

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 **Endpoint 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!*

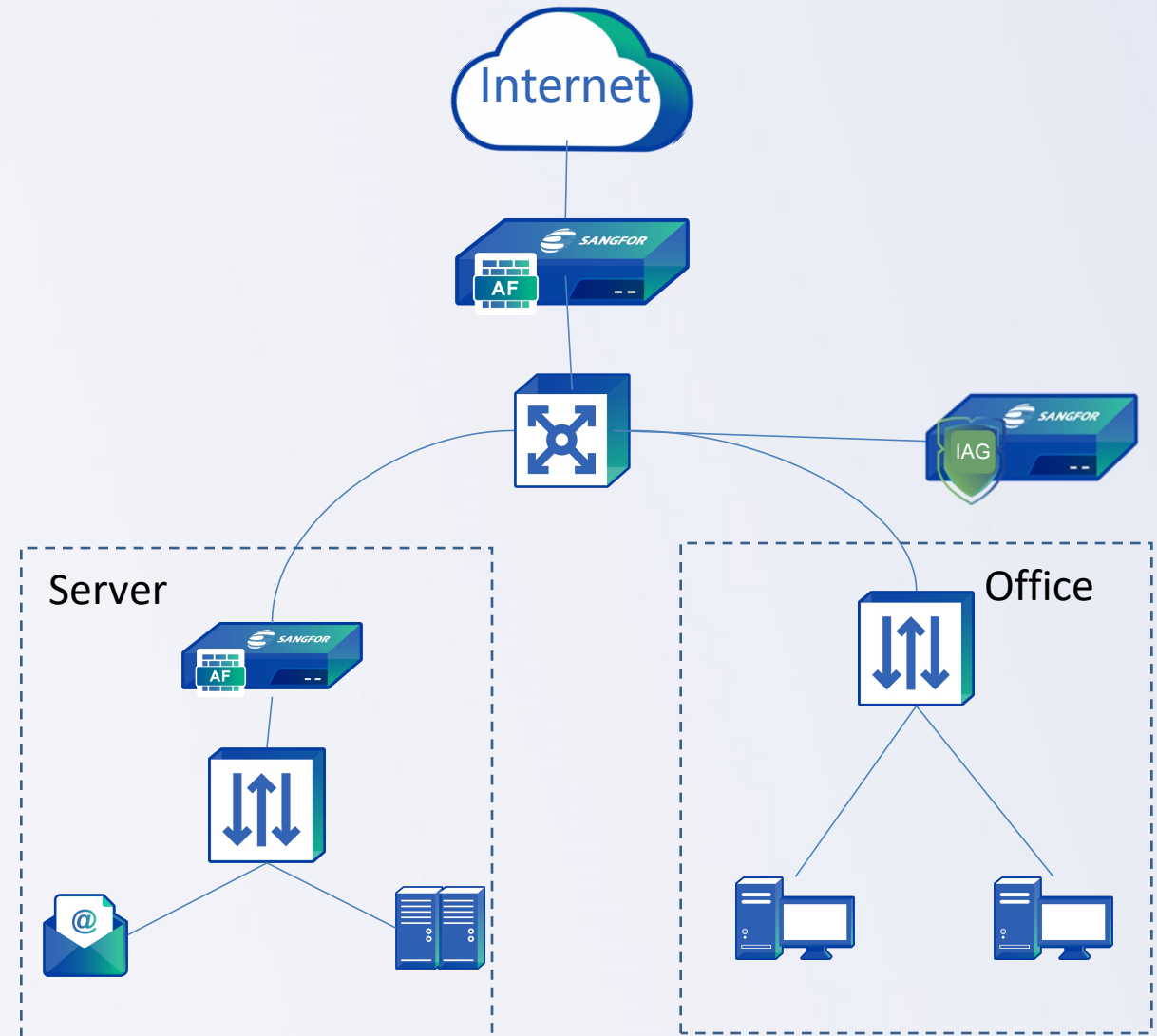
3.Asset Management Test Example

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.

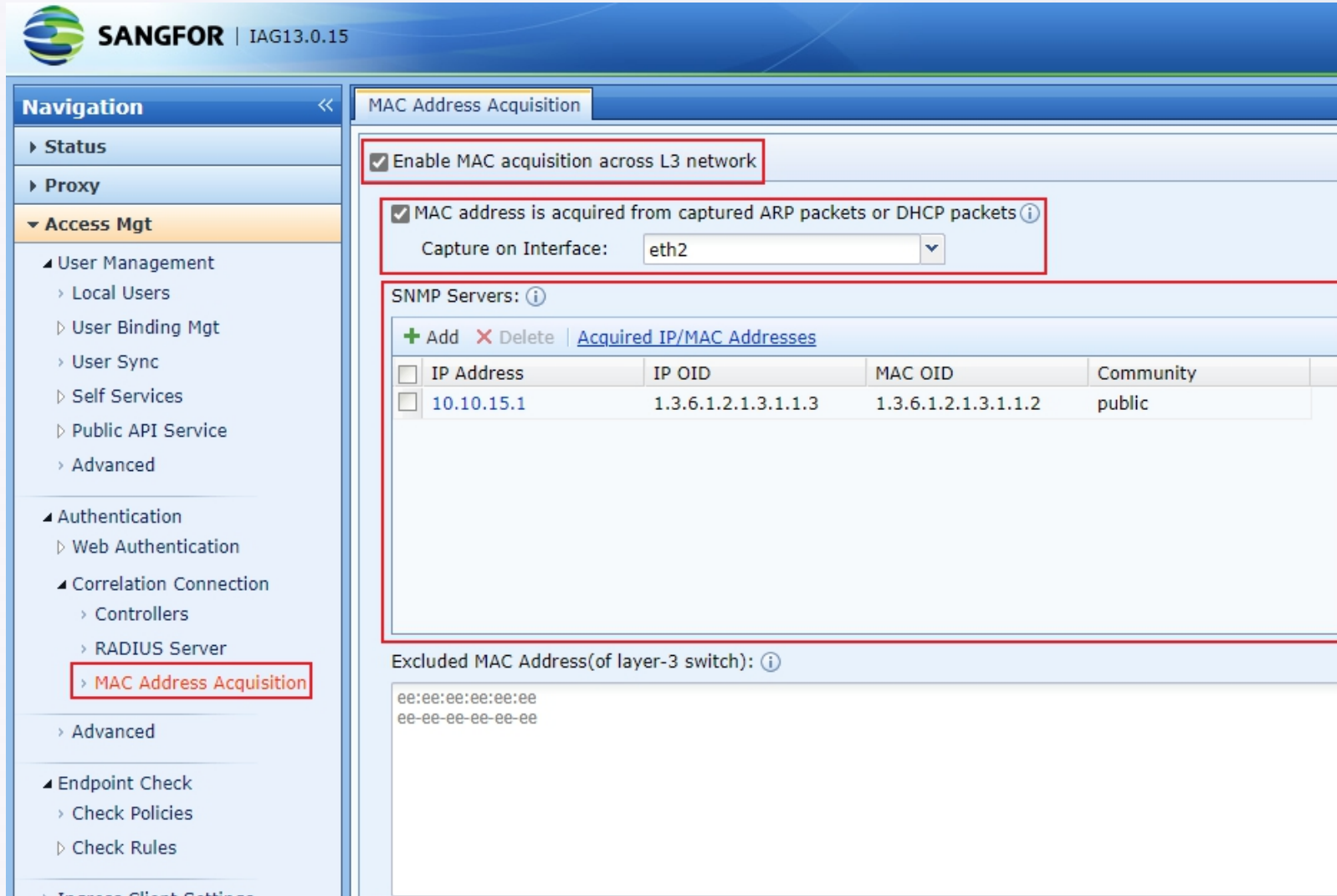
The picture on the right is an example of mirroring: mirror the tcp/dhcp traffic of the switch to the IAG, and the IAG will identify it based on the characteristics of the traffic.

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



The screenshot shows the SANGFOR IAG13.0.15 web interface for configuring MAC Address Acquisition. The left sidebar contains a navigation menu with the following items:

- Navigation <<
- Status
- Proxy
- Access Mgt
 - User Management
 - Local Users
 - User Binding Mgt
 - User Sync
 - Self Services
 - Public API Service
 - Advanced
 - Authentication
 - Web Authentication
 - Correlation Connection
 - Controllers
 - RADIUS Server
 - MAC Address Acquisition
 - Advanced
 - Endpoint Check
 - Check Policies
 - Check Rules
 - Increase Client Settings

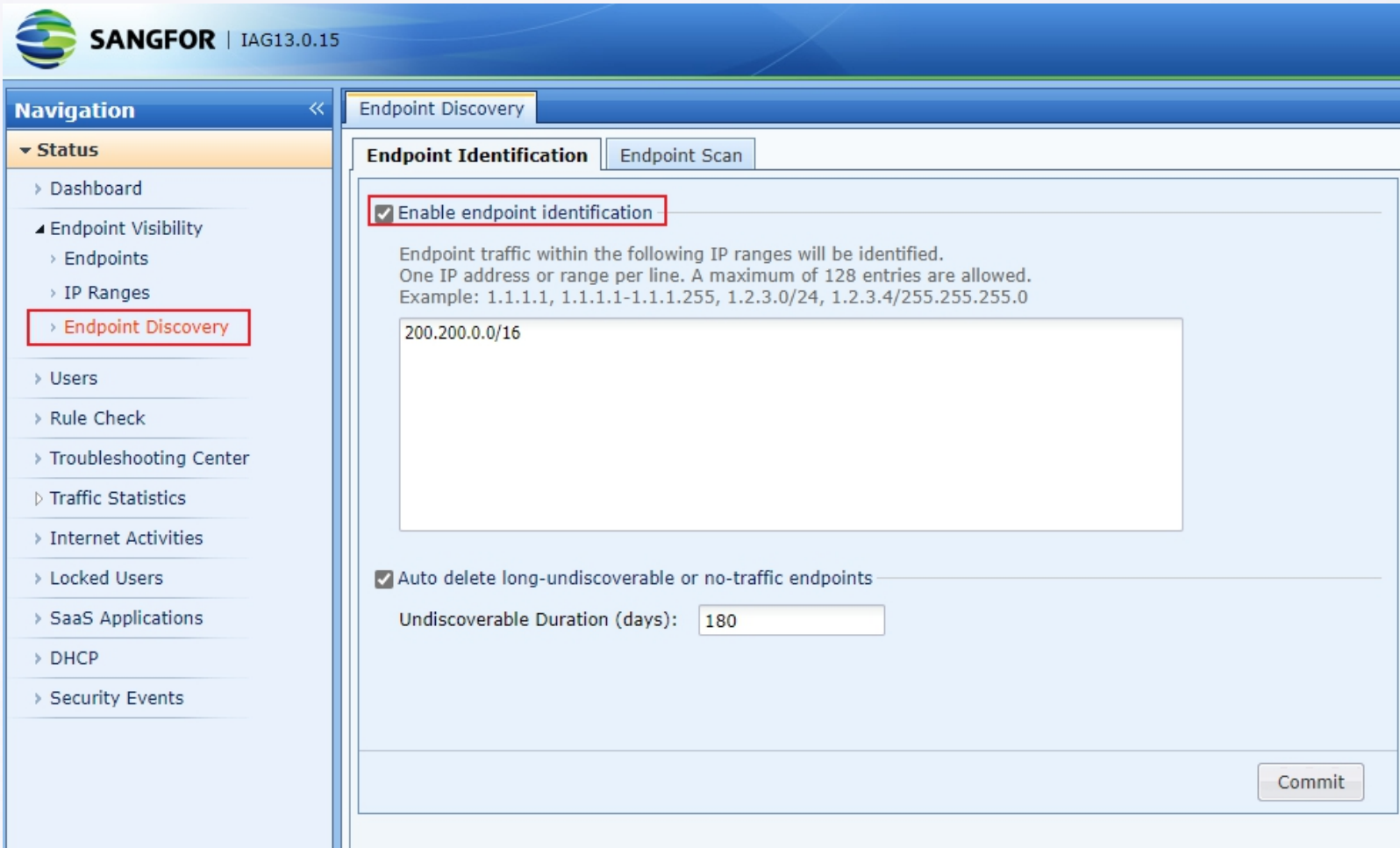
The main content area is titled "MAC Address Acquisition" and contains the following configuration options:

- Enable MAC acquisition across L3 network
- MAC address is acquired from captured ARP packets or DHCP packets ⓘ
Capture on Interface: eth2
- SNMP Servers: ⓘ
 - + Add X Delete | [Acquired IP/MAC Addresses](#)

