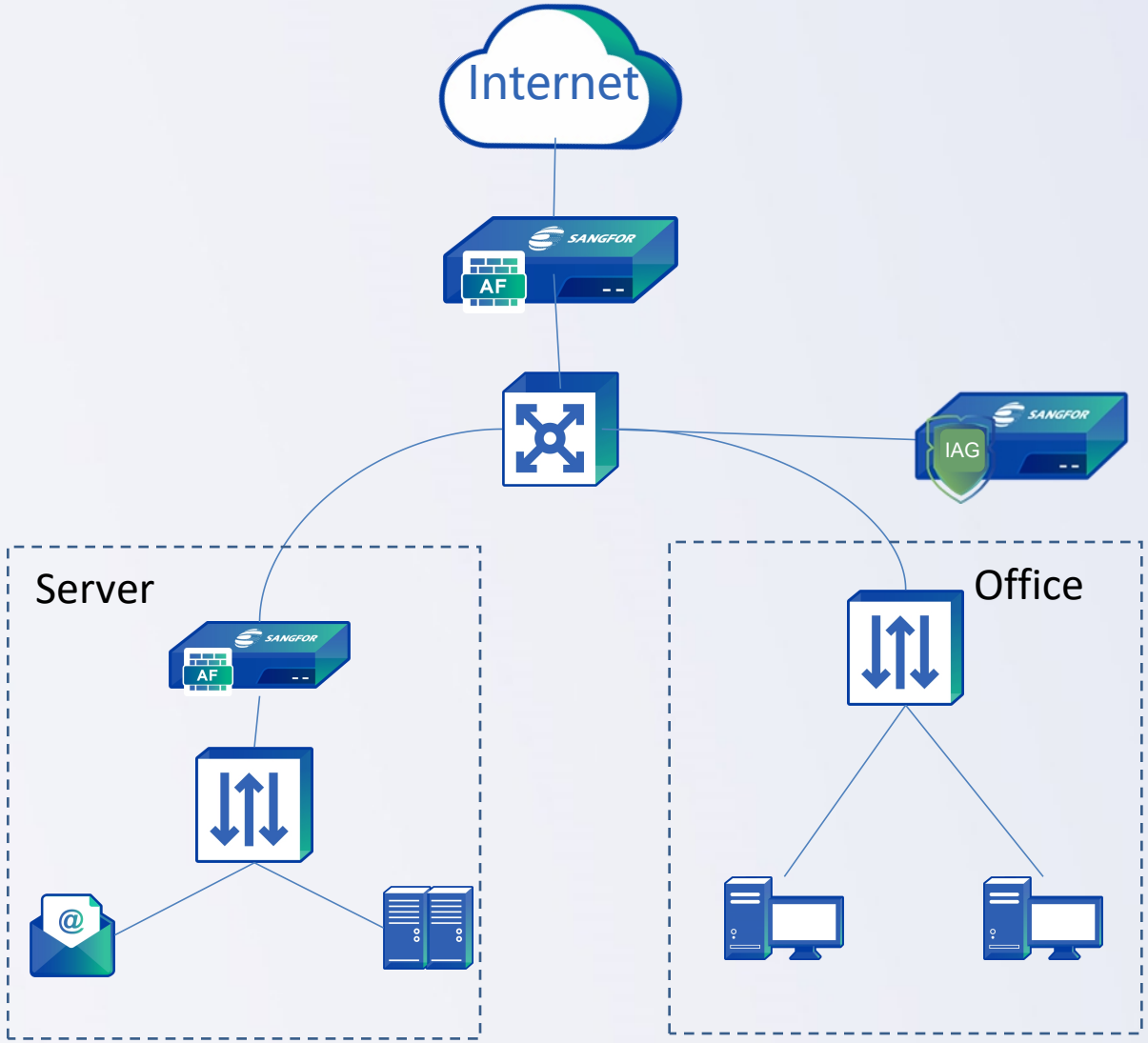
3.Asset Management Test Example

Background: Asset identification is not related to IAG deployment mode, as long as the traffic can reach the IAG, it can be bridged, routed, and mirrored.

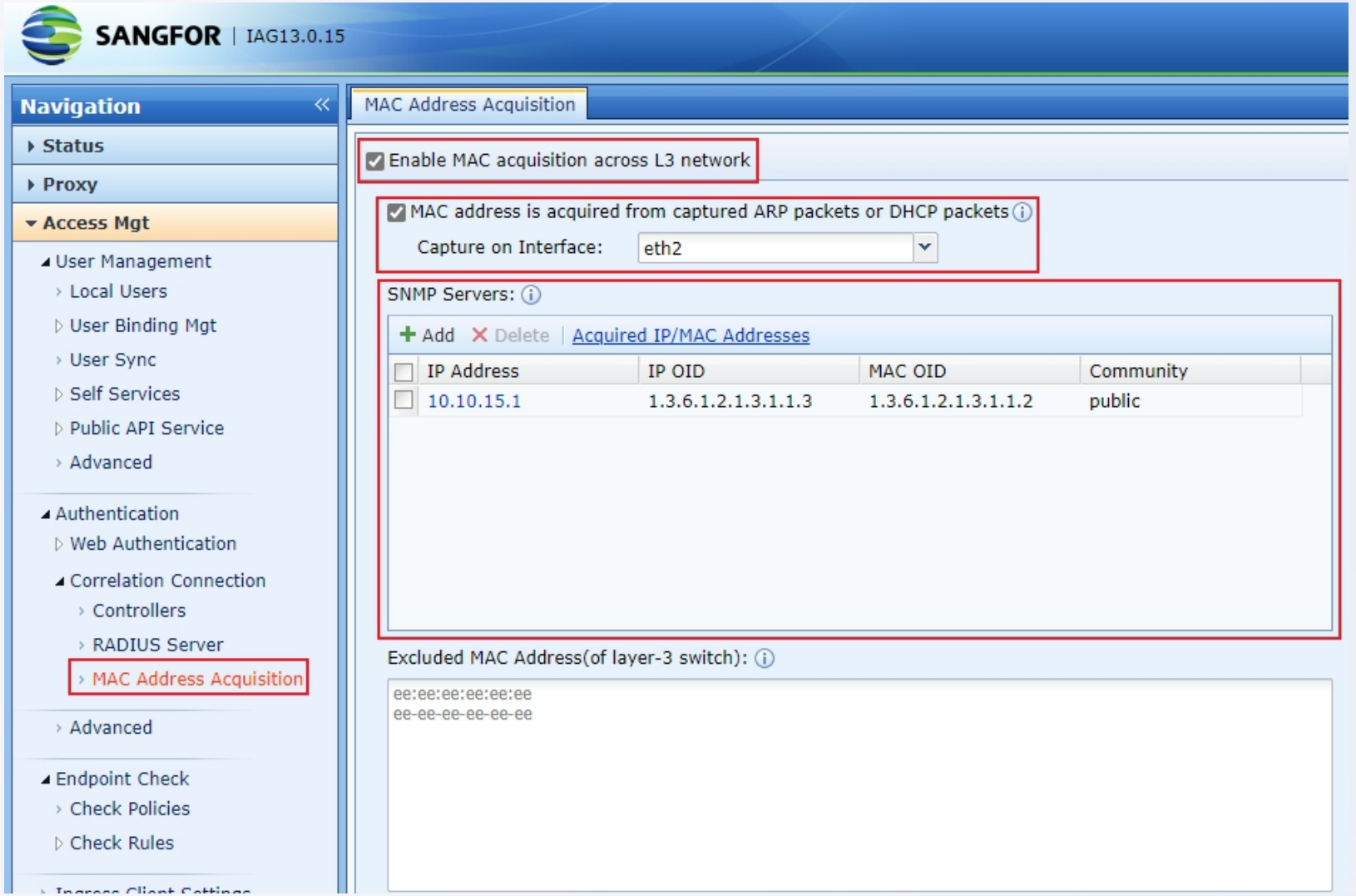
The picture on the right is an example of mirroring: mirror the tcp/dhcp traffic of the switch to the IAG, and the IAG will identify it based on the characteristics of the traffic.

Test PC: windows PC, MAC PC

Note: If it is a cross 3-layer environment, in order to ensure a better recognition effect, please mirror the DHCP and ARP package or obtain the accurate MAC address by taking the MAC across the three-layer.

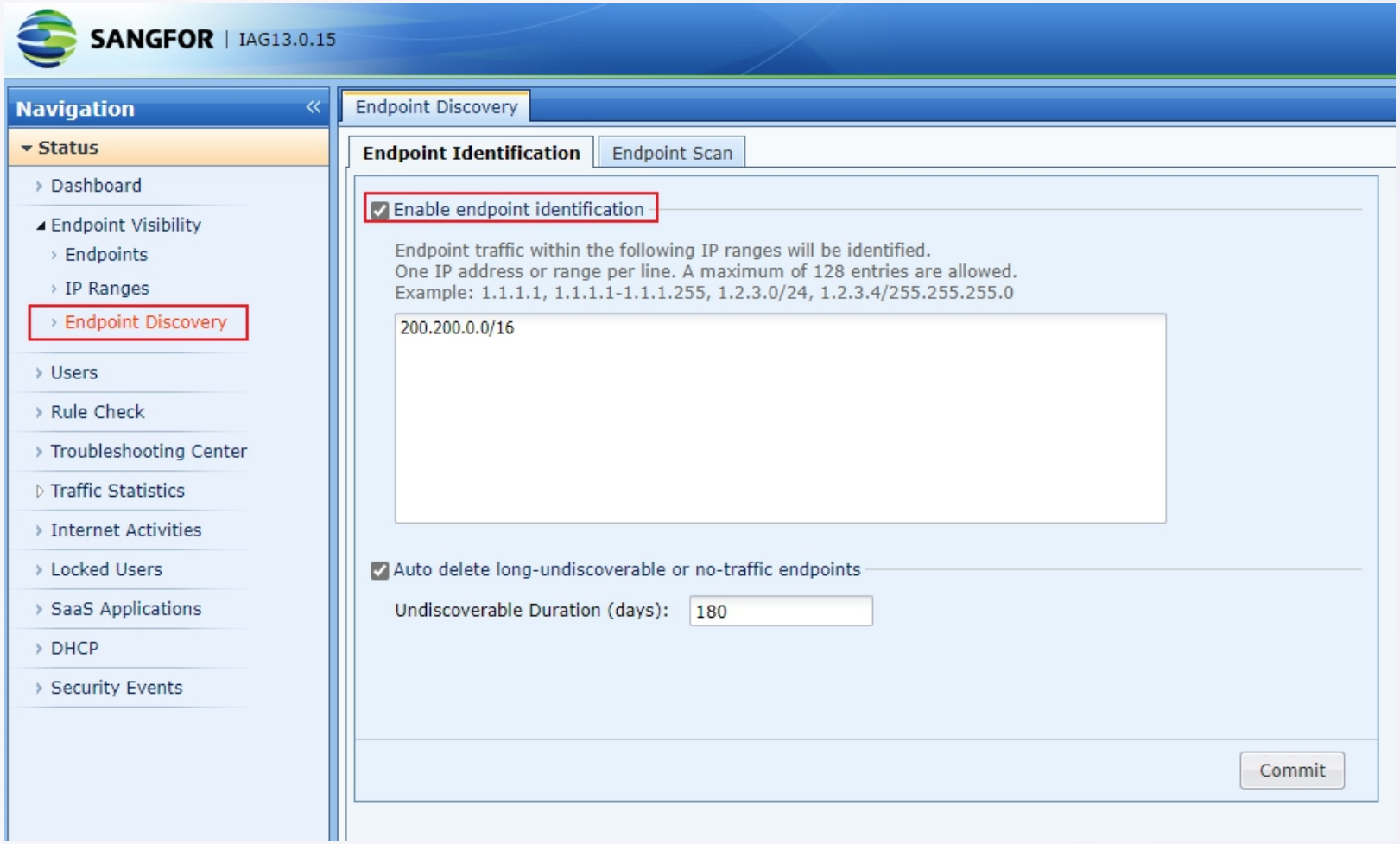


3.1 Get MAC Across Three Layers



3.2 Enable Asset Identification

Confirm that IAG turns on the Endpoint Identification function (default is off):

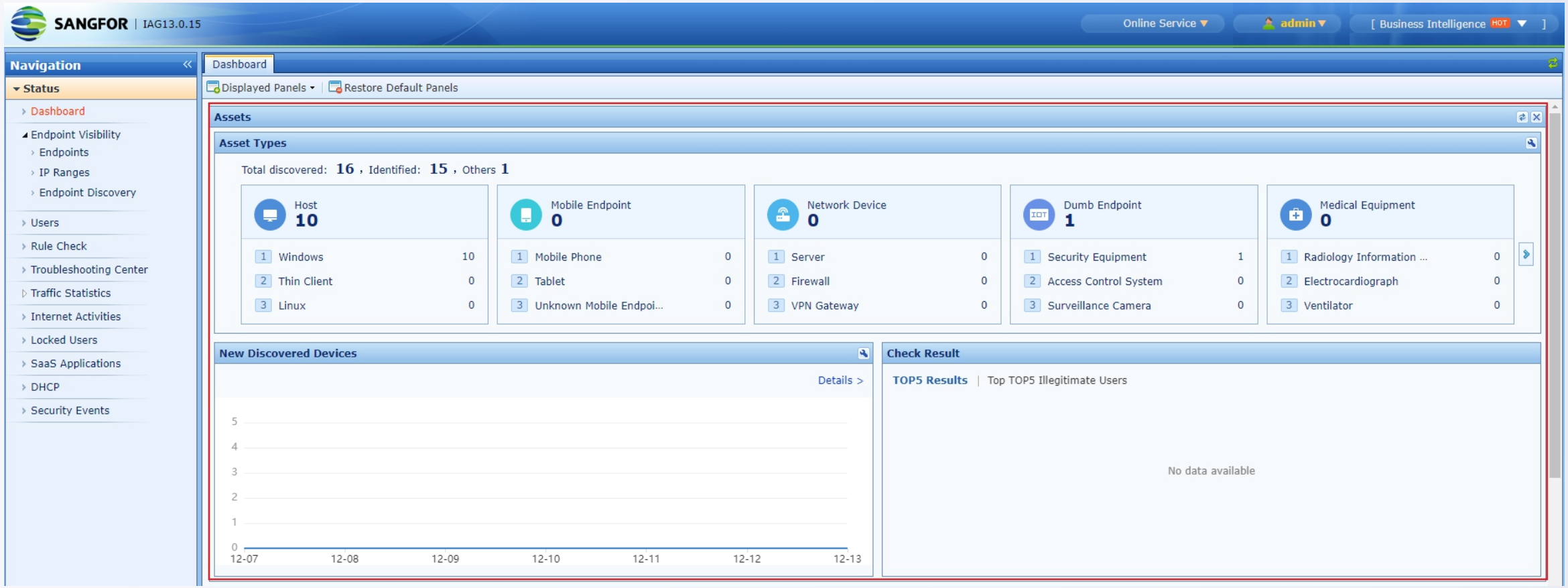


1. After enabling the Endpoint Identification function of the entire network, you need to configure the range of the IP segment you want to identify, and the traffic of the Endpoints in this network segment needs to be able to reach the IAG.

2. If it is a bypass deployment, you can click Auto Obtain, and the bypass monitoring network segment address will be automatically filled in.