<input type="checkbox"/>	IP Address	IP OID	MAC OID	Community
<input type="checkbox"/>	10.10.15.1	1.3.6.1.2.1.3.1.1.3	1.3.6.1.2.1.3.1.1.2	public
- Excluded MAC Address(of layer-3 switch): ⓘ
 - ee:ee:ee:ee:ee:ee
 - ee-ee-ee-ee-ee-ee

3.2 Enable Asset Identification

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



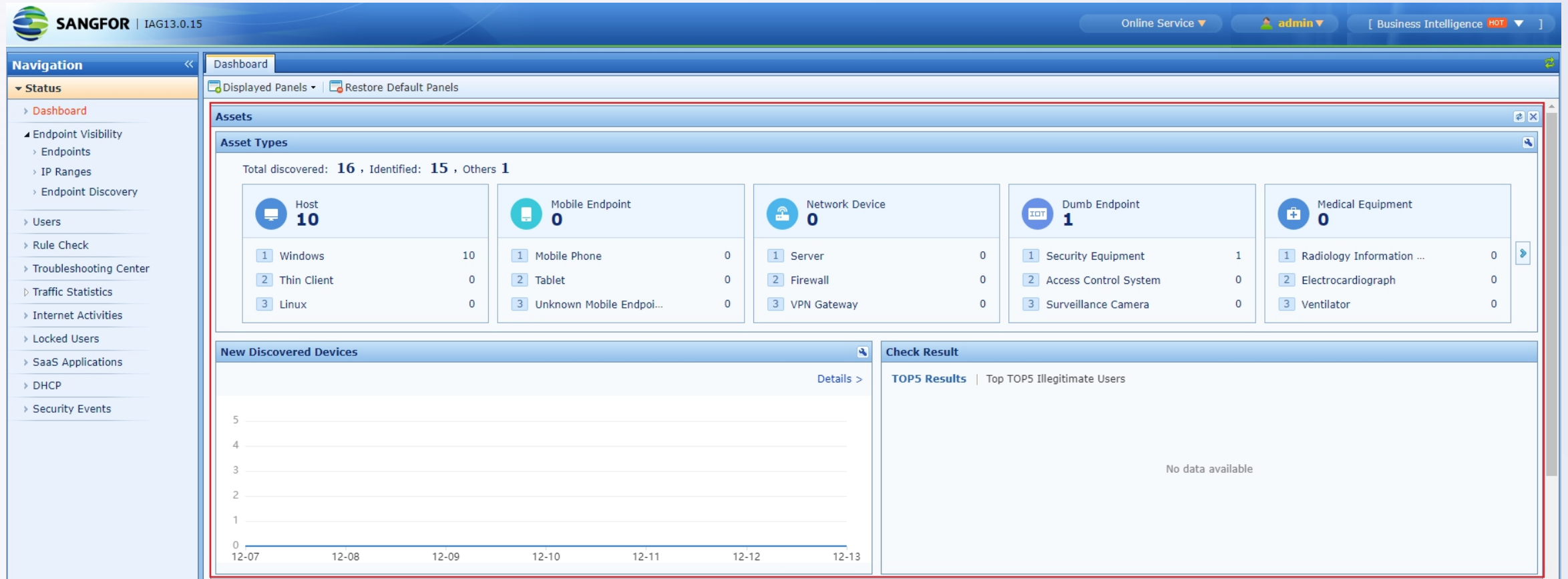
The screenshot shows the SANGFOR IAG13.0.15 web interface. The left navigation pane is expanded to 'Endpoint Discovery'. The main content area is titled 'Endpoint Discovery' and contains two tabs: 'Endpoint Identification' (selected) and 'Endpoint Scan'. Under 'Endpoint Identification', the checkbox 'Enable endpoint identification' is checked and highlighted with a red box. Below this, a text area contains the IP range '200.200.0.0/16'. Further down, the checkbox 'Auto delete long-undiscoverable or no-traffic endpoints' is also checked. Below this checkbox, the 'Undiscoverable Duration (days)' is set to '180'. A 'Commit' button is located at the bottom right of the configuration area.

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

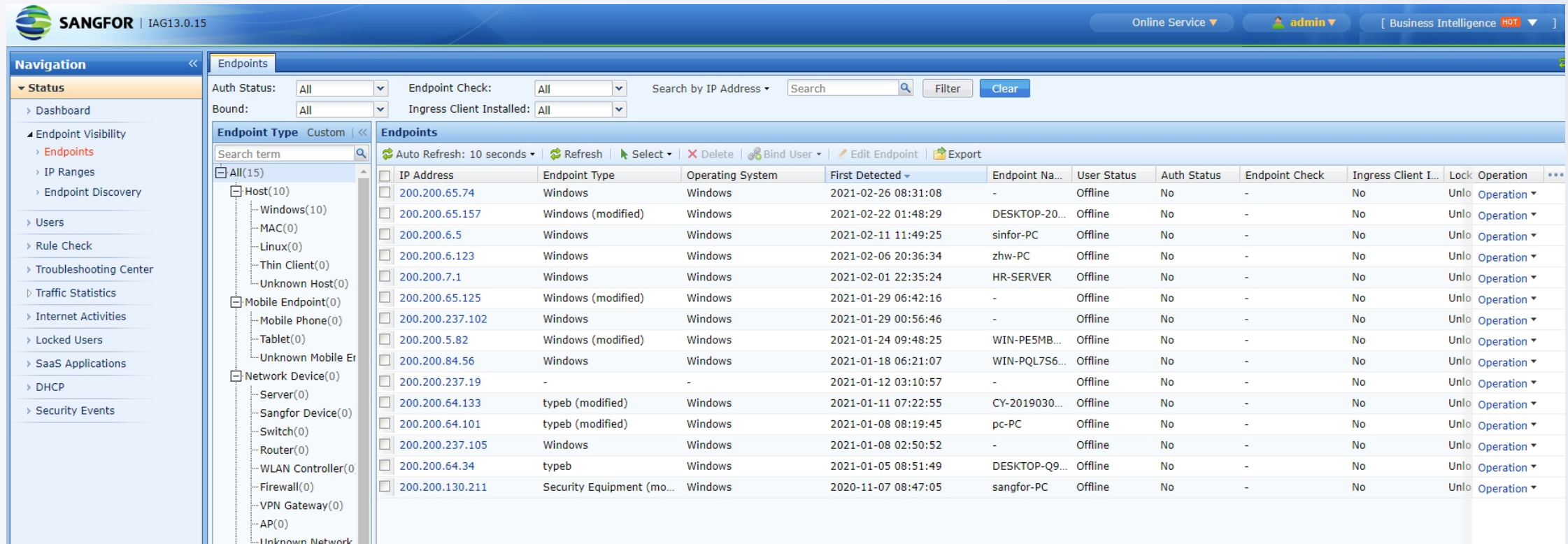
Go to the homepage to view the overall asset profile:



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:



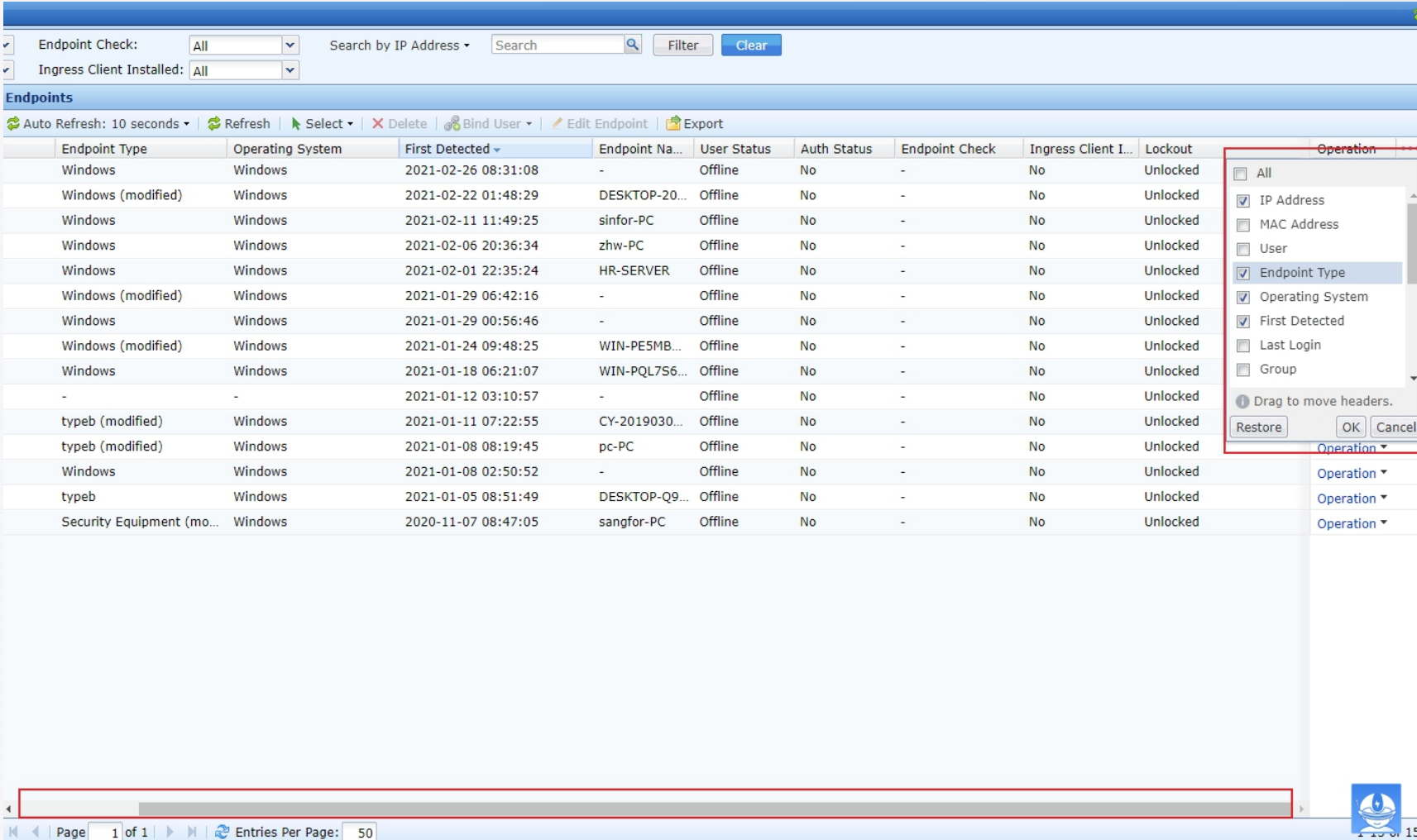
The screenshot displays the SANGFOR management console interface. The top navigation bar shows the SANGFOR logo, version IAG13.0.15, and user information (admin). The main content area is titled 'Endpoints' and features a search bar and filter options. A left sidebar provides navigation for various system components. The central table lists identified endpoints with the following columns: IP Address, Endpoint Type, Operating System, First Detected, Endpoint Name, User Status, Auth Status, Endpoint Check, Ingress Client Installed, Lock, and Operation. The table contains 15 entries, all currently in an 'Offline' state.

IP Address	Endpoint Type	Operating System	First Detected	Endpoint Name	User Status	Auth Status	Endpoint Check	Ingress Client Installed	Lock	Operation
200.200.65.74	Windows	Windows	2021-02-26 08:31:08	-	Offline	No	-	No	Unlo	Operation
200.200.65.157	Windows (modified)	Windows	2021-02-22 01:48:29	DESKTOP-20...	Offline	No	-	No	Unlo	Operation
200.200.6.5	Windows	Windows	2021-02-11 11:49:25	sinfor-PC	Offline	No	-	No	Unlo	Operation
200.200.6.123	Windows	Windows	2021-02-06 20:36:34	zhw-PC	Offline	No	-	No	Unlo	Operation
200.200.7.1	Windows	Windows	2021-02-01 22:35:24	HR-SERVER	Offline	No	-	No	Unlo	Operation
200.200.65.125	Windows (modified)	Windows	2021-01-29 06:42:16	-	Offline	No	-	No	Unlo	Operation
200.200.237.102	Windows	Windows	2021-01-29 00:56:46	-	Offline	No	-	No	Unlo	Operation
200.200.5.82	Windows (modified)	Windows	2021-01-24 09:48:25	WIN-PE5MB...	Offline	No	-	No	Unlo	Operation
200.200.84.56	Windows	Windows	2021-01-18 06:21:07	WIN-PQL7S6...	Offline	No	-	No	Unlo	Operation
200.200.237.19	-	-	2021-01-12 03:10:57	-	Offline	No	-	No	Unlo	Operation
200.200.64.133	typeb (modified)	Windows	2021-01-11 07:22:55	CY-2019030...	Offline	No	-	No	Unlo	Operation
200.200.64.101	typeb (modified)	Windows	2021-01-08 08:19:45	pc-PC	Offline	No	-	No	Unlo	Operation
200.200.237.105	Windows	Windows	2021-01-08 02:50:52	-	Offline	No	-	No	Unlo	Operation
200.200.64.34	typeb	Windows	2021-01-05 08:51:49	DESKTOP-Q9...	Offline	No	-	No	Unlo	Operation
200.200.130.211	Security Equipment (mo...	Windows	2020-11-07 08:47:05	sangfor-PC	Offline	No	-	No	Unlo	Operation

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.

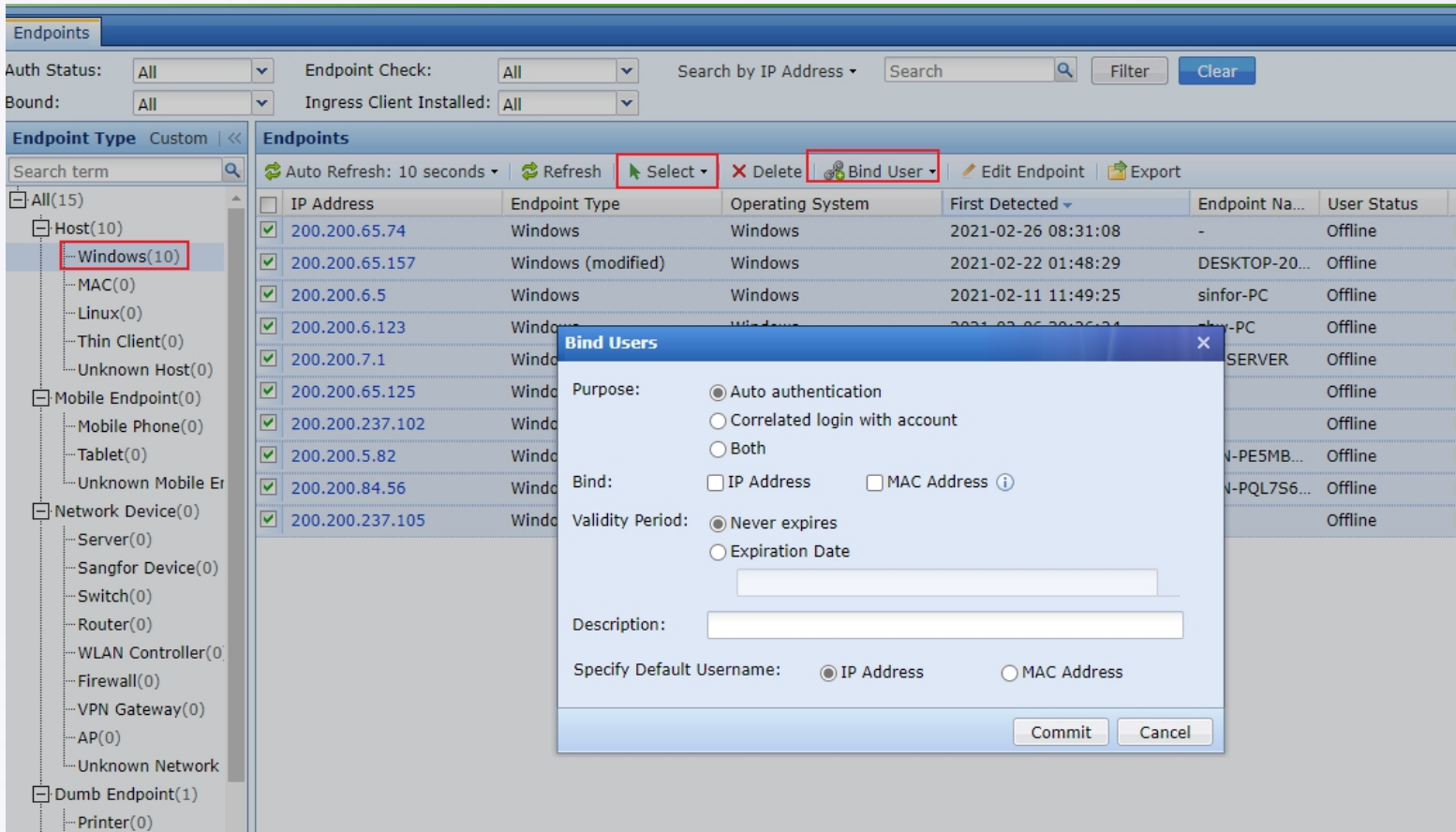


The screenshot shows the Sangfor endpoint management interface. At the top, there are filters for 'Endpoint Check' (set to 'All') and 'Ingress Client Installed' (set to 'All'). A search bar is available for 'Search by IP Address'. Below the filters is a table of endpoints with columns: Endpoint Type, Operating System, First Detected, Endpoint Name, User Status, Auth Status, Endpoint Check, Ingress Client I..., Lockout, and Operation. A context menu is open over the 'Operation' column of the first row, showing a list of columns to be displayed: All, IP Address, MAC Address, User, Endpoint Type, Operating System, First Detected, Last Login, and Group. The 'Endpoint Type' and 'Operating System' options are checked. The menu also includes a 'Drag to move headers.' instruction and 'Restore', 'OK', and 'Cancel' buttons. At the bottom, there is a pagination bar showing 'Page 1 of 1' and 'Entries Per Page: 50'.

Endpoint Type	Operating System	First Detected	Endpoint Name	User Status	Auth Status	Endpoint Check	Ingress Client I...	Lockout	Operation
Windows	Windows	2021-02-26 08:31:08	-	Offline	No	-	No	Unlocked	Operation
Windows (modified)	Windows	2021-02-22 01:48:29	DESKTOP-20...	Offline	No	-	No	Unlocked	Operation
Windows	Windows	2021-02-11 11:49:25	sinfor-PC	Offline	No	-	No	Unlocked	Operation
Windows	Windows	2021-02-06 20:36:34	zhw-PC	Offline	No	-	No	Unlocked	Operation
Windows	Windows	2021-02-01 22:35:24	HR-SERVER	Offline	No	-	No	Unlocked	Operation
Windows (modified)	Windows	2021-01-29 06:42:16	-	Offline	No	-	No	Unlocked	Operation
Windows	Windows	2021-01-29 00:56:46	-	Offline	No	-	No	Unlocked	Operation
Windows (modified)	Windows	2021-01-24 09:48:25	WIN-PE5MB...	Offline	No	-	No	Unlocked	Operation
Windows	Windows	2021-01-18 06:21:07	WIN-PQL7S6...	Offline	No	-	No	Unlocked	Operation
-	-	2021-01-12 03:10:57	-	Offline	No	-	No	Unlocked	Operation
typeb (modified)	Windows	2021-01-11 07:22:55	CY-2019030...	Offline	No	-	No	Unlocked	Operation
typeb (modified)	Windows	2021-01-08 08:19:45	pc-PC	Offline	No	-	No	Unlocked	Operation
Windows	Windows	2021-01-08 02:50:52	-	Offline	No	-	No	Unlocked	Operation
typeb	Windows	2021-01-05 08:51:49	DESKTOP-Q9...	Offline	No	-	No	Unlocked	Operation
Security Equipment (mo...	Windows	2020-11-07 08:47:05	sangfor-PC	Offline	No	-	No	Unlocked	Operation

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 screenshot displays the Sangfor Endpoint management interface. On the left, a tree view shows the 'Endpoint Type' organization structure, with 'Host(10)' expanded to show 'Windows(10)'. The main area shows a table of endpoints with columns for IP Address, Endpoint Type, Operating System, First Detected, Endpoint Name, and User Status. A 'Bind Users' dialog box is open in the foreground, allowing configuration for a batch of endpoints. The dialog includes options for Purpose (Auto authentication, Correlated login with account, Both), Bind (IP Address, MAC Address), Validity Period (Never expires, Expiration Date), and Specify Default Username (IP Address, MAC Address). The 'Commit' and 'Cancel' buttons are visible at the bottom of the dialog.

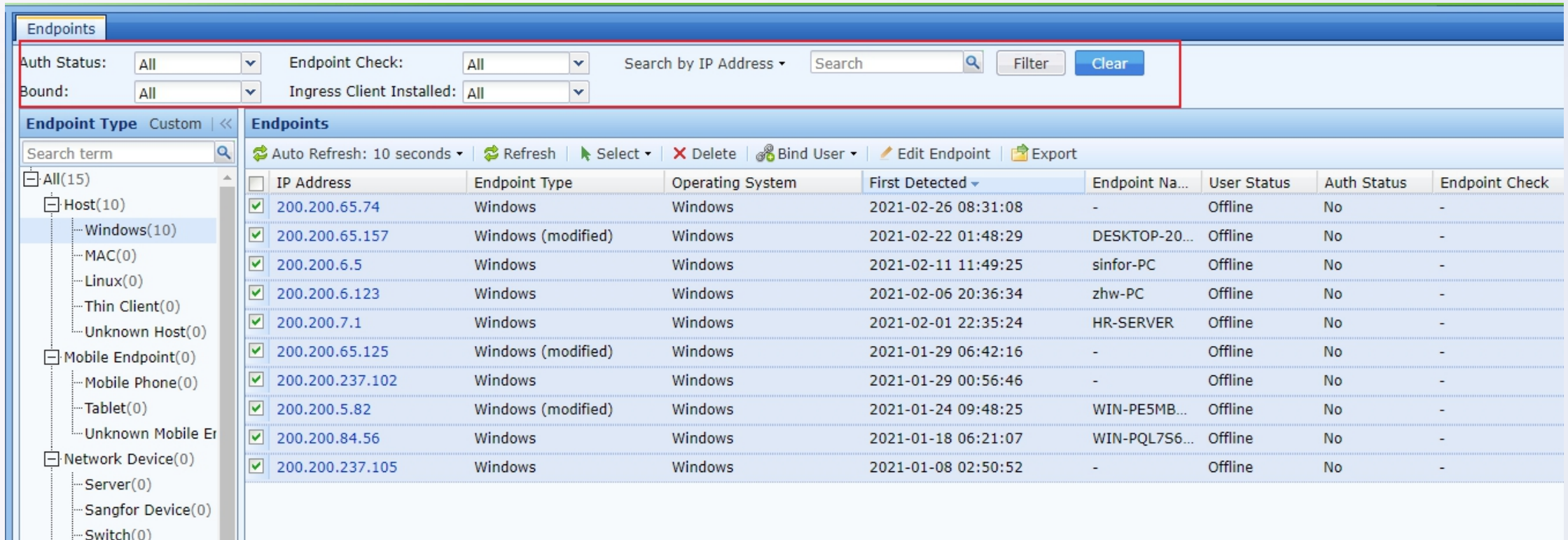
IP Address	Endpoint Type	Operating System	First Detected	Endpoint Name	User Status
200.200.65.74	Windows	Windows	2021-02-26 08:31:08	-	Offline
200.200.65.157	Windows (modified)	Windows	2021-02-22 01:48:29	DESKTOP-20...	Offline
200.200.6.5	Windows	Windows	2021-02-11 11:49:25	sinfor-PC	Offline
200.200.6.123	Windows	Windows	2021-02-05 20:26:24	sinfor-PC	Offline
200.200.7.1	Windows	Windows		SERVER	Offline
200.200.65.125	Windows	Windows			Offline
200.200.237.102	Windows	Windows		N-PE5MB...	Offline
200.200.5.82	Windows	Windows		N-PQL7S6...	Offline
200.200.84.56	Windows	Windows			Offline
200.200.237.105	Windows	Windows			Offline

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.