3.3 View the Effects of Asset Identification

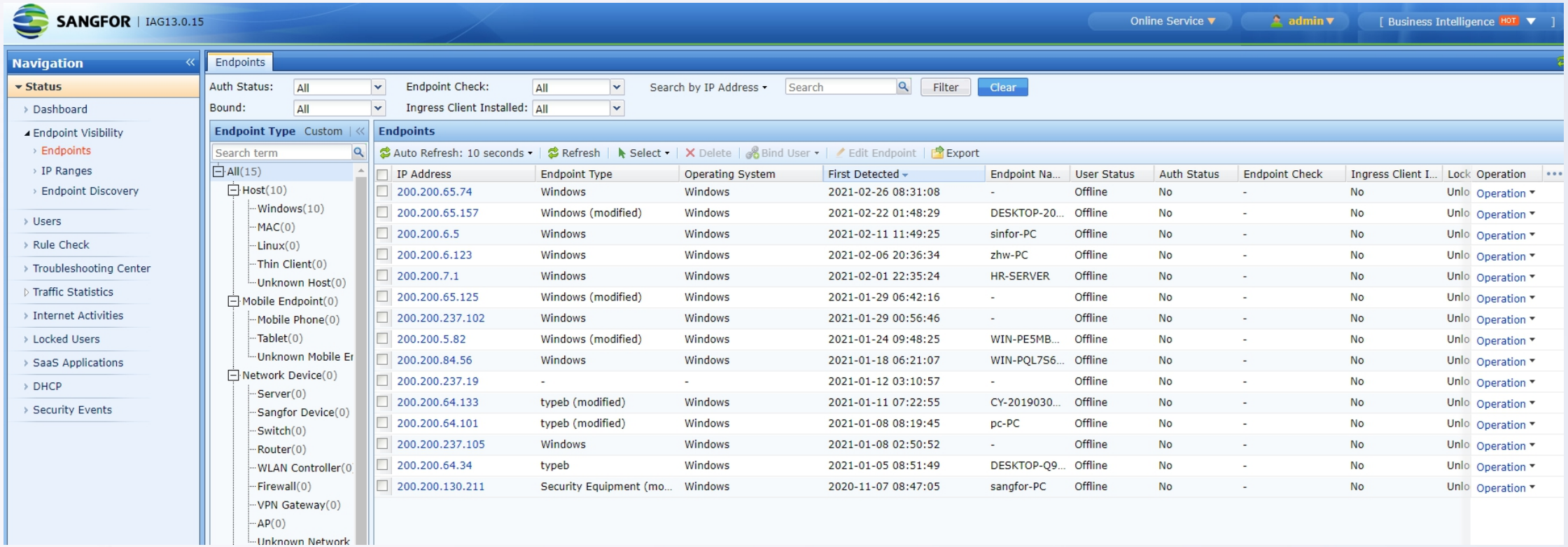
Go to the homepage to view the overall asset profile:



Display asset status from multiple dimensions, including asset distribution, newly discovered trends, and compliance violations.

3.4 Viewing the Effects of Asset Identification

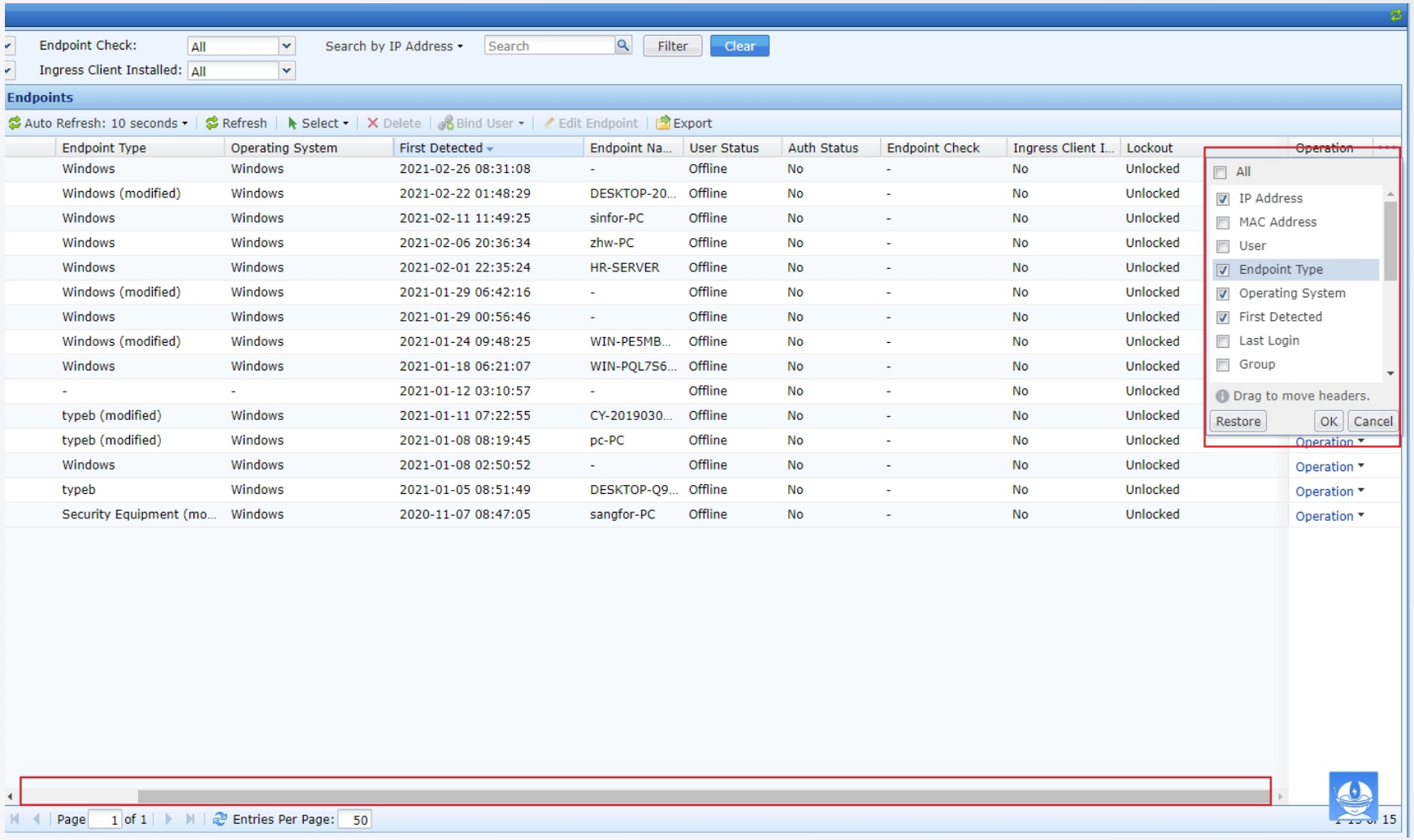
View all identified asset information in the asset list:



The endpoint list page displays all the Endpoints currently identified, and clusters are made according to the Endpoint type. Click the corresponding Endpoint type to filter out the corresponding Endpoint.

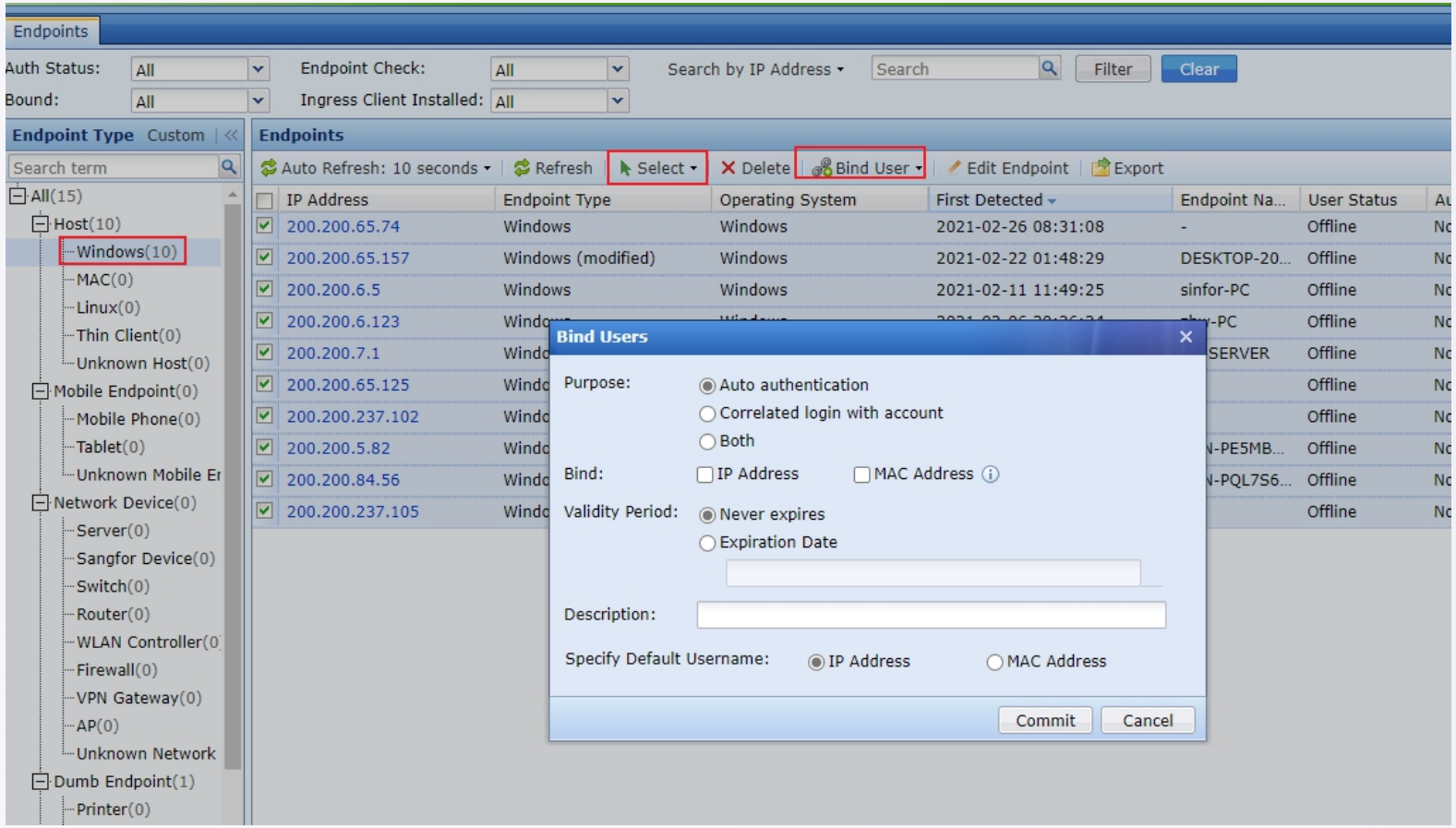
3.5 Viewing the Effects of Asset Identification

Customize the display column content: Click on the node shown in the figure below to display the complete column content. You can customize which columns to display according to the degree of interest, and drag up and down to adjust the display order. If you want to display all, a scroll bar will be displayed below To fully display all column contents.



3.6 Fast Batch Approval Access

In the Endpoint list, filter out the Endpoints that you want to release quickly (such as dumb Endpoints, PCs trusted by the intranet, etc.), and then add user bindings in batches, and add the Endpoints to authentication-free.

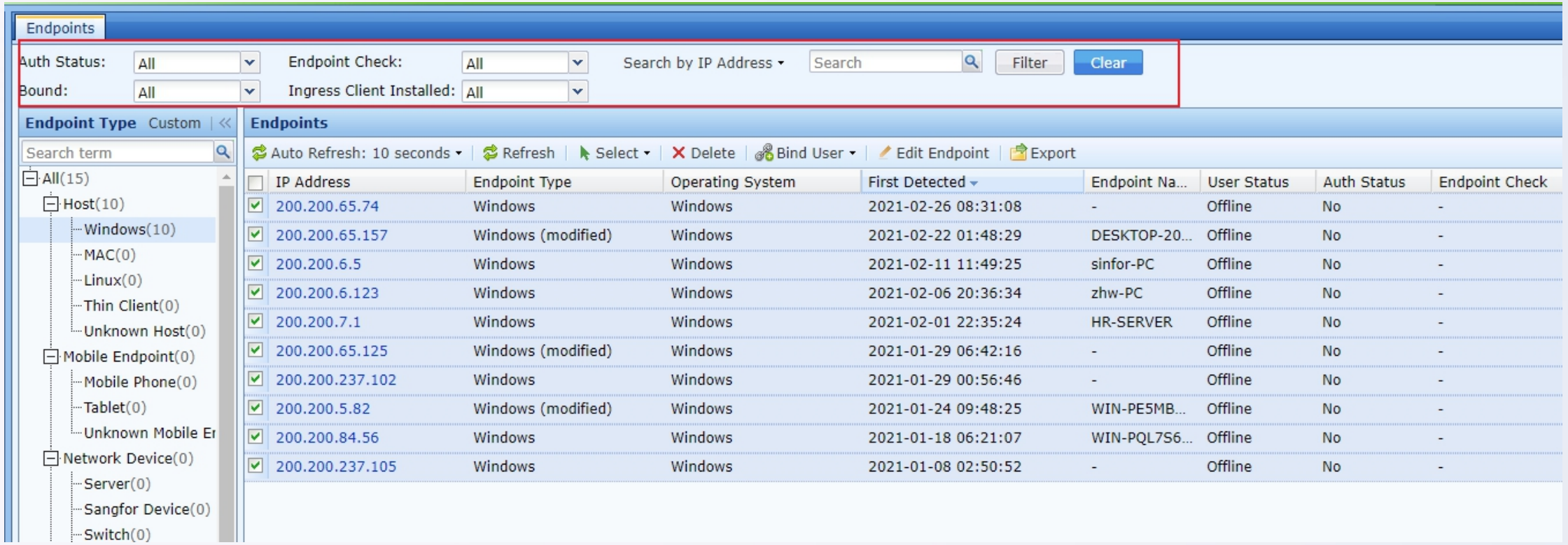


The picture on the left takes Windows PC as an example:
Filter out Windows PC according to the Endpoint type organization structure, then select the Endpoints that you want to release in batches, and add authentication-free, you can quickly complete the effect of rapid release according to the Endpoint type.

Remarks: similar to dumb Endpoints, filter out dumb Endpoints and add them in batches without authentication.

3.7 Fast Batch Approval Access

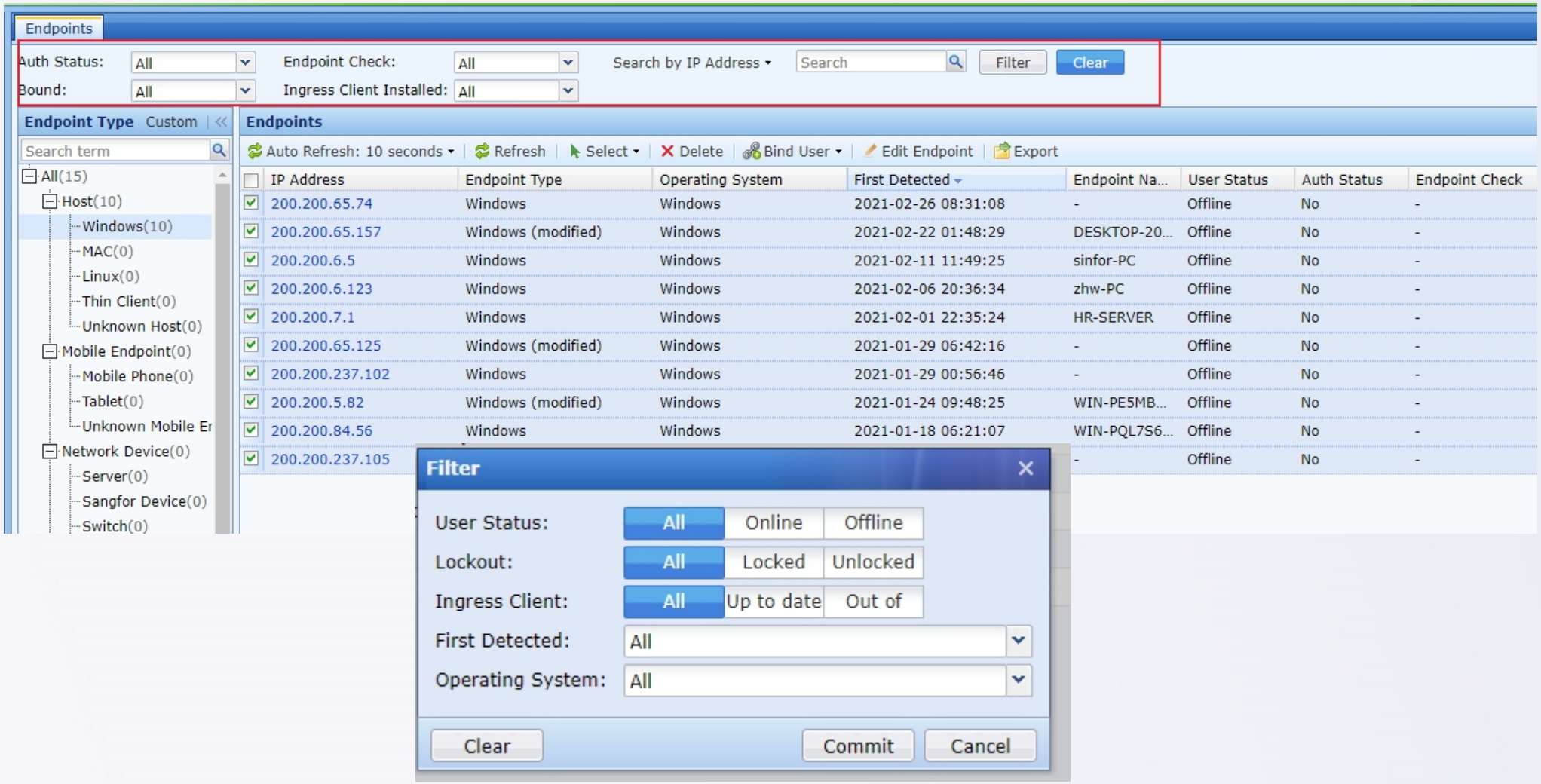
In the Endpoint list, filter out the Endpoints that you want to release quickly (such as dumb Endpoints, PCs trusted by the intranet, etc.), and then add user bindings in batches, and add the Endpoints to authentication-free.