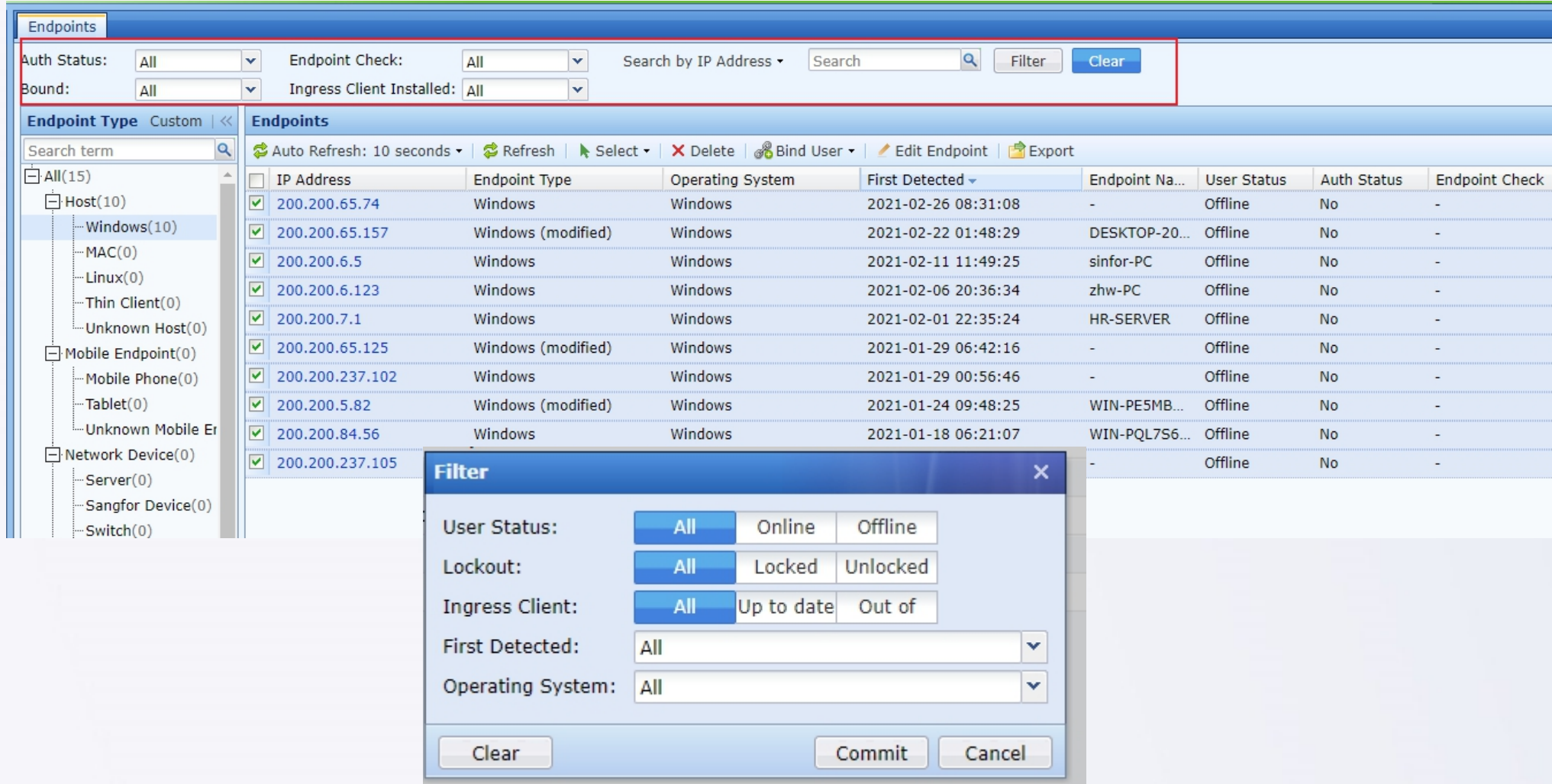
The screenshot displays the Sangfor Endpoint management interface. At the top, there are filter controls for 'Auth Status' (All), 'Endpoint Check' (All), 'Bound' (All), and 'Ingress Client Installed' (All). A search bar for 'IP Address' is also present. Below the filters, the 'Endpoints' table is shown with columns for IP Address, Endpoint Type, Operating System, First Detected, Endpoint Name, User Status, Auth Status, and Endpoint Check. The table lists 15 endpoints, all of which are Windows-based and currently offline. A tree view on the left shows the hierarchy of endpoints, including Hosts, Mobile Endpoints, and Network Devices.

IP Address	Endpoint Type	Operating System	First Detected	Endpoint Name	User Status	Auth Status	Endpoint Check
200.200.65.74	Windows	Windows	2021-02-26 08:31:08	-	Offline	No	-
200.200.65.157	Windows (modified)	Windows	2021-02-22 01:48:29	DESKTOP-20...	Offline	No	-
200.200.6.5	Windows	Windows	2021-02-11 11:49:25	sinfor-PC	Offline	No	-
200.200.6.123	Windows	Windows	2021-02-06 20:36:34	zhw-PC	Offline	No	-
200.200.7.1	Windows	Windows	2021-02-01 22:35:24	HR-SERVER	Offline	No	-
200.200.65.125	Windows (modified)	Windows	2021-01-29 06:42:16	-	Offline	No	-
200.200.237.102	Windows	Windows	2021-01-29 00:56:46	-	Offline	No	-
200.200.5.82	Windows (modified)	Windows	2021-01-24 09:48:25	WIN-PE5MB...	Offline	No	-
200.200.84.56	Windows	Windows	2021-01-18 06:21:07	WIN-PQL7S6...	Offline	No	-
200.200.237.105	Windows	Windows	2021-01-08 02:50:52	-	Offline	No	-

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:



The screenshot displays the Sangfor Endpoints management interface. At the top, there are filter controls for Auth Status, Bound, Endpoint Check, and Ingress Client Installed, all set to 'All'. A search bar is available for searching by IP Address. Below the filters is a table of endpoints with columns for IP Address, Endpoint Type, Operating System, First Detected, Endpoint Name, User Status, Auth Status, and Endpoint Check. A 'Filter' dialog box is open in the foreground, allowing for more granular filtering based on User Status, Lockout, Ingress Client, First Detected, and Operating System.

IP Address	Endpoint Type	Operating System	First Detected	Endpoint Name	User Status	Auth Status	Endpoint Check
200.200.65.74	Windows	Windows	2021-02-26 08:31:08	-	Offline	No	-
200.200.65.157	Windows (modified)	Windows	2021-02-22 01:48:29	DESKTOP-20...	Offline	No	-
200.200.6.5	Windows	Windows	2021-02-11 11:49:25	sinfor-PC	Offline	No	-
200.200.6.123	Windows	Windows	2021-02-06 20:36:34	zhw-PC	Offline	No	-
200.200.7.1	Windows	Windows	2021-02-01 22:35:24	HR-SERVER	Offline	No	-
200.200.65.125	Windows (modified)	Windows	2021-01-29 06:42:16	-	Offline	No	-
200.200.237.102	Windows	Windows	2021-01-29 00:56:46	-	Offline	No	-
200.200.5.82	Windows (modified)	Windows	2021-01-24 09:48:25	WIN-PE5MB...	Offline	No	-
200.200.84.56	Windows	Windows	2021-01-18 06:21:07	WIN-PQL756...	Offline	No	-
200.200.237.105					Offline	No	-

Filter Dialog Box:

- User Status: All (selected), Online, Offline
- Lockout: All (selected), Locked, Unlocked
- Ingress Client: All (selected), Up to date, Out of
- First Detected: All (dropdown)
- Operating System: All (dropdown)

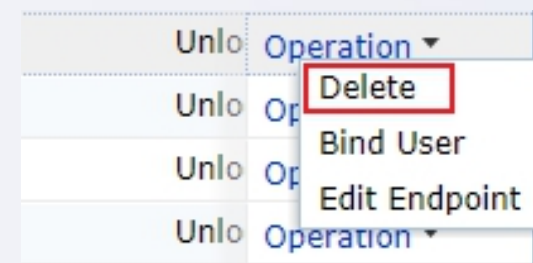
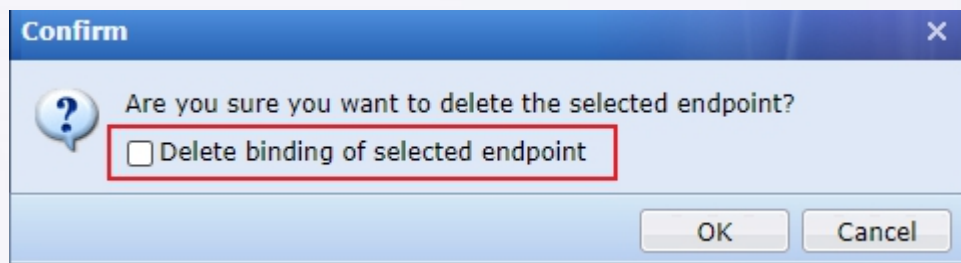
3.9 Asset Management - Delete

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:

Endpoints delete in batches

Auto Refresh: 10 seconds | Refresh | Select | **Delete** | Bind User | Edit Endpoint | Export

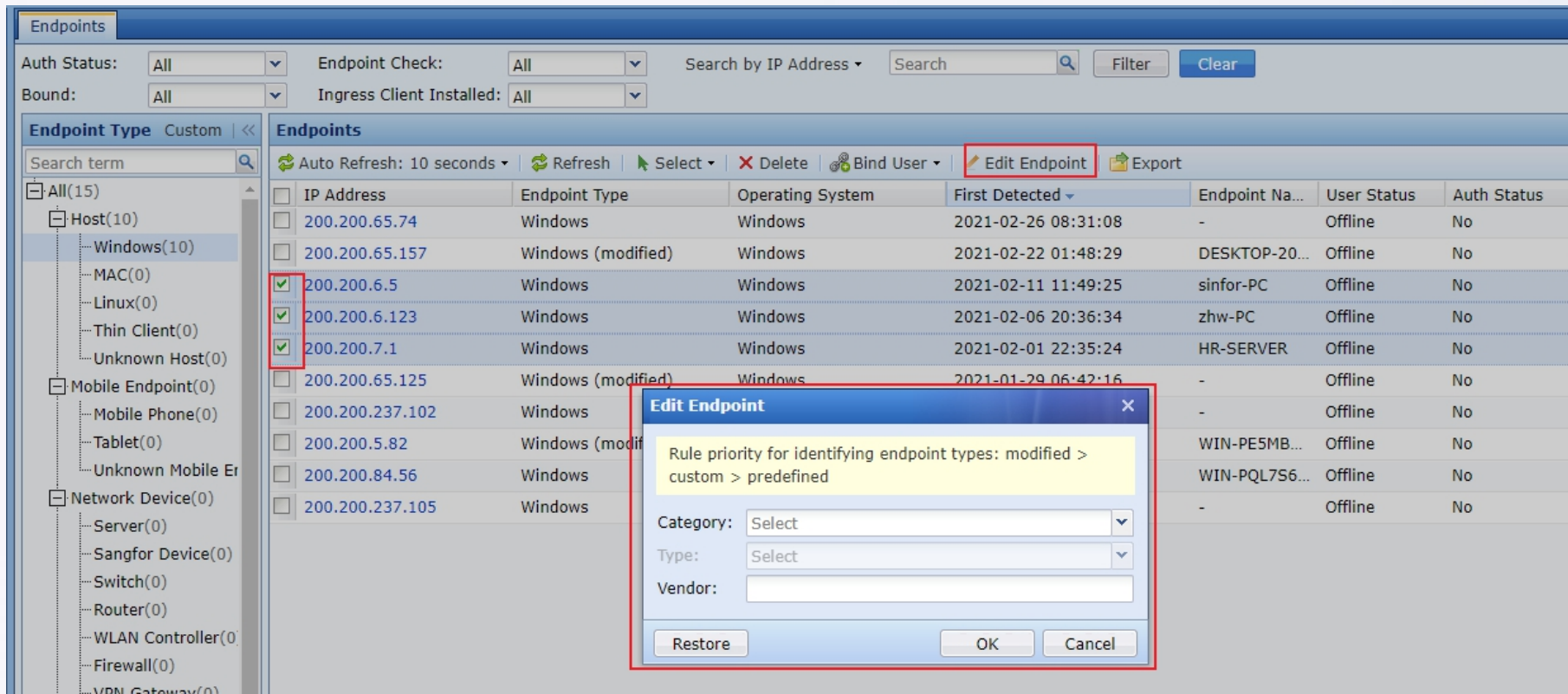
IP Address	Endpoint Type	Operating System	First Detected	Endpoint Na...	User Status	Auth Status	Endpoint Check	Ingress Client I...	Lock	Operation
<input checked="" type="checkbox"/> 200.200.65.74	Windows	Windows	2021-02-26 08:31:08	-	Offline	No	-	No	Unlo	Operation ▾
<input checked="" type="checkbox"/> 200.200.65.157	Windows (modified)	Windows	2021-02-22 01:48:29	DESKTOP-20...	Offline	No	-	No	Unlo	Operation ▾
<input checked="" type="checkbox"/> 200.200.6.5	Windows	Windows	2021-02-11 11:49:25	sinfor-PC	Offline	No	-	No	Unlo	Operation ▾
<input type="checkbox"/> 200.200.6.123	Windows	Windows	2021-02-06 20:36:34	zhw-PC	Offline	No	-	No	Unlo	Operation ▾
<input type="checkbox"/> 200.200.7.1	Windows	Windows	2021-02-01 22:35:24	HR-SERVER	Offline	No	-	No	Unlo	Operation ▾
<input type="checkbox"/> 200.200.65.125	Windows (modified)	Windows	2021-01-29 06:42:16	-	Offline	No	-	No	Unlo	Operation ▾
<input type="checkbox"/> 200.200.237.102	Windows	Windows	2021-01-29 00:56:46	-	Offline	No	-	No	Unlo	Operation ▾
<input type="checkbox"/> 200.200.5.82	Windows (modified)	Windows	2021-01-24 09:48:25	WIN-PE5MB...	Offline	No	-	No	Unlo	Operation ▾
<input type="checkbox"/> 200.200.84.56	Windows	Windows	2021-01-18 06:21:07	WIN-PQL7S6...	Offline	No	-	No	Unlo	Operation ▾
<input type="checkbox"/> 200.200.237.105	Windows	Windows	2021-01-08 02:50:52	-	Offline	No	-	No	Unlo	Operation ▾



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:



The screenshot shows the 'Endpoints' management interface. At the top, there are filters for 'Auth Status', 'Endpoint Check', 'Bound', and 'Ingress Client Installed'. Below these is a search bar and a table of endpoints. The table has columns for 'IP Address', 'Endpoint Type', 'Operating System', 'First Detected', 'Endpoint Name', 'User Status', and 'Auth Status'. Three endpoints are selected with checkboxes: 200.200.6.5, 200.200.6.123, and 200.200.7.1. An 'Edit Endpoint' button is highlighted in red. A dialog box titled 'Edit Endpoint' is open, showing a message about rule priority and fields for 'Category', 'Type', and 'Vendor'. The 'Edit Endpoint' button in the table is also highlighted in red.

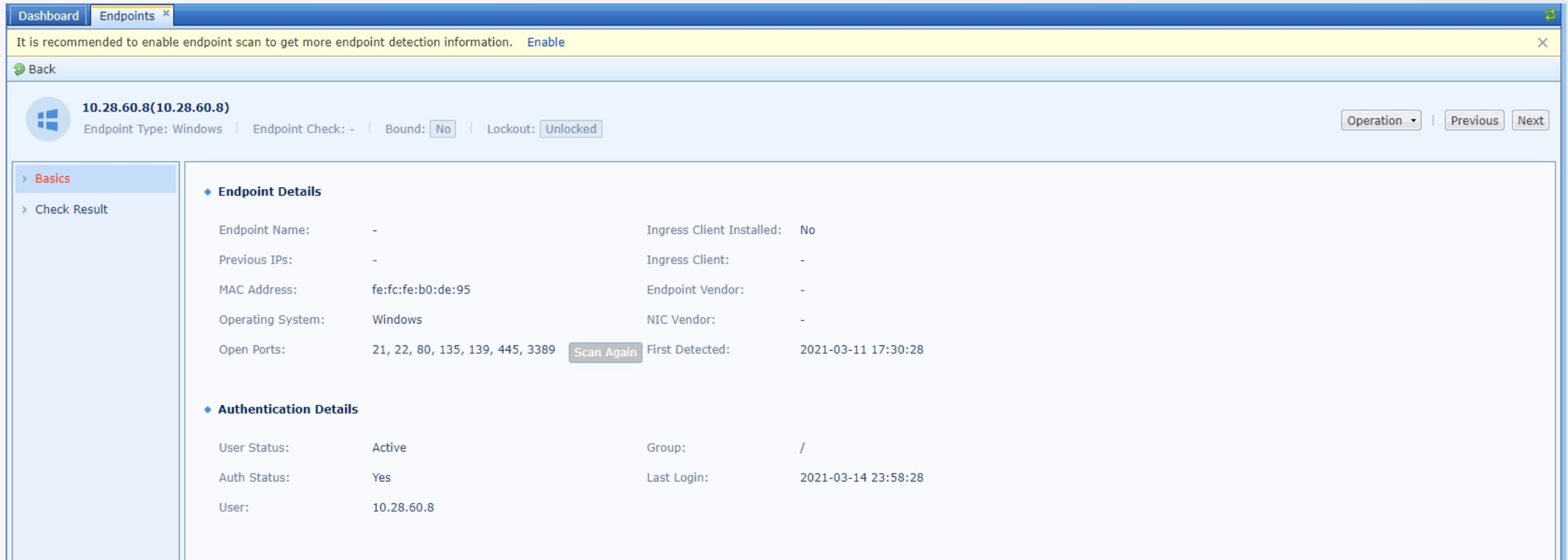
IP Address	Endpoint Type	Operating System	First Detected	Endpoint Name	User Status	Auth Status
<input type="checkbox"/> 200.200.65.74	Windows	Windows	2021-02-26 08:31:08	-	Offline	No
<input type="checkbox"/> 200.200.65.157	Windows (modified)	Windows	2021-02-22 01:48:29	DESKTOP-20...	Offline	No
<input checked="" type="checkbox"/> 200.200.6.5	Windows	Windows	2021-02-11 11:49:25	sinfor-PC	Offline	No
<input checked="" type="checkbox"/> 200.200.6.123	Windows	Windows	2021-02-06 20:36:34	zhw-PC	Offline	No
<input checked="" type="checkbox"/> 200.200.7.1	Windows	Windows	2021-02-01 22:35:24	HR-SERVER	Offline	No
<input type="checkbox"/> 200.200.65.125	Windows (modified)	Windows	2021-01-29 06:42:16	-	Offline	No
<input type="checkbox"/> 200.200.237.102	Windows	-	-	-	Offline	No
<input type="checkbox"/> 200.200.5.82	Windows (modified)	-	-	WIN-PE5MB...	Offline	No
<input type="checkbox"/> 200.200.84.56	Windows	-	-	WIN-PQL7S6...	Offline	No
<input type="checkbox"/> 200.200.237.105	Windows	-	-	-	Offline	No

Unlo	Operation ▾
Unlo	Operation ▾
Unlo	Operation ▾
Unlo	Operation ▾
Unlo	Delete Bind User Edit Endpoint
Unlo	Operation ▾
Unlo	Operation ▾

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:



Dashboard Endpoints

It is recommended to enable endpoint scan to get more endpoint detection information. [Enable](#)

Back

10.28.60.8(10.28.60.8)
 Endpoint Type: Windows | Endpoint Check: - | Bound: | Lockout:

Operation | Previous Next

> Basics

> Check Result

◆ **Endpoint Details**

Endpoint Name:	-	Ingress Client Installed:	No
Previous IPs:	-	Ingress Client:	-
MAC Address:	fe:fc:fe:b0:de:95	Endpoint Vendor:	-
Operating System:	Windows	NIC Vendor:	-
Open Ports:	21, 22, 80, 135, 139, 445, 3389	First Detected:	2021-03-11 17:30:28

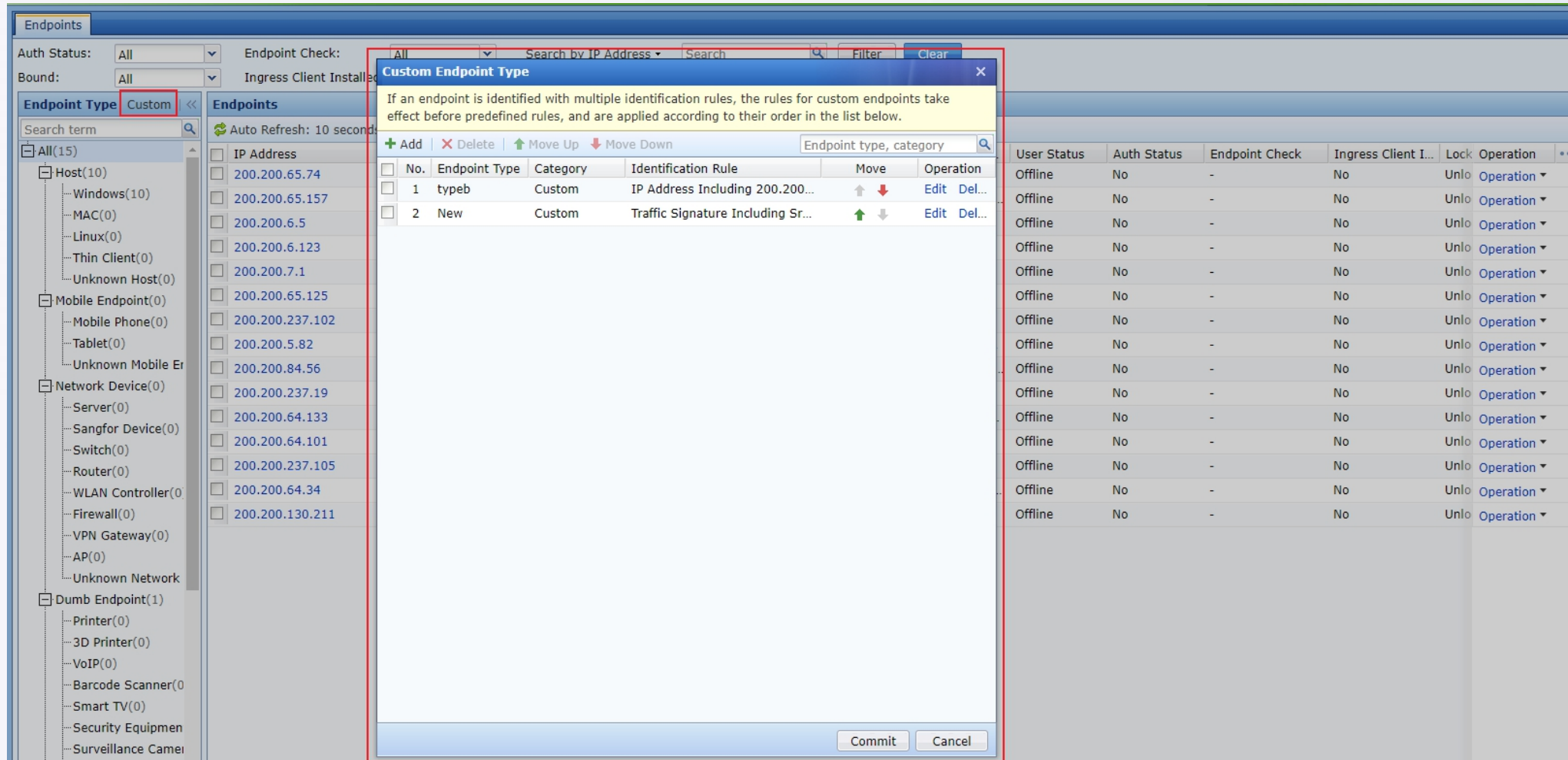
Scan Again

◆ **Authentication Details**

User Status:	Active	Group:	/
Auth Status:	Yes	Last Login:	2021-03-14 23:58:28
User:	10.28.60.8		

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:



Custom Endpoint Type

If an endpoint is identified with multiple identification rules, the rules for custom endpoints take effect before predefined rules, and are applied according to their order in the list below.

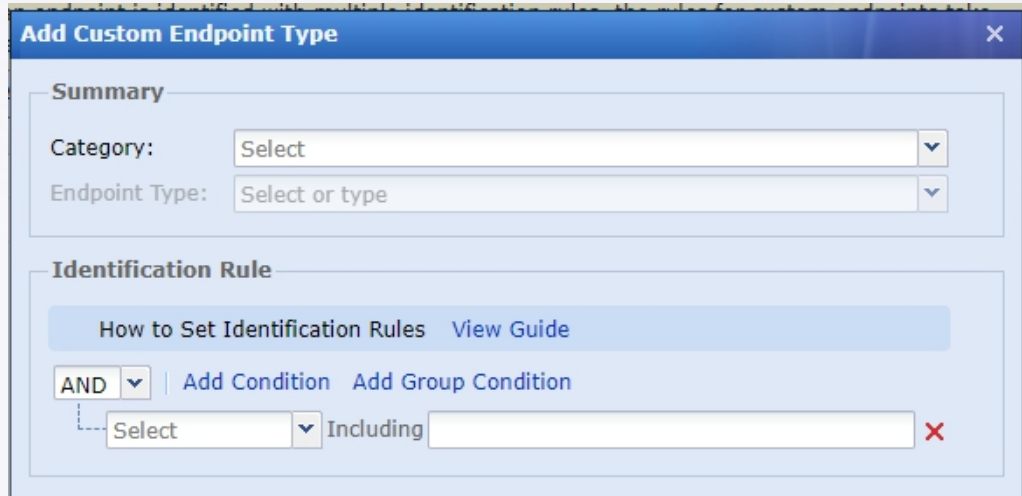
+ Add | X Delete | ↑ Move Up | ↓ Move Down

No.	Endpoint Type	Category	Identification Rule	Move	Operation
1	typeb	Custom	IP Address Including 200.200...	↑ ↓	Edit Del...
2	New	Custom	Traffic Signature Including Sr...	↑ ↓	Edit Del...