You can also filter out the desired Endpoint according to the first access time, IP segment, user, etc. in the filter conditions, and add authentication-free.

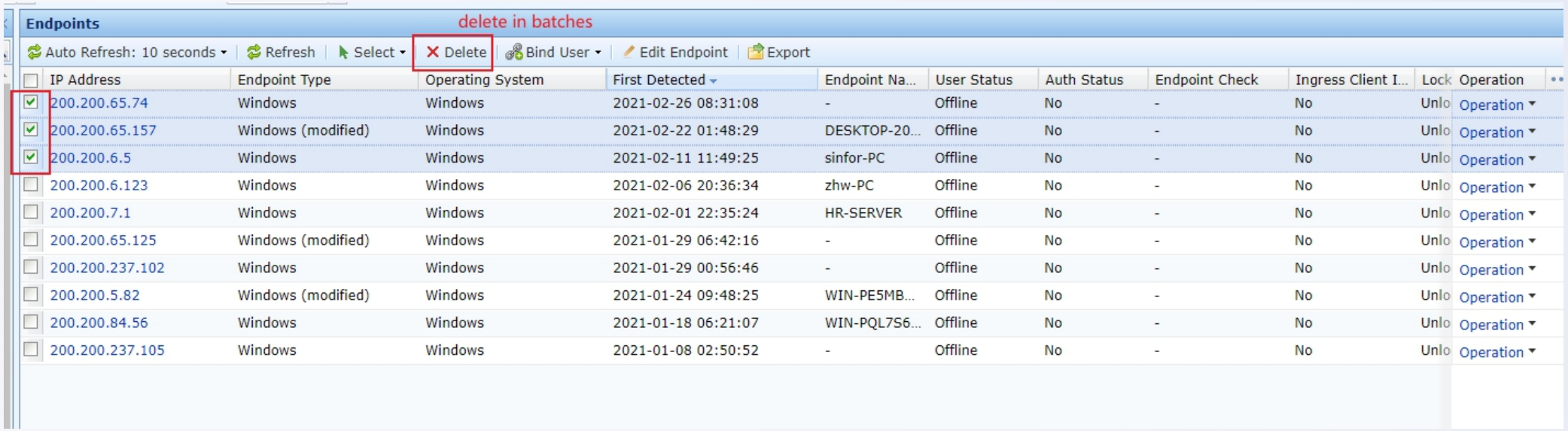
3.8 Asset Management - Search

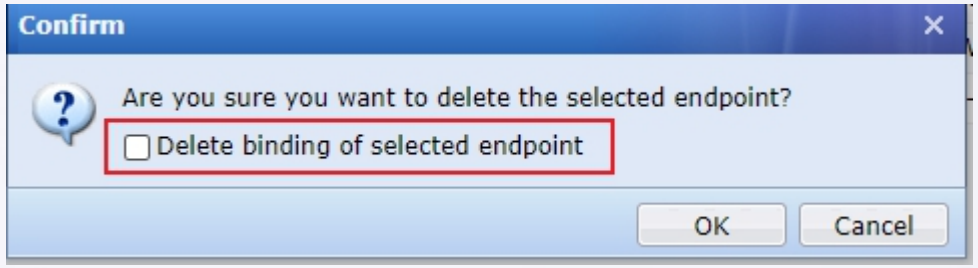
In the asset list, quickly filter out asset information based on asset status (such as viewing which Endpoints are not compliant). If you need to filter more (filter out win7), click More to delete:

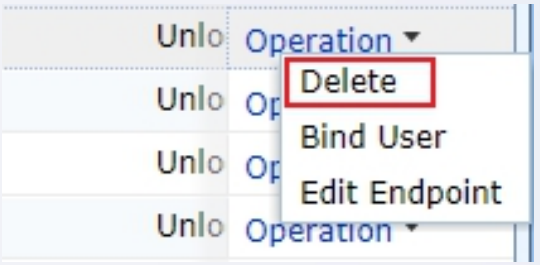


3.9 Asset Management - Delete

In the asset list, you can delete assets that have not been discovered for a long time. When deleting, it will synchronously check whether to delete the binding relationship:



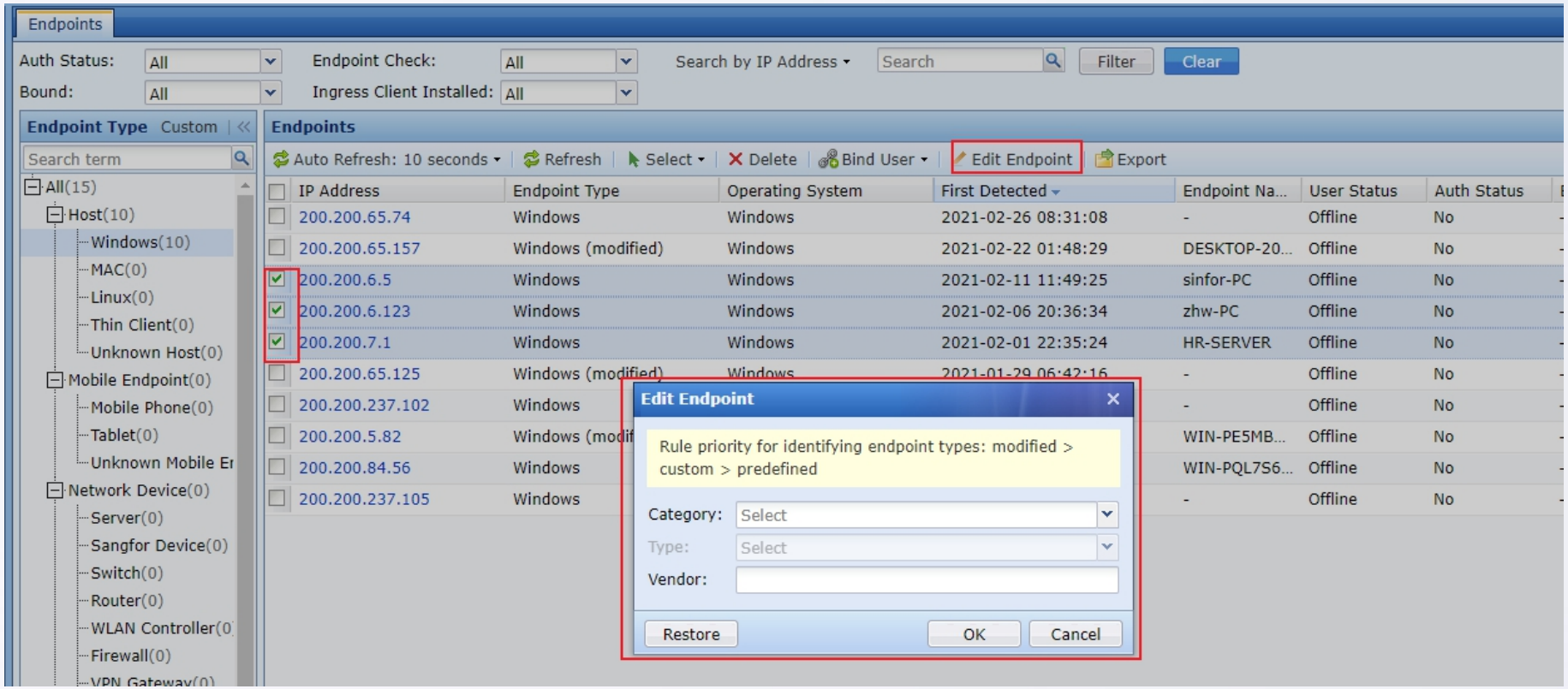




Delete single Endpoint

3.10 Asset management - Change

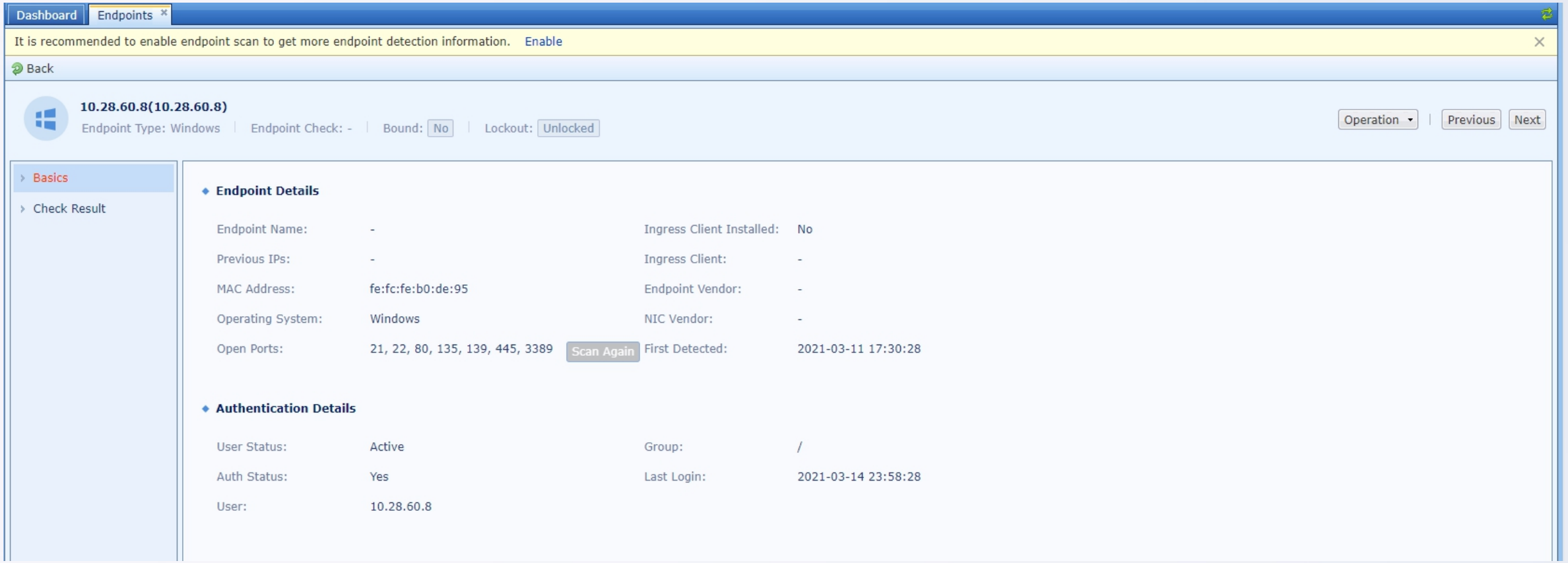
In the asset list, you can directly modify the Endpoint with a clear Endpoint type identification error, and also support batch modification:



Edit single Endpoint

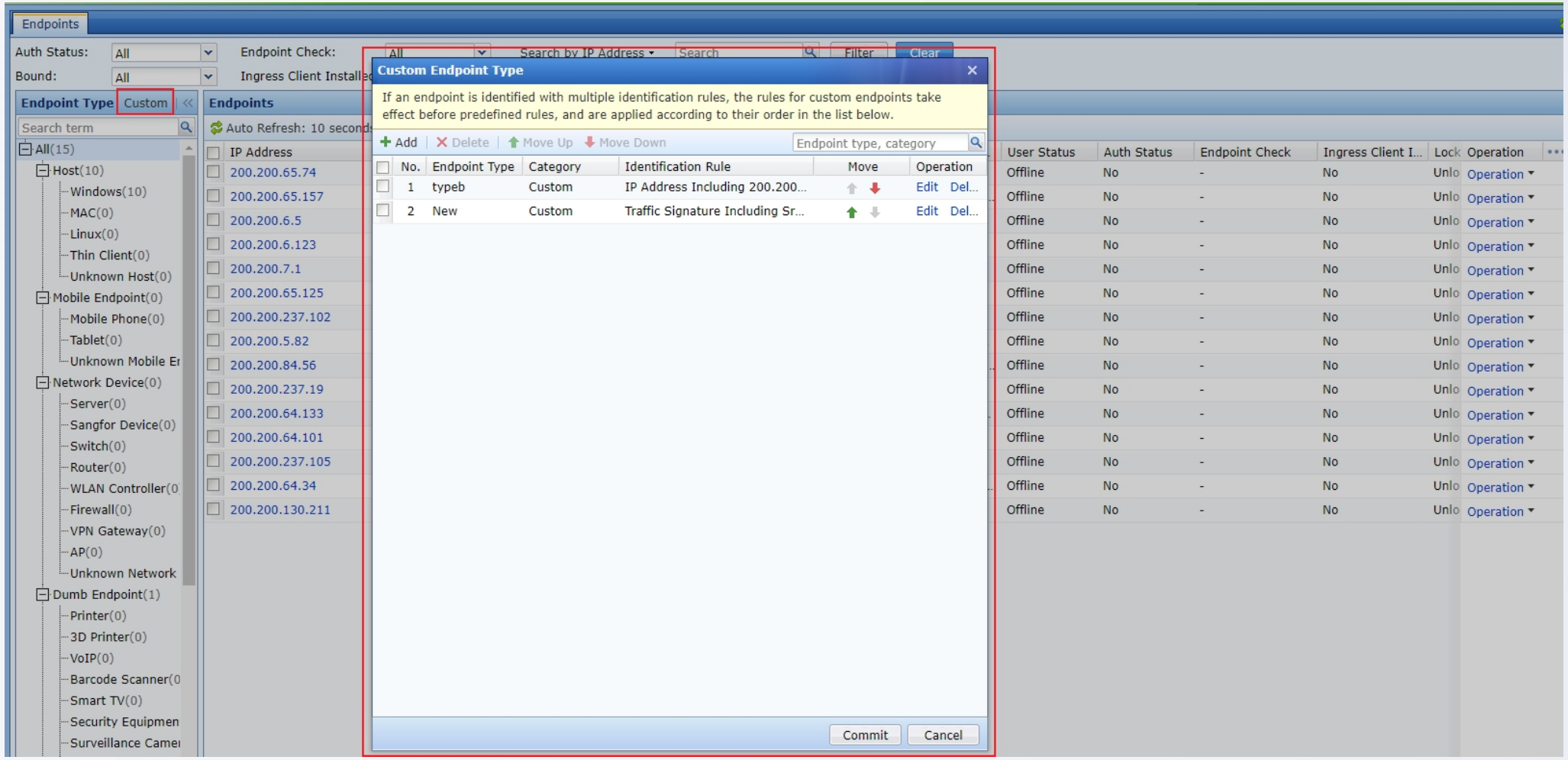
3.11 Asset Management - View Details

To view asset details, click on the IP address to open the asset details page, first view the basic information, as shown below:



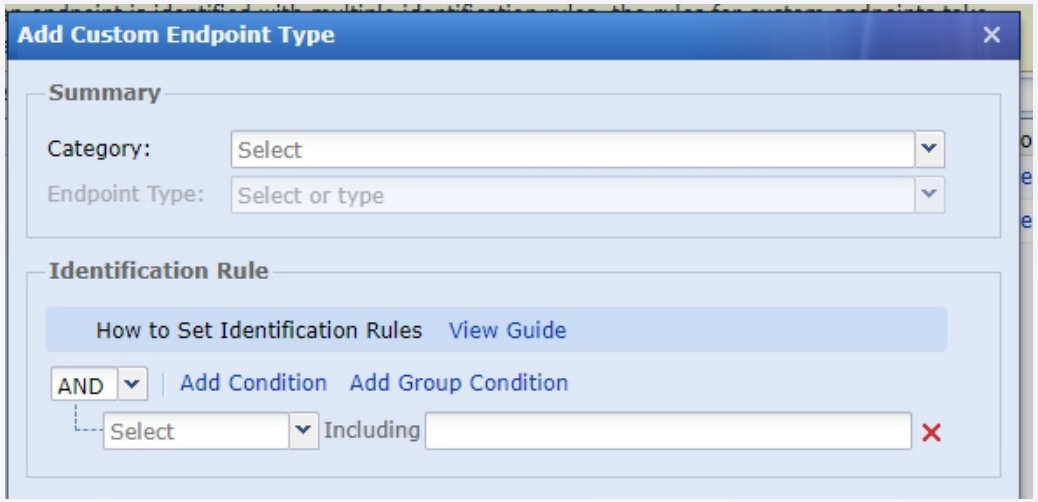
3.12 Asset Management - Custom Endpoint Type

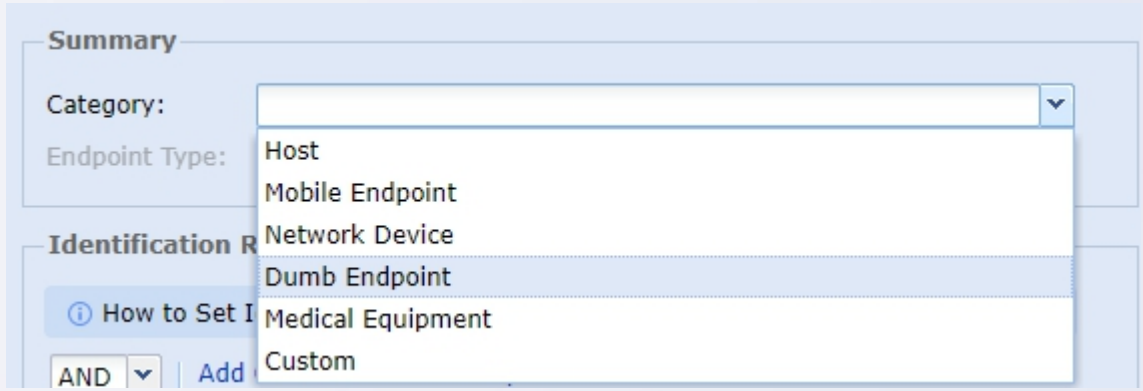
For unrecognized Endpoints or Endpoints with incorrect recognition, the Endpoint type can be customized according to the characteristics, and the Endpoint characteristics are matched according to the priority from top to bottom. If it matches, the Endpoint type of the Endpoint will be set according to the custom Endpoint type. In the left tree of the Endpoint type, the corresponding Endpoint type will also be added, as shown in the figure below:

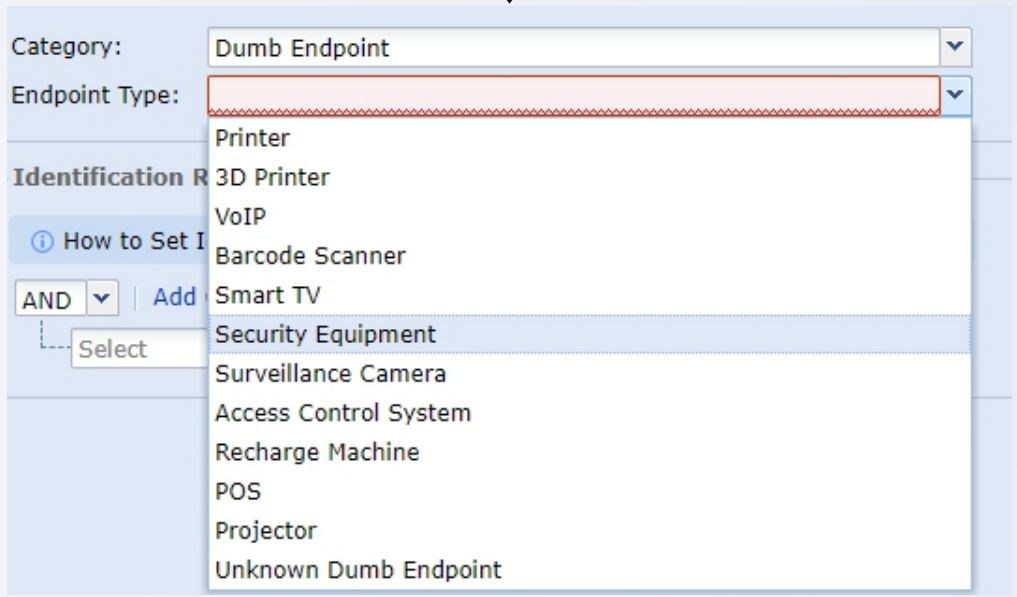


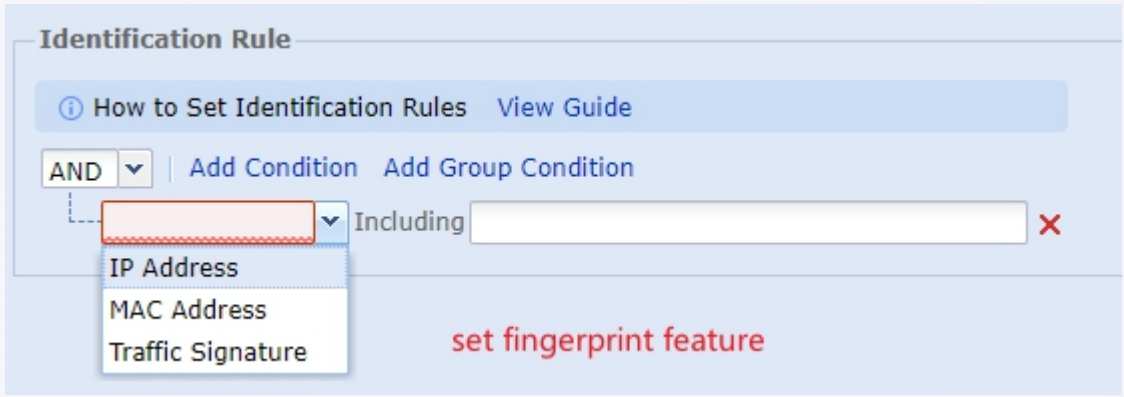
3.13 Asset Management - Custom Endpoint Type

Add a custom Endpoint type, as shown below:







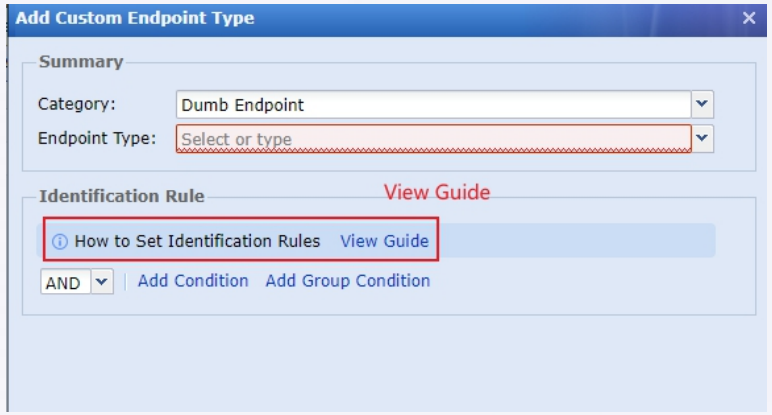


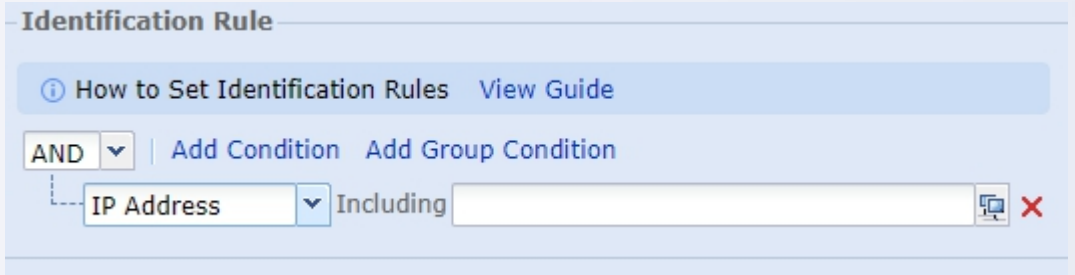
3.14 Asset Management - Custom Endpoint Type

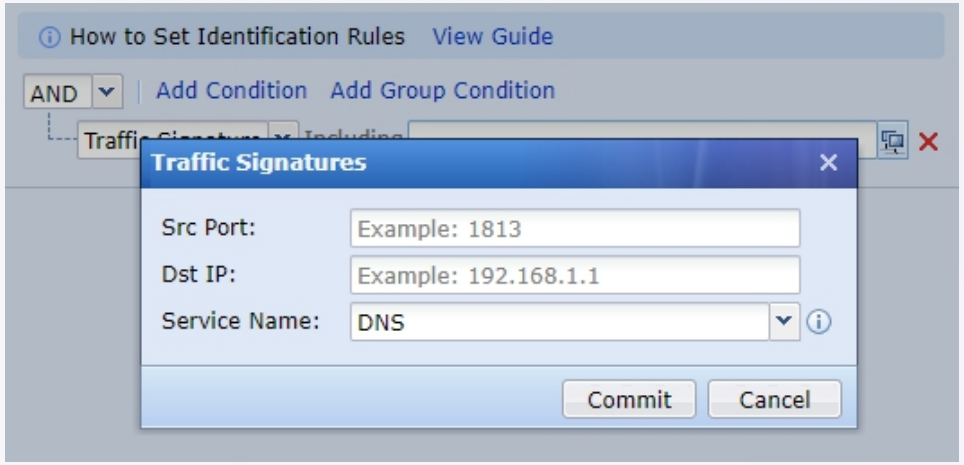
Set fingerprint features, as shown below:

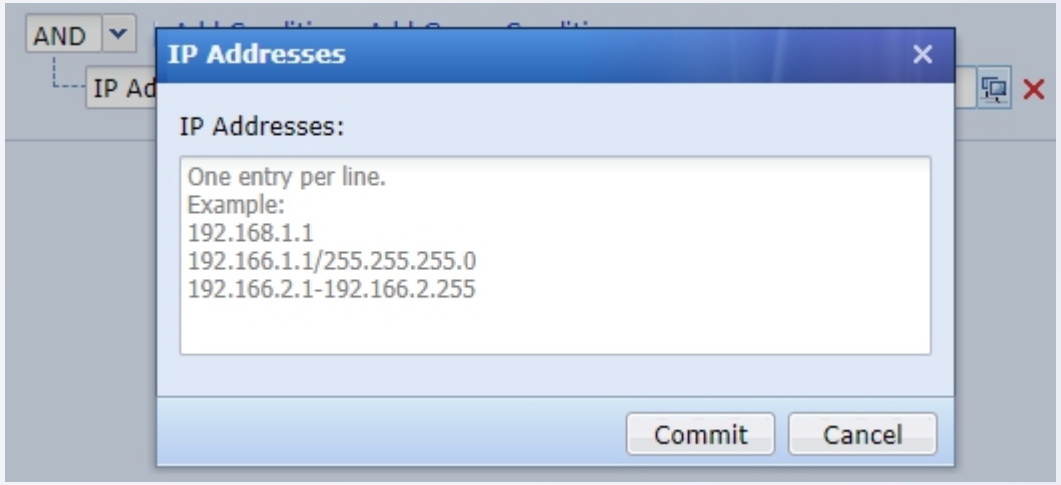
Example 1: The company newly purchased a batch of cameras. The first six digits of the MAC address have the characteristics of a fixed manufacturer. Select the MAC address in the conditions and fill in the first six digits of the mac address.

Example 2: The company uses Sangfor's virtual PC, the communication protocol is encrypted, and the recognition effect is not good according to the built-in library, but the data communicated with the fixed server has a fixed protocol. Select the flow characteristics in the conditions, and the target IP selects the server address and service name. Select the communication protocol between the virtual PC and the fixed server.



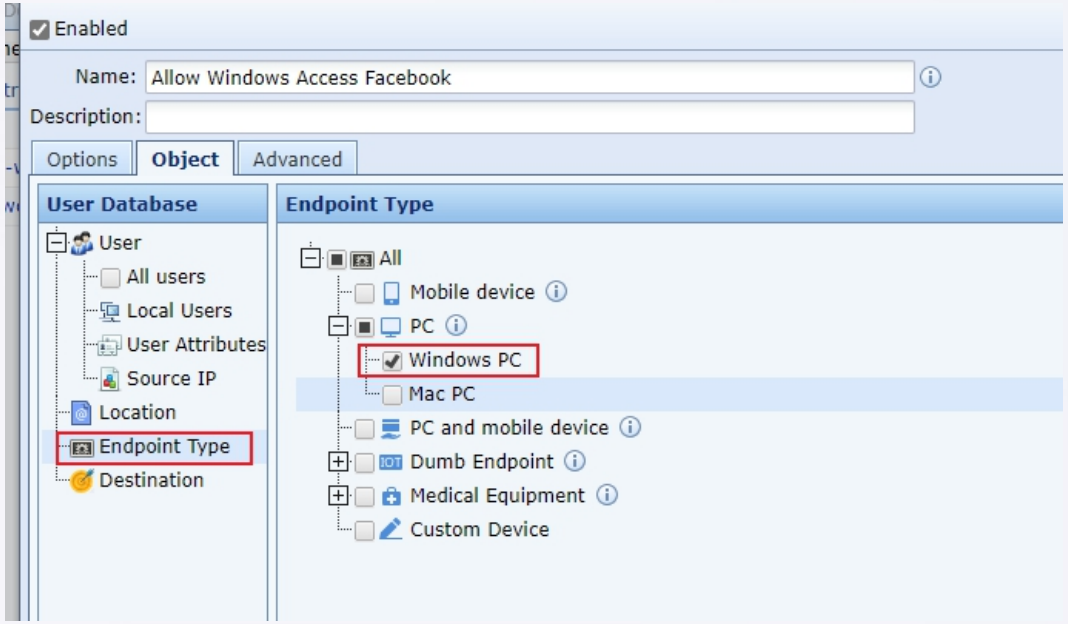


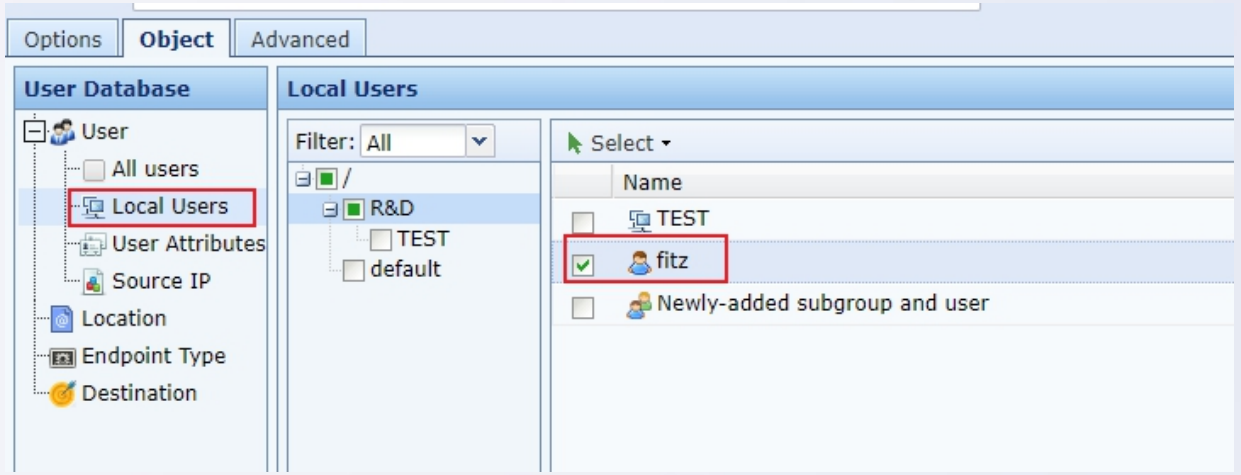


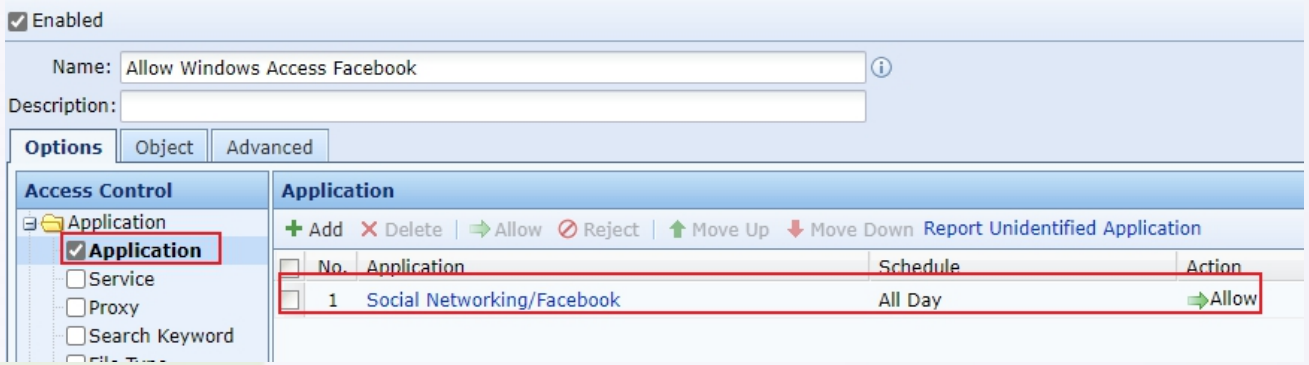


3.15 Configuring Control Strategy according to Endpoint Type

Configure the comparison of two new strategies in the access permission policy, and the applicable object is set to test PC. Here, two Endpoints of different Endpoint types are used to check the control effect. First, create a new policy that allows windowsPC to access the website, and the applicable object is test windowsPC.