Commit Cancel

3.13 Asset Management - Custom Endpoint Type

Add a custom Endpoint type, as shown below:



Add Custom Endpoint Type

Summary

Category: Select

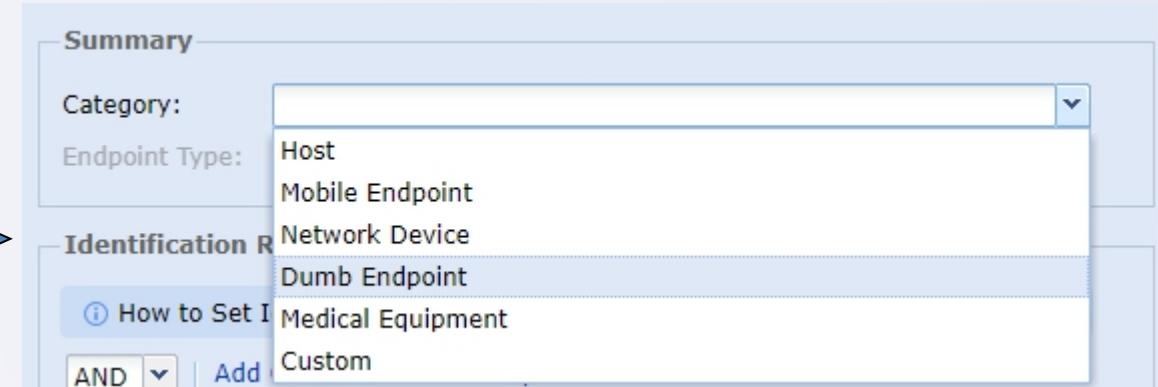
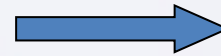
Endpoint Type: Select or type

Identification Rule

How to Set Identification Rules View Guide

AND Add Condition Add Group Condition

Select Including X



Summary

Category: [dropdown]

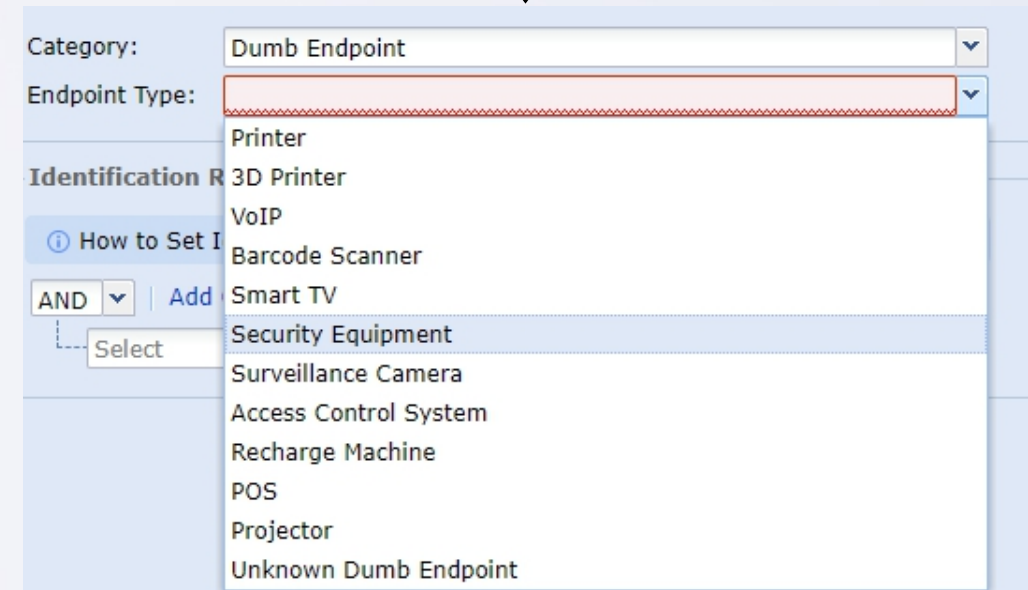
Endpoint Type: [dropdown menu open]

- Host
- Mobile Endpoint
- Network Device
- Dumb Endpoint
- Medical Equipment
- Custom

Identification Rule

How to Set I

AND Add



Category: Dumb Endpoint

Endpoint Type: [dropdown menu open]

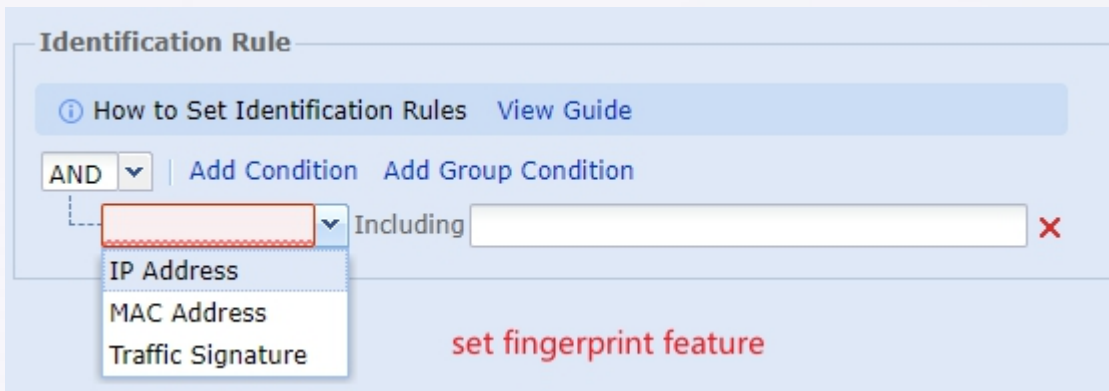
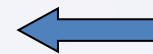
- Printer
- 3D Printer
- VoIP
- Barcode Scanner
- Smart TV
- Security Equipment
- Surveillance Camera
- Access Control System
- Recharge Machine
- POS
- Projector
- Unknown Dumb Endpoint

Identification Rule

How to Set I

AND Add

Select



Identification Rule

How to Set Identification Rules View Guide

AND Add Condition Add Group Condition

[dropdown menu open]

- IP Address
- MAC Address
- Traffic Signature

Including X

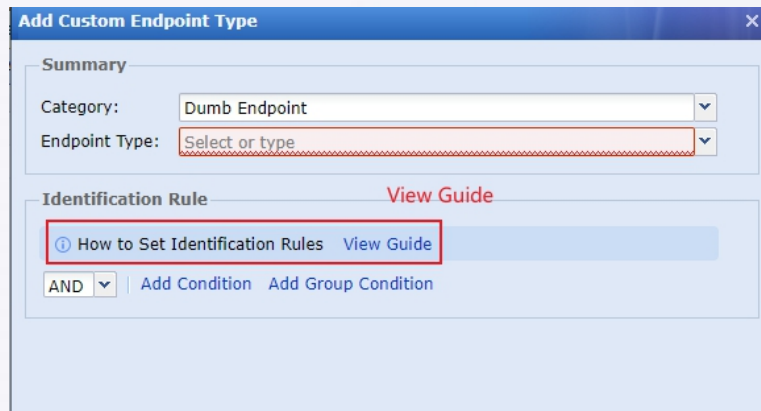
set fingerprint feature

3.14 Asset Management - Custom Endpoint Type

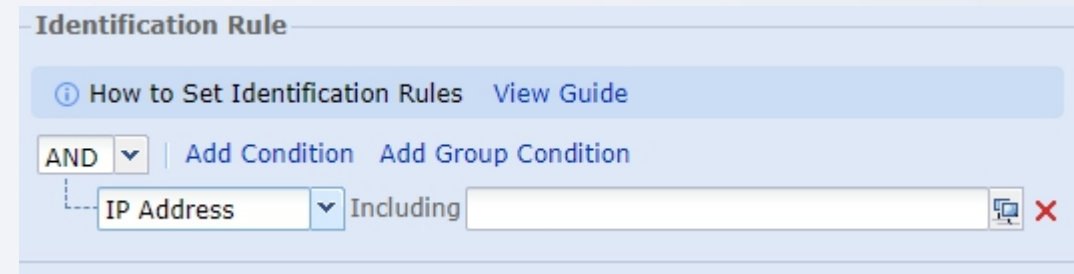
Set fingerprint features, as shown below:

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.



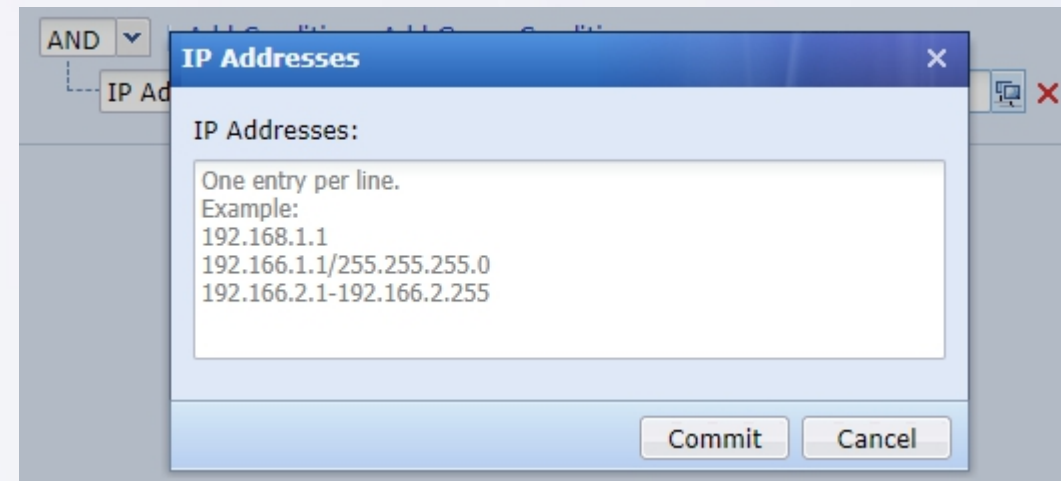
The 'Add Custom Endpoint Type' dialog box is shown. It has a 'Summary' section with 'Category' set to 'Dumb Endpoint' and 'Endpoint Type' set to 'Select or type'. Below is the 'Identification Rule' section, which includes a 'View Guide' link and a dropdown menu set to 'AND' with 'Add Condition' and 'Add Group Condition' options.



The 'Identification Rule' configuration area is shown. It features a 'View Guide' link, a dropdown menu set to 'AND', and 'Add Condition' and 'Add Group Condition' options. A condition is added: 'IP Address' with the operator 'Including' and an empty input field.



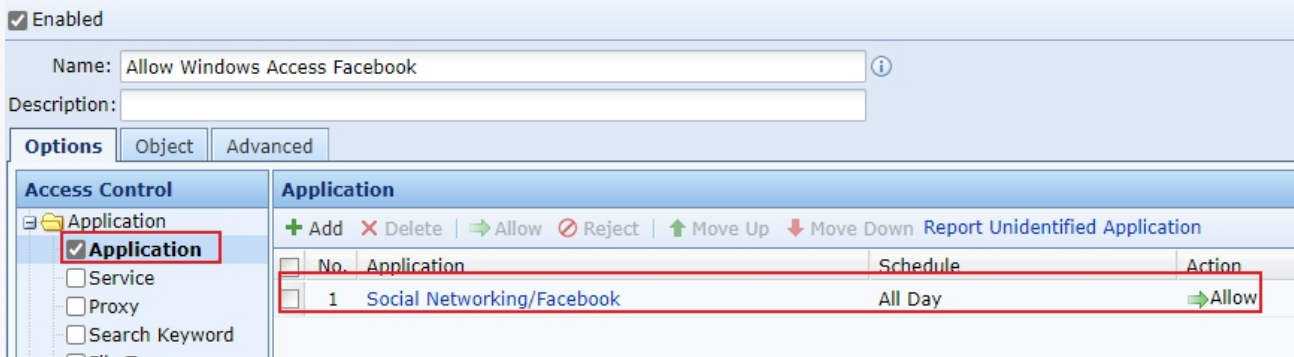
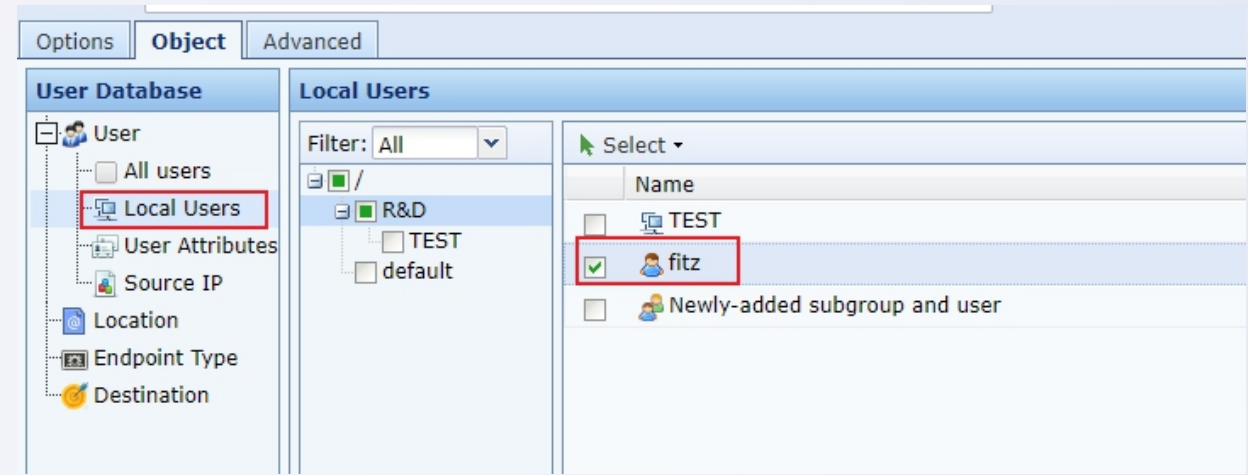
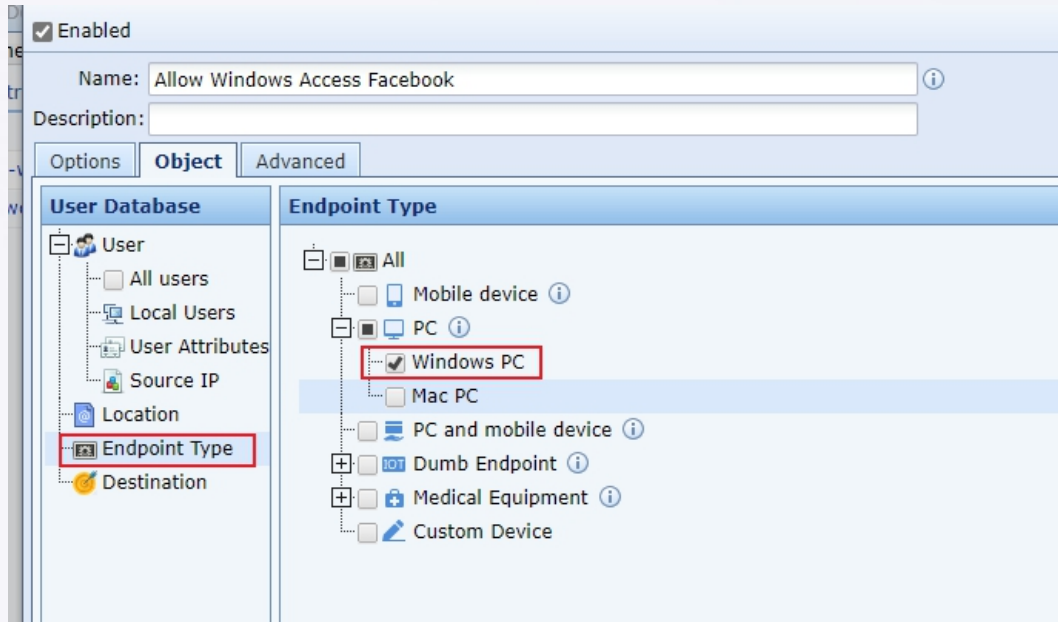
The 'Traffic Signatures' dialog box is shown. It contains fields for 'Src Port' (with example '1813'), 'Dst IP' (with example '192.168.1.1'), and 'Service Name' (set to 'DNS'). 'Commit' and 'Cancel' buttons are at the bottom.



The 'IP Addresses' dialog box is shown. It contains a text area for entering IP addresses, with instructions: 'One entry per line. Example: 192.168.1.1, 192.166.1.1/255.255.255.0, 192.166.2.1-192.166.2.255'. 'Commit' and 'Cancel' buttons are at the bottom.

3.15 Configuring Control Strategy according to Endpoint Type

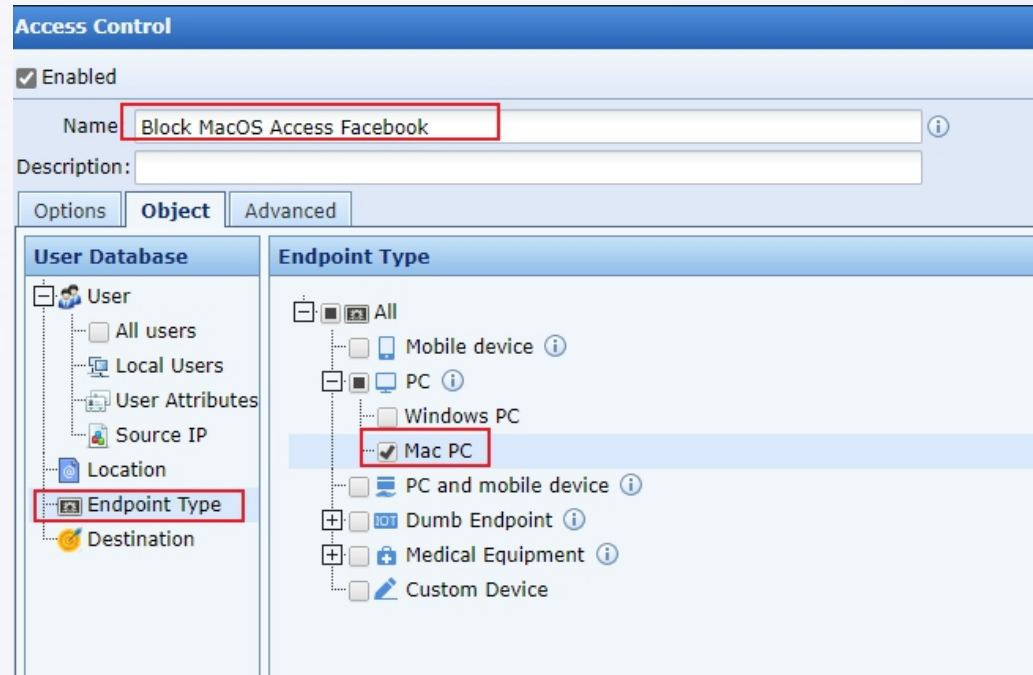
Configure the comparison of two new strategies in the access permission policy, and the applicable object is set to test PC. Here, two Endpoints of different Endpoint types are used to check the control effect. First, create a new policy that allows windowsPC to access the website, and the applicable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



Access Control

Enabled

Name:

Description:

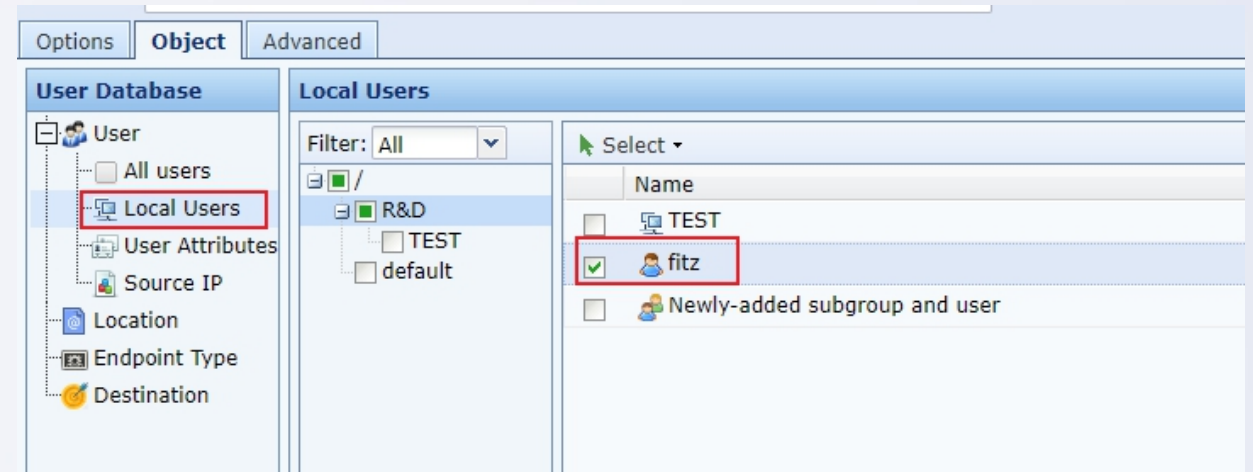
Options | **Object** | Advanced

User Database

- User
 - All users
 - Local Users
 - User Attributes
 - Source IP
 - Location
 - Endpoint Type**
 - Destination

Endpoint Type

- All
 - Mobile device
 - PC
 - Windows PC
 - Mac PC**
 - PC and mobile device
 - Dumb Endpoint
 - Medical Equipment
 - Custom Device



Options | **Object** | Advanced

User Database

- User
 - All users
 - Local Users**
 - User Attributes
 - Source IP
 - Location
 - Endpoint Type
 - Destination

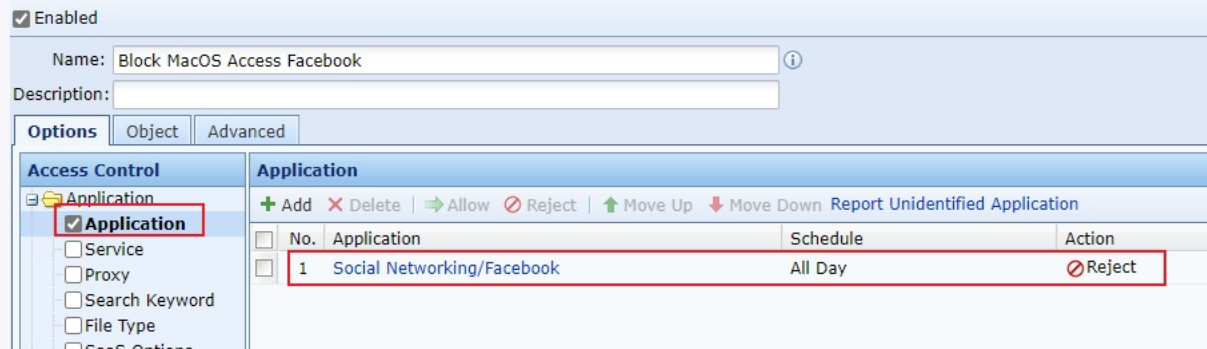
Local Users

Filter: All

- R&D
 - TEST
 - default

Select

Name
<input type="checkbox"/> TEST
<input checked="" type="checkbox"/> fitz
<input type="checkbox"/> Newly-added subgroup and user



Enabled

Name:

Description:

Options | Object | Advanced

Access Control

- Application**
- Service
- Proxy
- Search Keyword
- File Type
- SSS Options

Application

+ Add - Delete | → Allow | ↻ Reject | ↑ Move Up | ↓ Move Down | Report Unidentified Application

No.	Application	Schedule	Action
1	Social Networking/Facebook	All Day	Reject

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

Options | Object | Advanced

User Database

- User
 - All users
 - Local Users
 - User Attributes
 - Source IP
- Location
- Endpoint Type**
- Destination

Endpoint Type

- All
 - Mobile device ⓘ
 - PC ⓘ
 - Windows PC
 - Mac PC
 - PC and mobile device ⓘ
 - Dumb Endpoint ⓘ
 - Printer
 - 3D Printer
 - VoIP
 - Barcode Scanner
 - Smart TV
 - Security Equipment
 - Surveillance Camera
 - Access Control System
 - Recharge Machine
 - POS
 - Projector
 - Medical Equipment ⓘ
 - Radiology Information System
 - Monitor
 - Medical Printer
 - Electrocardiograph
 - Ventilator
 - Custom Device

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.

The screenshot displays the SANGFOR IP Management interface. On the left is a navigation menu with categories like Status, Dashboard, Endpoint Visibility, Endpoints, IP Ranges, Users, Rule Check, Troubleshooting Center, Traffic Statistics, Internet Activities, Locked Users, SaaS Applications, DHCP, Security Events, Proxy, Access Mgt, and Online Activities. The main area is split into two panes: 'IP Ranges' and 'IP Address Pool'. The 'IP Ranges' pane shows a tree view with 'RD (200.200.0.5...)' selected, containing sub-items '200.200.7.0/24' and '200.200.64.0/24'. The 'IP Address Pool' pane shows a grid for the '200.200.237.0/24' range, with a total of 256 IP addresses. A legend indicates 3 Normal, 0 Long-offline, and 253 Free addresses. The grid shows IP addresses from 0 to 255, with some cells highlighted in blue.