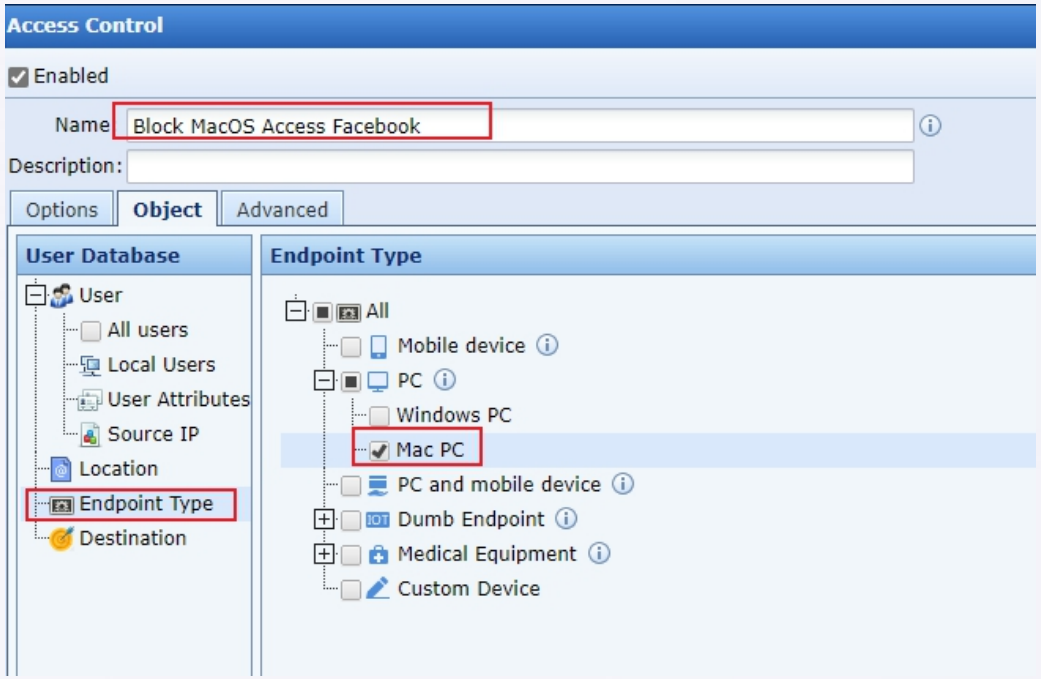


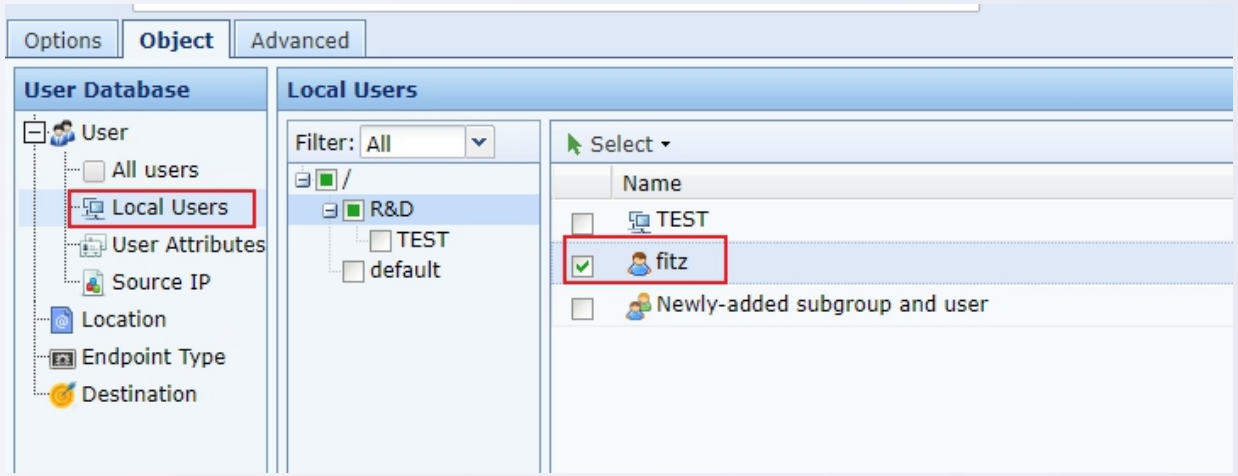


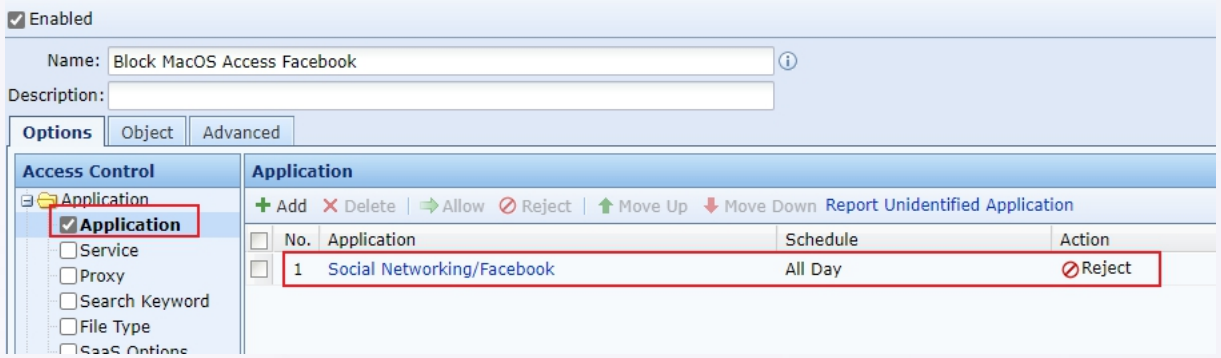
1. Allow access to Facebook in application control
2. Applicable users choose new test users
3. Choose WindowsPC as the Endpoint type

3.16 Configuring Control Strategy According to Endpoint Type

Create a new MAC PC deny access to the website policy, applicable to test MAC PC.







1. Block access to the Facebook application control
2. The user selects a new test user
3. Choose MAC PC for Endpoint type

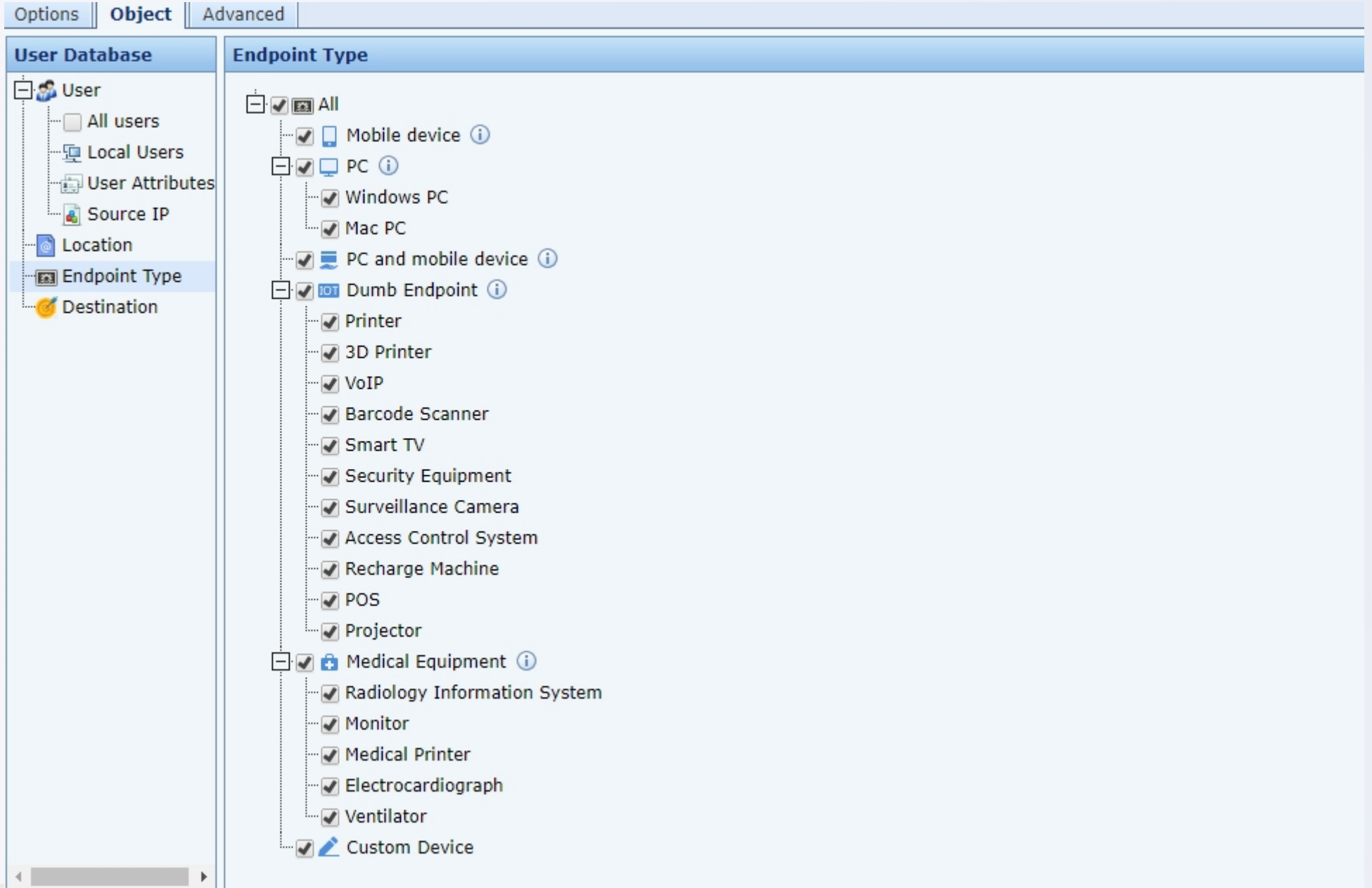
3.17 View Control Effects

Connect the test windowsPC and MacOS to the network and use the user name "Fitz" for authentication. After the authentication is successful, after the Endpoint types of these two Endpoints are displayed in the online users,

Use Mac PC to access "https://facebook.com" can not be accessed normally, other applications can be tried normally

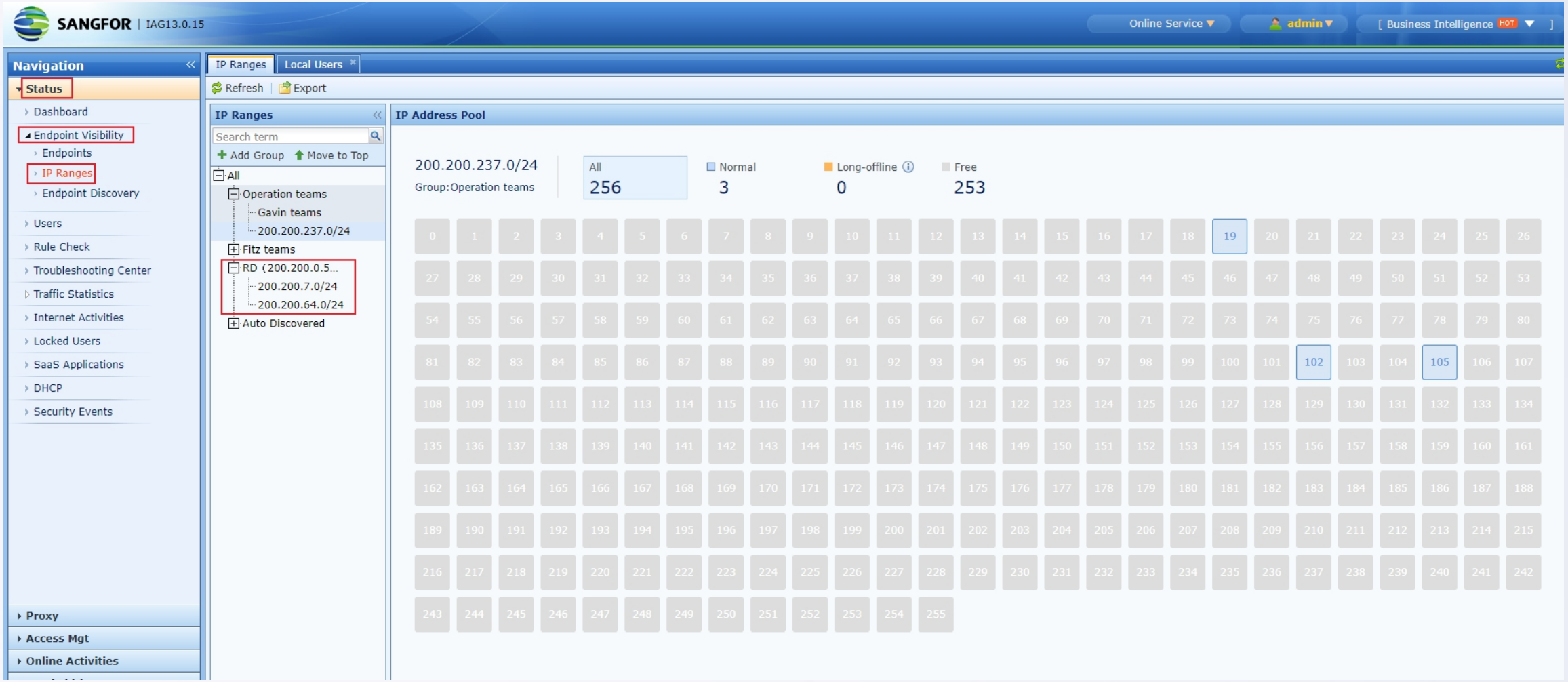
Use Windows PC to access "https://facebook.com", it can be accessed normally, and other applications can be tried normally

3.18 Endpoint Types Supported by IAG



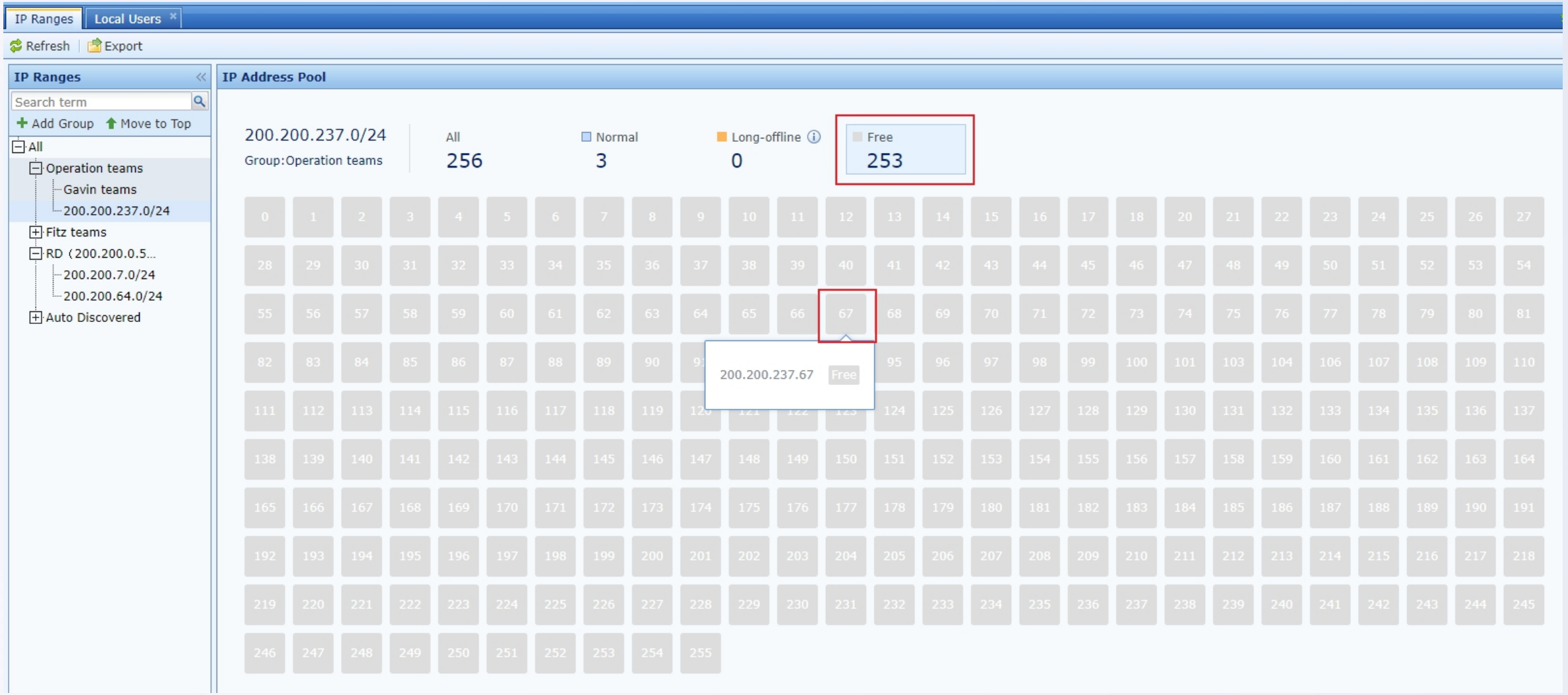
3.19 IP Management - Group Management

IP address management, you can classify IP information, for example, the R&D department has 2 C categories, which can be aggregated and displayed under one IP group.



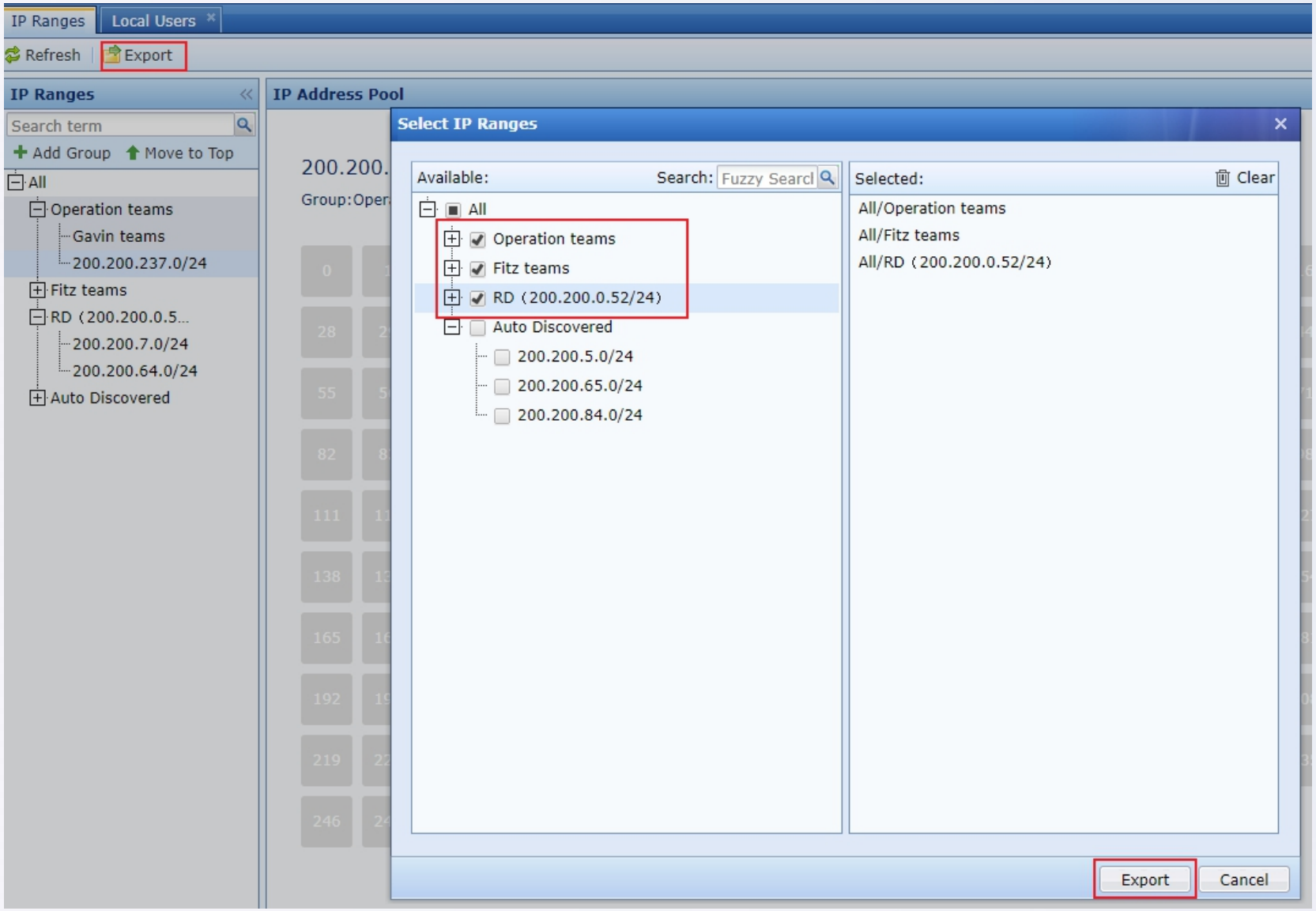
3.20 IP Management - Filtering

IP address management, quickly filter IP segments, check unused IPs, and assign them offline to Endpoints in need.



3.21 IP Management - Export

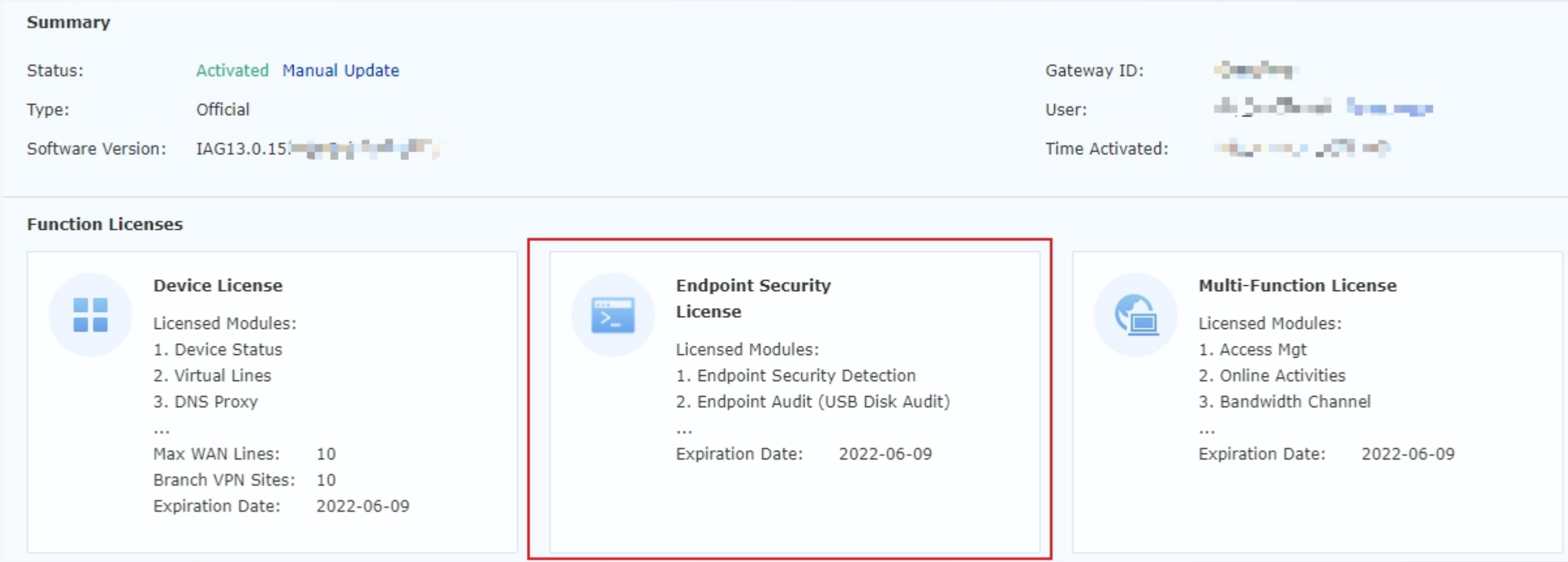
IP address management, export IP address segments.



4. Endpoint Check Feature Update

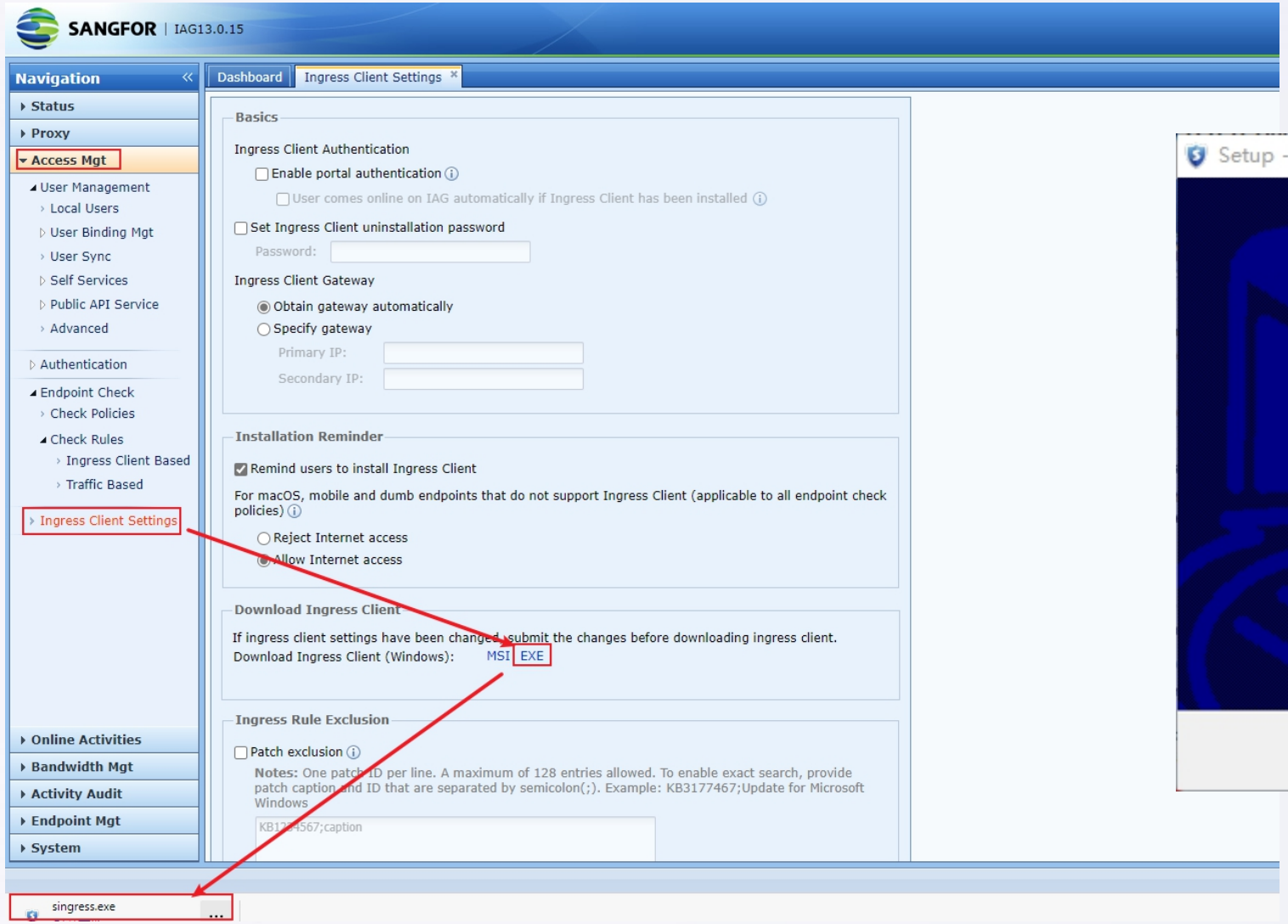
In IAG 13.0.15, we provide a new Endpoint check feature, you can experience it according to the following guidelines.

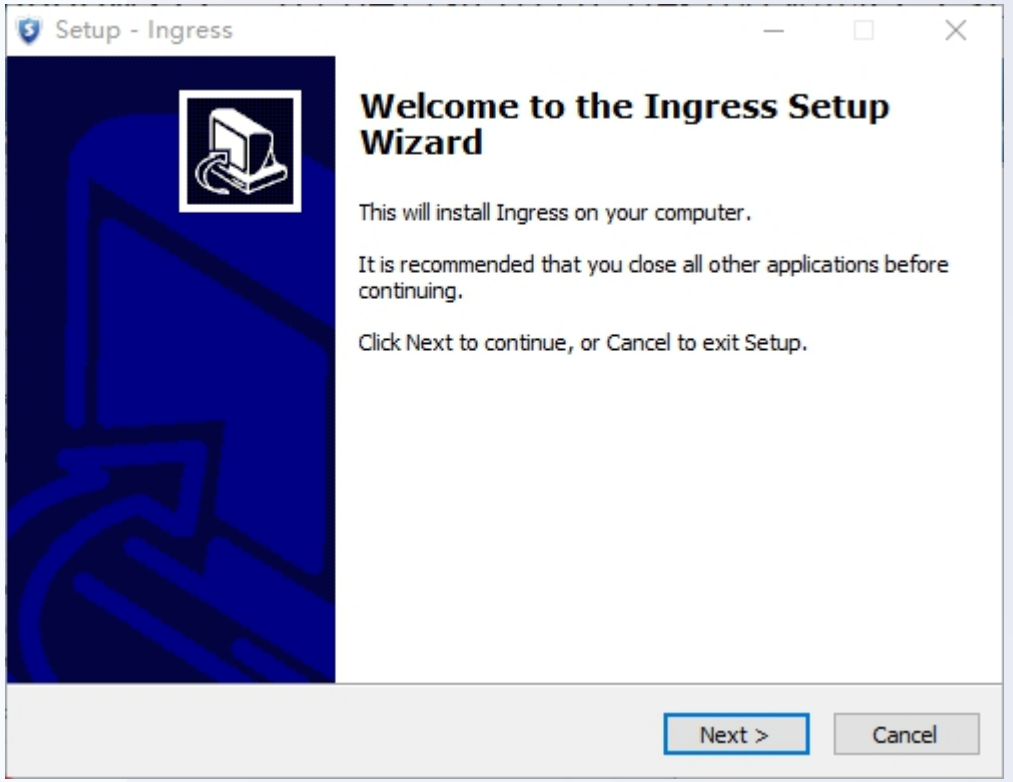
First of all, you need to ensure that your Endpoint Security License is within the validity period. If you are a beta user, we will provide you with a 6-month free trial License. Please contact your local Sangfor office to activate the authorization.



4.1 Endpoint Check Client Download

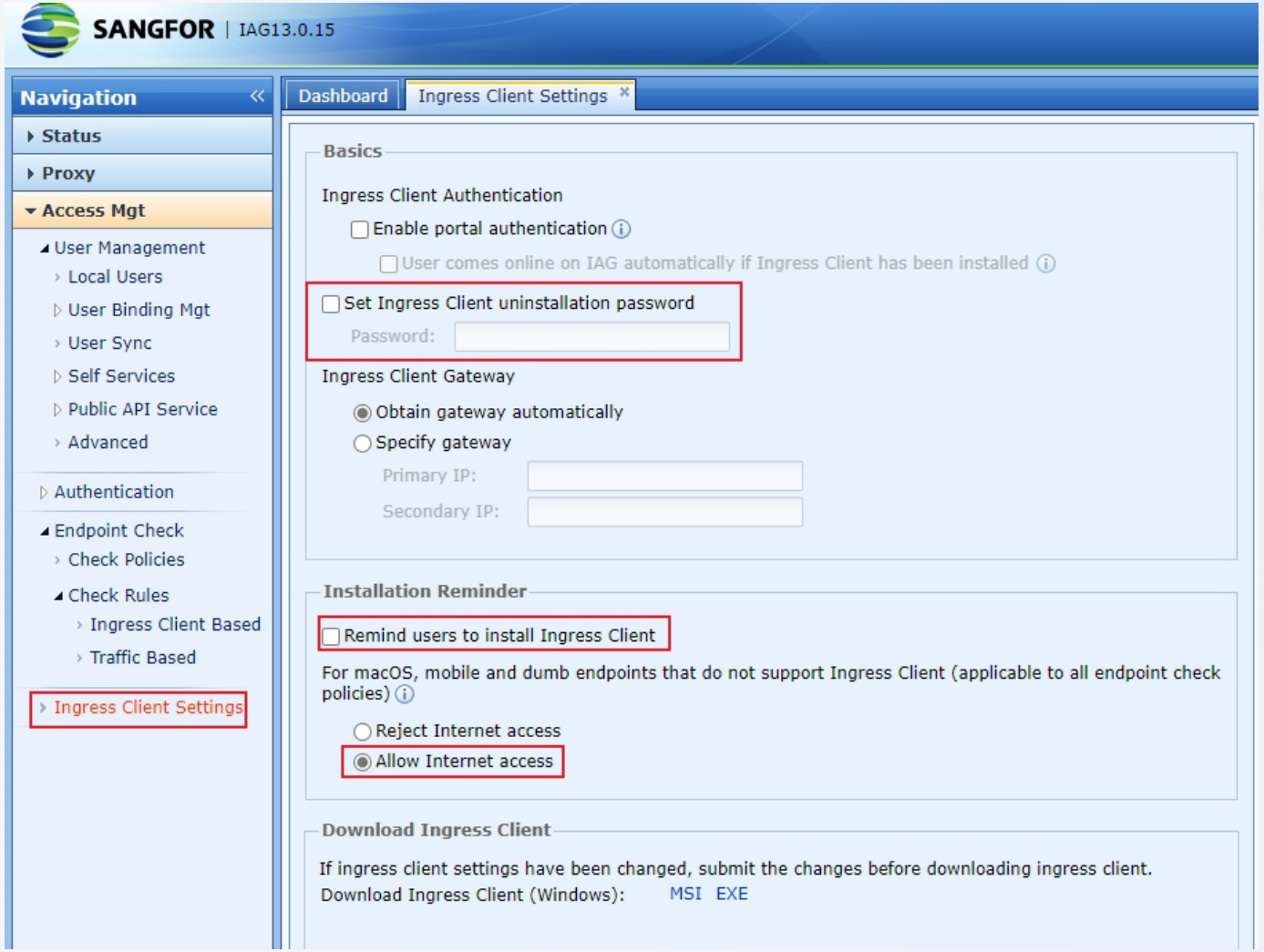
First, you need to prepare a Windows PC, download and install the ingress client on your PC through the following methods.





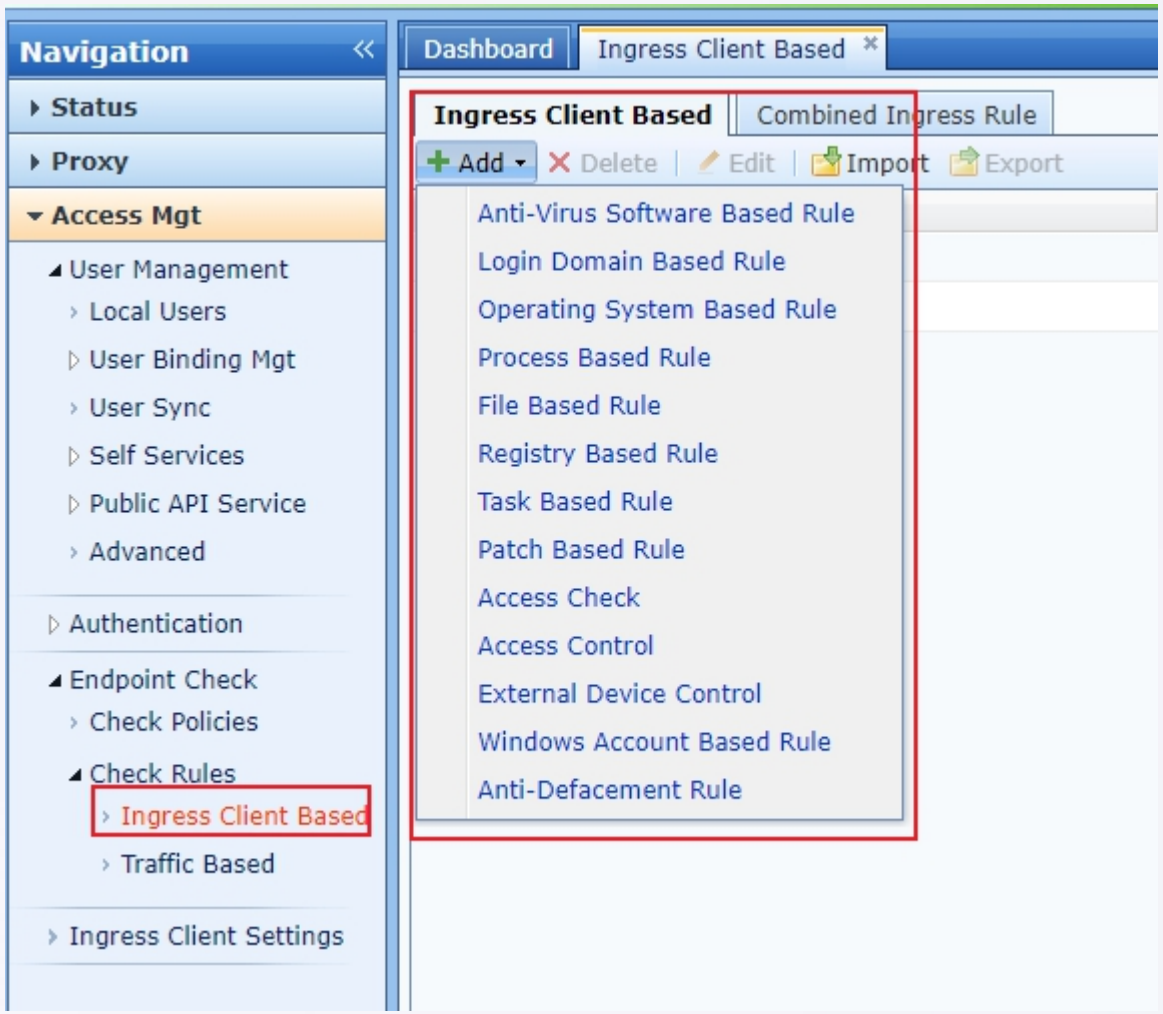
4.2 Ingress Characteristics Configuration

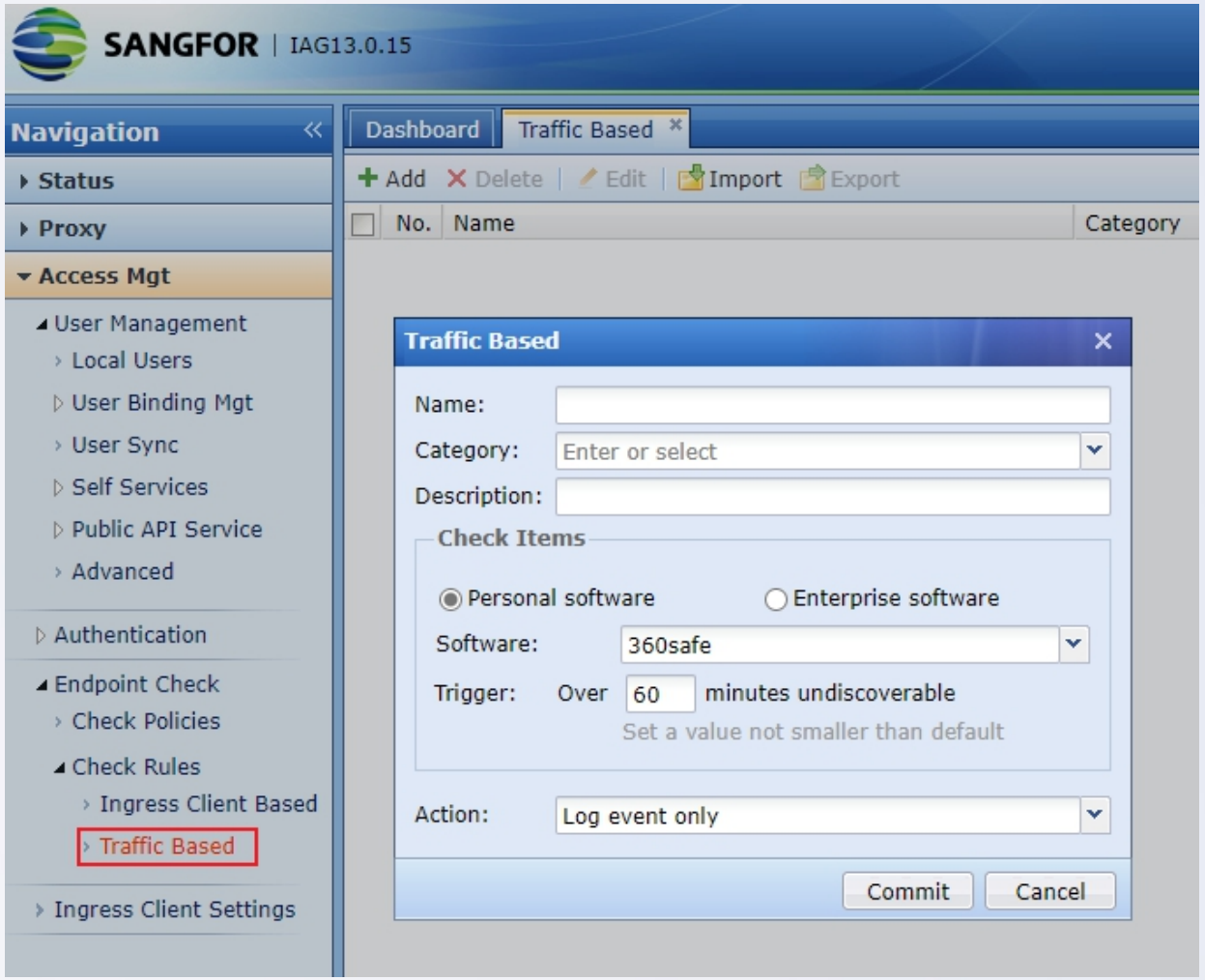
After the installation is complete, in order to avoid affecting your corporate network or test environment, we recommend that you turn off the following configuration options first.



4.3 Checking Rule Description

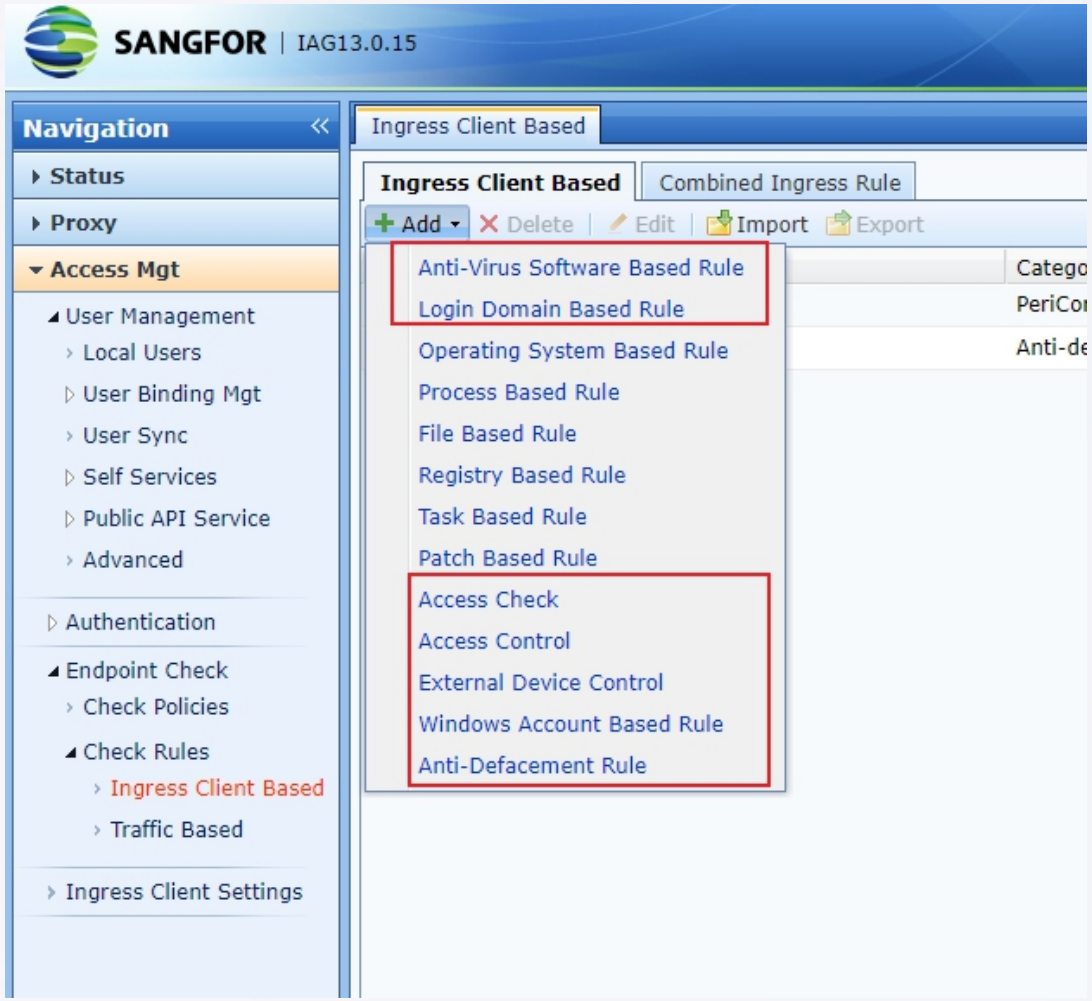
At present, we support ingress checking through two ways, one is based on client checking, the other is no-client checking.

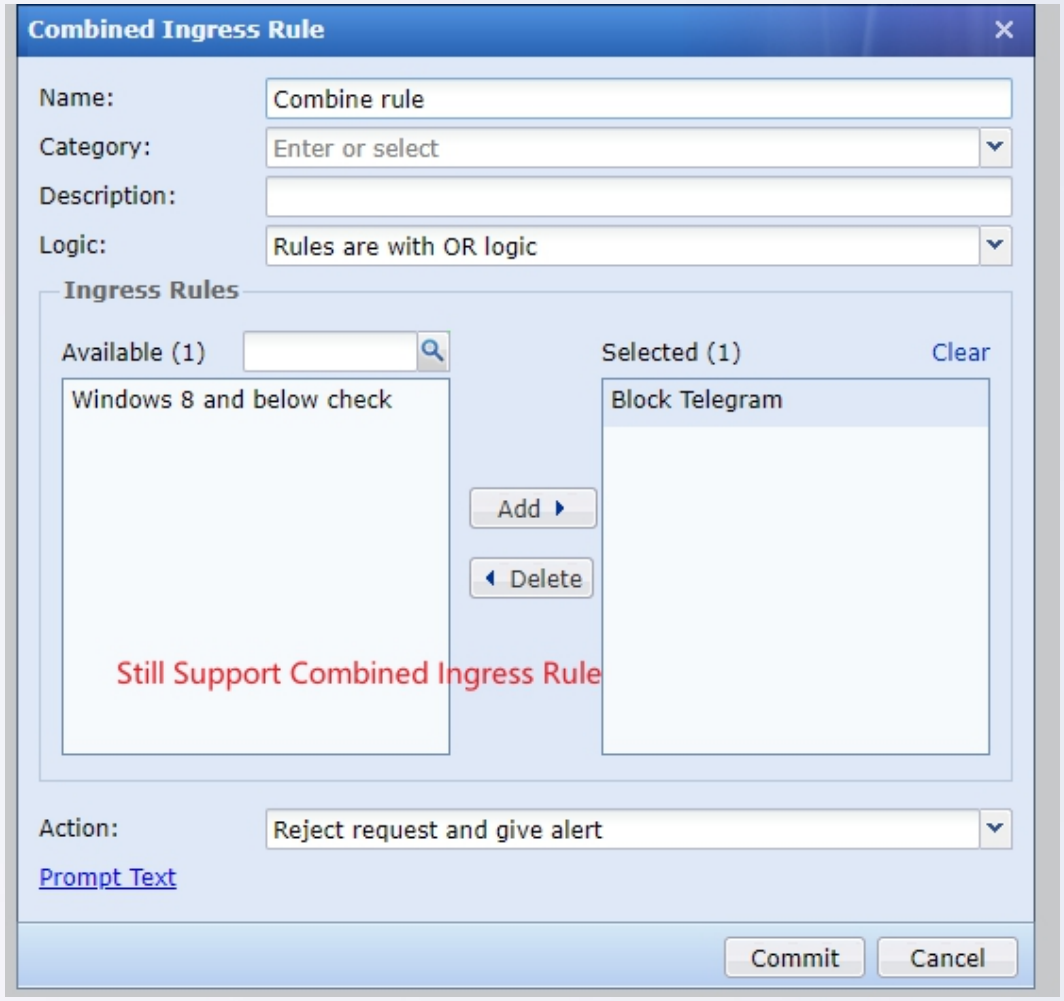




4.4 Configuration Ingress Client Checking Rules

In this update, we have added Anti-Virus Software Based Rule, Login Domain Based Rule, Access Check, Access Control, External Device Control, Windows Account Based Rule and Anti-Defacement Rule based on the original access rules.

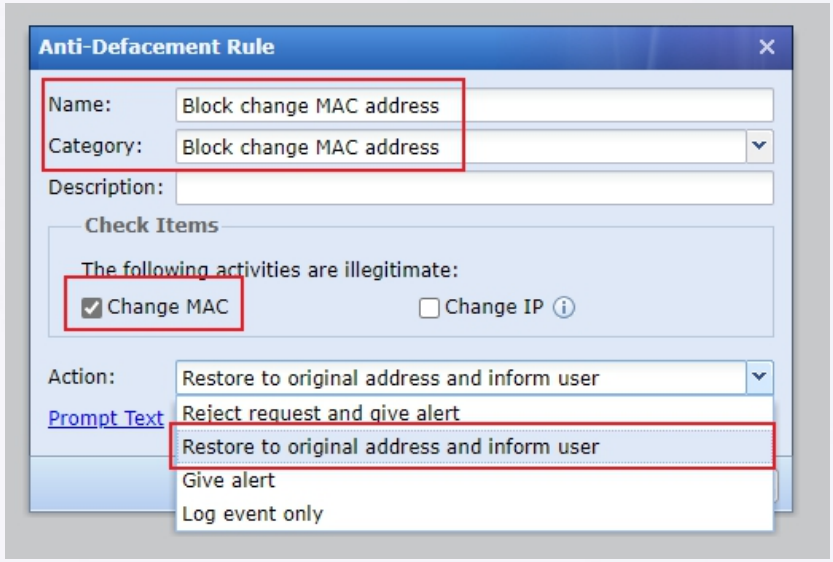


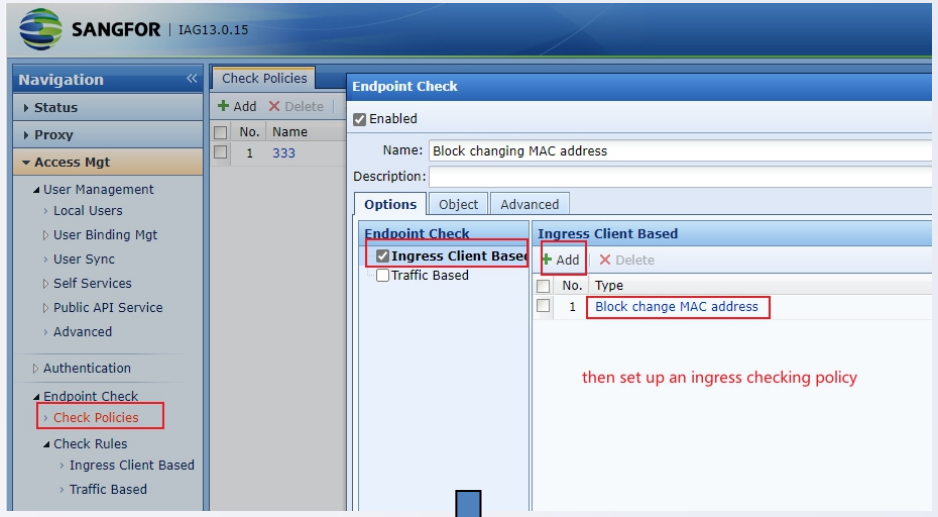


4.5 Ingress Client Checking Example

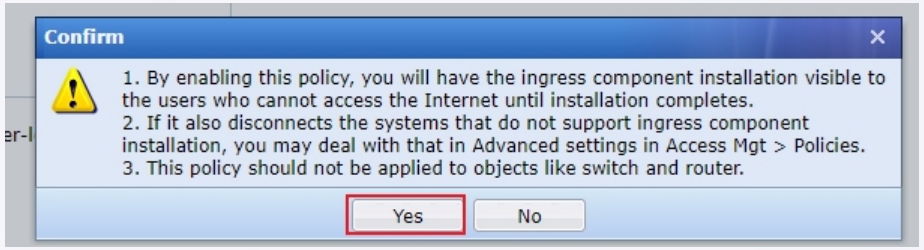
Let's take the example of prohibiting users from changing the MAC address. We can configure a tamper-proof rule, choose to prohibit modification of the MAC address, and at the same time, choose to restore the original MAC address and notify the user.

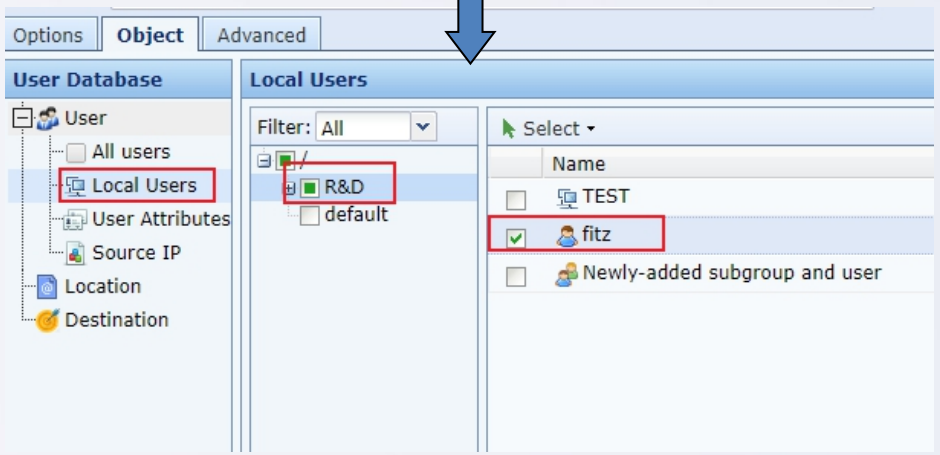
Set ingress check policy





Set ingress check rule





4.6 Ingress Client Check Results

We tried to modify the MAC address on Fitz's computer, and we found that the modification failed, and we also received a prompt.

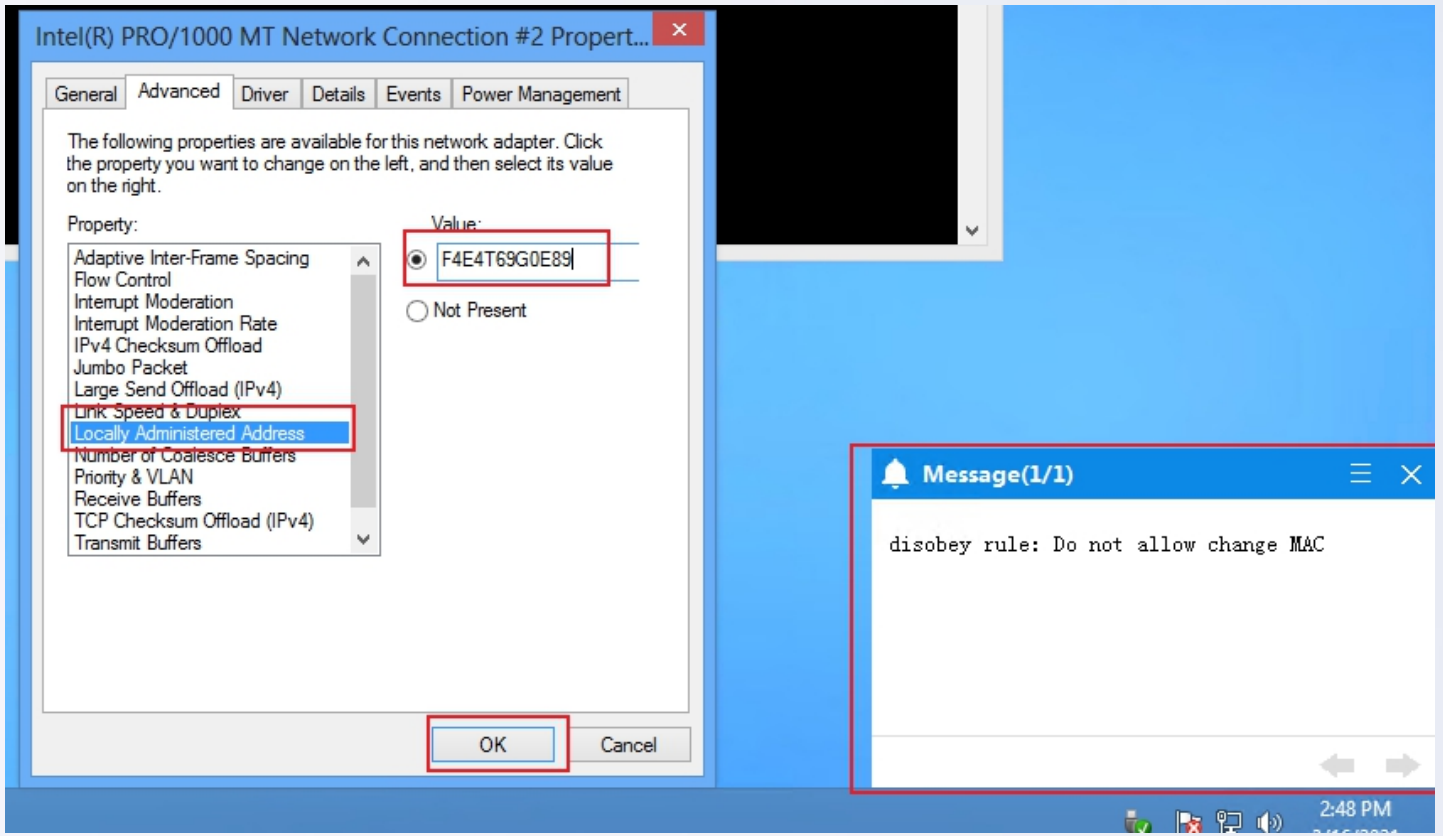
In addition, we can also see this record on the IAG compliance check results page.

Details

User: 10.28.60.26 | Group: /

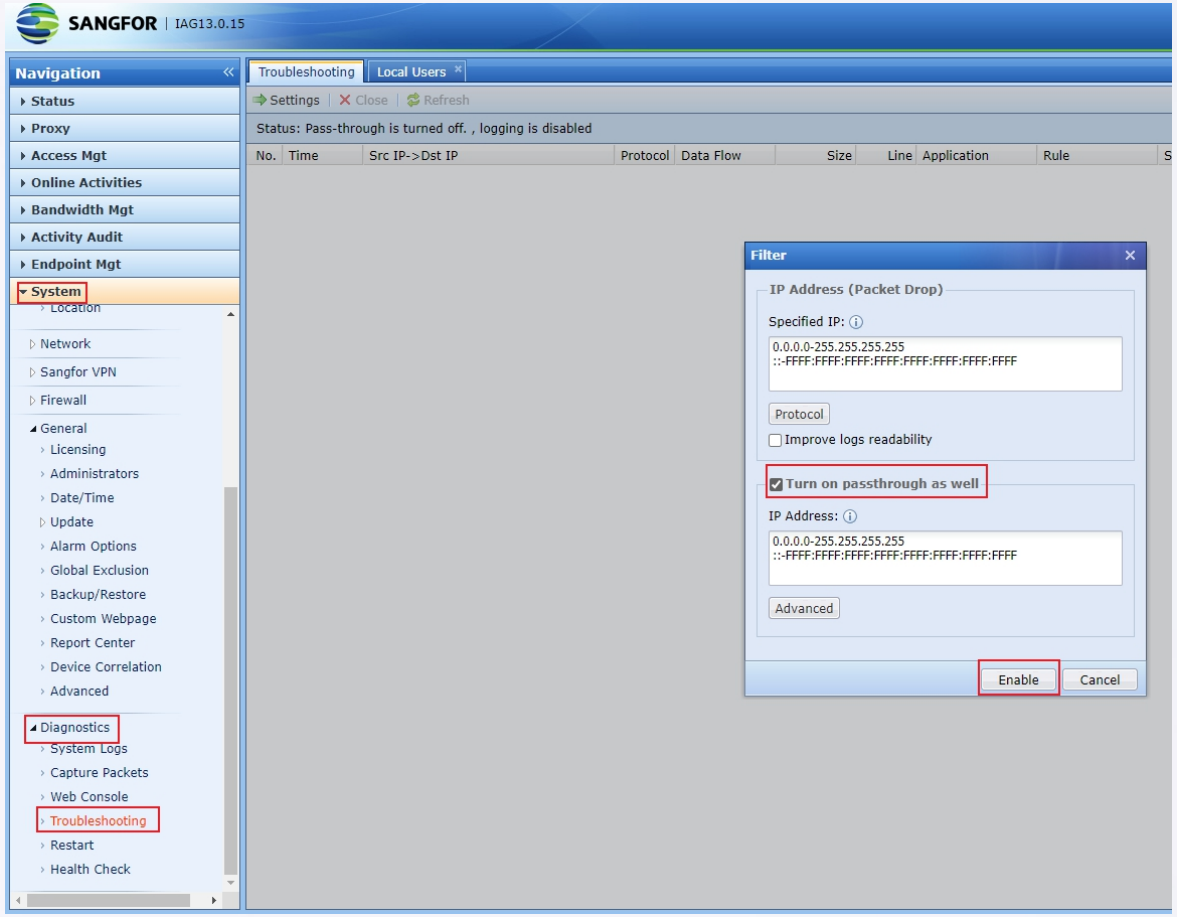
Source IP:	10.28.60.26
Location:	Not specified
Ingress Rule	Do not allow change MAC
Object	Anti-defacement
Description	-
Result	Legitimate
Action	Restore to original address and inform user
Prompt Context	pass detection
Details	-

Less Options



Emergency Measures

When you are trying IAG13.0.15 Beta and encounter problems, you can consider:
1. Delete/Disable related control policy.
2. If the problem still does not disappear, please open the Internet troubleshooting, and get in touch with us ASAP.



Sangfor Technical Support Center

Technical Service Center: +60 127117511 (7129)

Email: tech.support@sangfor.com

Website: community.sangfor.com

SANGFOR

Thanks