IP Address	Status
0	Free
1	Free
2	Free
3	Free
4	Free
5	Free
6	Free
7	Free
8	Free
9	Free
10	Free
11	Free
12	Free
13	Free
14	Free
15	Free
16	Free
17	Free
18	Free
19	Normal
20	Free
21	Free
22	Free
23	Free
24	Free
25	Free
26	Free
27	Free
28	Free
29	Free
30	Free
31	Free
32	Free
33	Free
34	Free
35	Free
36	Free
37	Free
38	Free
39	Free
40	Free
41	Free
42	Free
43	Free
44	Free
45	Free
46	Free
47	Free
48	Free
49	Free
50	Free
51	Free
52	Free
53	Free
54	Free
55	Free
56	Free
57	Free
58	Free
59	Free
60	Free
61	Free
62	Free
63	Free
64	Free
65	Free
66	Free
67	Free
68	Free
69	Free
70	Free
71	Free
72	Free
73	Free
74	Free
75	Free
76	Free
77	Free
78	Free
79	Free
80	Free
81	Free
82	Free
83	Free
84	Free
85	Free
86	Free
87	Free
88	Free
89	Free
90	Free
91	Free
92	Free
93	Free
94	Free
95	Free
96	Free
97	Free
98	Free
99	Free
100	Free
101	Free
102	Normal
103	Free
104	Free
105	Normal
106	Free
107	Free
108	Free
109	Free
110	Free
111	Free
112	Free
113	Free
114	Free
115	Free
116	Free
117	Free
118	Free
119	Free
120	Free
121	Free
122	Free
123	Free
124	Free
125	Free
126	Free
127	Free
128	Free
129	Free
130	Free
131	Free
132	Free
133	Free
134	Free
135	Free
136	Free
137	Free
138	Free
139	Free
140	Free
141	Free
142	Free
143	Free
144	Free
145	Free
146	Free
147	Free
148	Free
149	Free
150	Free
151	Free
152	Free
153	Free
154	Free
155	Free
156	Free
157	Free
158	Free
159	Free
160	Free
161	Free
162	Free
163	Free
164	Free
165	Free
166	Free
167	Free
168	Free
169	Free
170	Free
171	Free
172	Free
173	Free
174	Free
175	Free
176	Free
177	Free
178	Free
179	Free
180	Free
181	Free
182	Free
183	Free
184	Free
185	Free
186	Free
187	Free
188	Free
189	Free
190	Free
191	Free
192	Free
193	Free
194	Free
195	Free
196	Free
197	Free
198	Free
199	Free
200	Free
201	Free
202	Free
203	Free
204	Free
205	Free
206	Free
207	Free
208	Free
209	Free
210	Free
211	Free
212	Free
213	Free
214	Free
215	Free
216	Free
217	Free
218	Free
219	Free
220	Free
221	Free
222	Free
223	Free
224	Free
225	Free
226	Free
227	Free
228	Free
229	Free
230	Free
231	Free
232	Free
233	Free
234	Free
235	Free
236	Free
237	Free
238	Free
239	Free
240	Free
241	Free
242	Free
243	Free
244	Free
245	Free
246	Free
247	Free
248	Free
249	Free
250	Free
251	Free
252	Free
253	Free
254	Free
255	Free

3.20 IP Management - Filtering



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

The screenshot displays the Sangfor IP Management interface. At the top, there are tabs for 'IP Ranges' and 'Local Users'. Below the tabs are 'Refresh' and 'Export' buttons. The main area is titled 'IP Address Pool' and shows details for the '200.200.237.0/24' range. A summary bar indicates: All 256, Normal 3, Long-offline 0, and Free 253. The 'Free' count is highlighted with a red box. Below this is a grid of IP addresses from 0 to 255. A tooltip for IP 200.200.237.67 shows it is 'Free'. A legend at the top right of the grid defines the status colors: Normal (blue), Long-offline (orange), and Free (light blue).

IP Address	Status
0	Free
1	Free
2	Free
3	Free
4	Free
5	Free
6	Free
7	Free
8	Free
9	Free
10	Free
11	Free
12	Free
13	Free
14	Free
15	Free
16	Free
17	Free
18	Free
19	Free
20	Free
21	Free
22	Free
23	Free
24	Free
25	Free
26	Free
27	Free
28	Free
29	Free
30	Free
31	Free
32	Free
33	Free
34	Free
35	Free
36	Free
37	Free
38	Free
39	Free
40	Free
41	Free
42	Free
43	Free
44	Free
45	Free
46	Free
47	Free
48	Free
49	Free
50	Free
51	Free
52	Free
53	Free
54	Free
55	Free
56	Free
57	Free
58	Free
59	Free
60	Free
61	Free
62	Free
63	Free
64	Free
65	Free
66	Free
67	Free
68	Free
69	Free
70	Free
71	Free
72	Free
73	Free
74	Free
75	Free
76	Free
77	Free
78	Free
79	Free
80	Free
81	Free
82	Free
83	Free
84	Free
85	Free
86	Free
87	Free
88	Free
89	Free
90	Free
91	Free
92	Free
93	Free
94	Free
95	Free
96	Free
97	Free
98	Free
99	Free
100	Free
101	Free
102	Free
103	Free
104	Free
105	Free
106	Free
107	Free
108	Free
109	Free
110	Free
111	Free
112	Free
113	Free
114	Free
115	Free
116	Free
117	Free
118	Free
119	Free
120	Free
121	Free
122	Free
123	Free
124	Free
125	Free
126	Free
127	Free
128	Free
129	Free
130	Free
131	Free
132	Free
133	Free
134	Free
135	Free
136	Free
137	Free
138	Free
139	Free
140	Free
141	Free
142	Free
143	Free
144	Free
145	Free
146	Free
147	Free
148	Free
149	Free
150	Free
151	Free
152	Free
153	Free
154	Free
155	Free
156	Free
157	Free
158	Free
159	Free
160	Free
161	Free
162	Free
163	Free
164	Free
165	Free
166	Free
167	Free
168	Free
169	Free
170	Free
171	Free
172	Free
173	Free
174	Free
175	Free
176	Free
177	Free
178	Free
179	Free
180	Free
181	Free
182	Free
183	Free
184	Free
185	Free
186	Free
187	Free
188	Free
189	Free
190	Free
191	Free
192	Free
193	Free
194	Free
195	Free
196	Free
197	Free
198	Free
199	Free
200	Free
201	Free
202	Free
203	Free
204	Free
205	Free
206	Free
207	Free
208	Free
209	Free
210	Free
211	Free
212	Free
213	Free
214	Free
215	Free
216	Free
217	Free
218	Free
219	Free
220	Free
221	Free
222	Free
223	Free
224	Free
225	Free
226	Free
227	Free
228	Free
229	Free
230	Free
231	Free
232	Free
233	Free
234	Free
235	Free
236	Free
237	Free
238	Free
239	Free
240	Free
241	Free
242	Free
243	Free
244	Free
245	Free
246	Free
247	Free
248	Free
249	Free
250	Free
251	Free
252	Free
253	Free
254	Free
255	Free

3.21 IP Management - Export



IP address management, export IP address segments.

The screenshot shows the IP Management interface with the 'Export' button highlighted in red. A 'Select IP Ranges' dialog box is open, showing a tree view of IP ranges. The 'RD (200.200.0.52/24)' range is selected and highlighted in blue. The 'Export' button in the dialog is also highlighted in red.

Available:

- All
- Operation teams
- Fitz teams
- RD (200.200.0.52/24)
- Auto Discovered
 - 200.200.5.0/24
 - 200.200.65.0/24
 - 200.200.84.0/24

Selected:

- All/Operation teams
- All/Fitz teams
- All/RD (200.200.0.52/24)

Buttons: Export, Cancel

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.

Summary


Status: **Activated** [Manual Update](#)

Type: Official

Software Version: IAG13.0.15: 

Gateway ID: 

User: 

Time Activated: 

Function Licenses



Device License

Licensed Modules:

1. Device Status
2. Virtual Lines
3. DNS Proxy

...

Max WAN Lines: 10

Branch VPN Sites: 10

Expiration Date: 2022-06-09



Endpoint Security License

Licensed Modules:

1. Endpoint Security Detection
2. Endpoint Audit (USB Disk Audit)

...

Expiration Date: 2022-06-09



Multi-Function License

Licensed Modules:

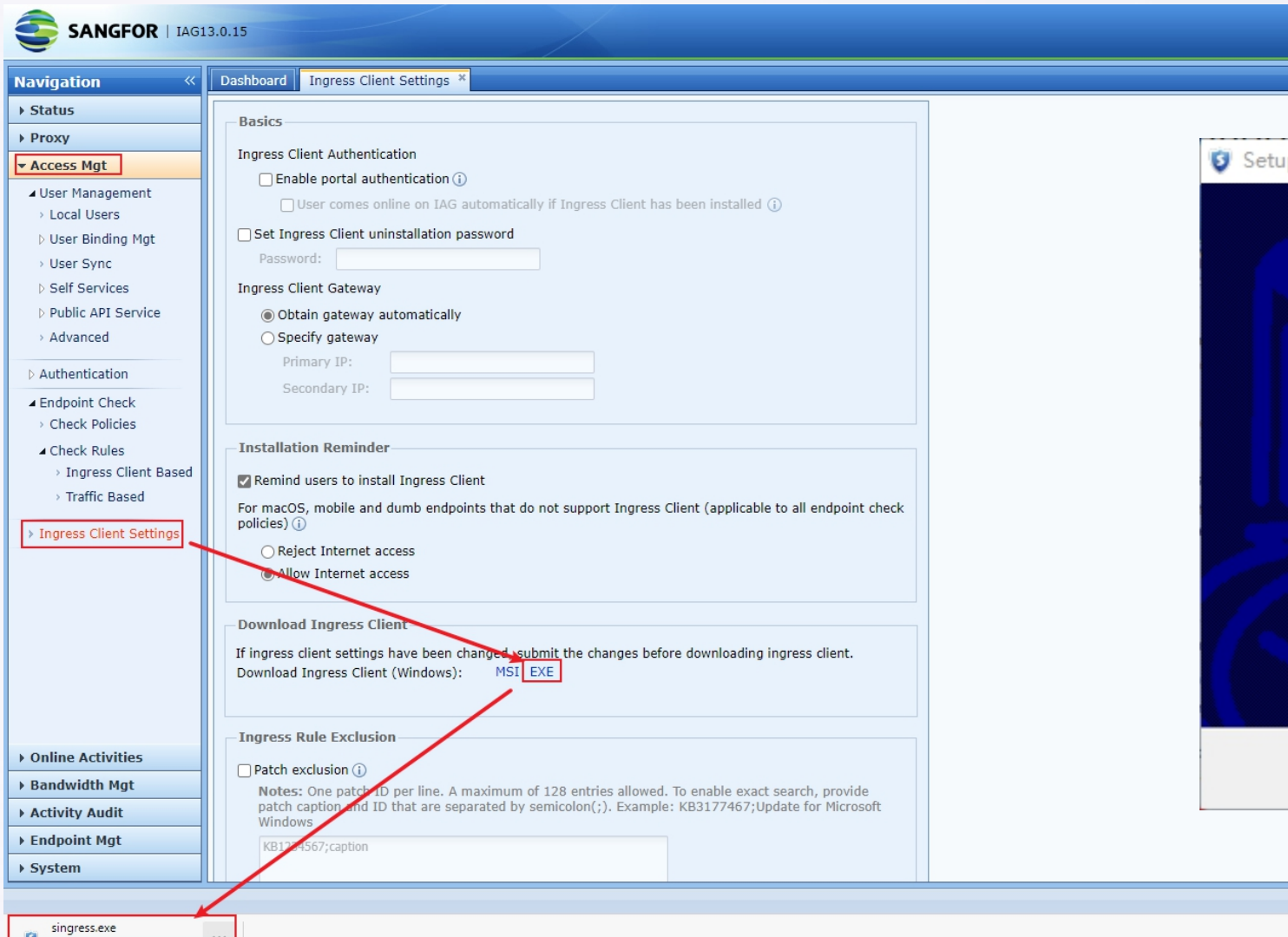
1. Access Mgt
2. Online Activities
3. Bandwidth Channel

...

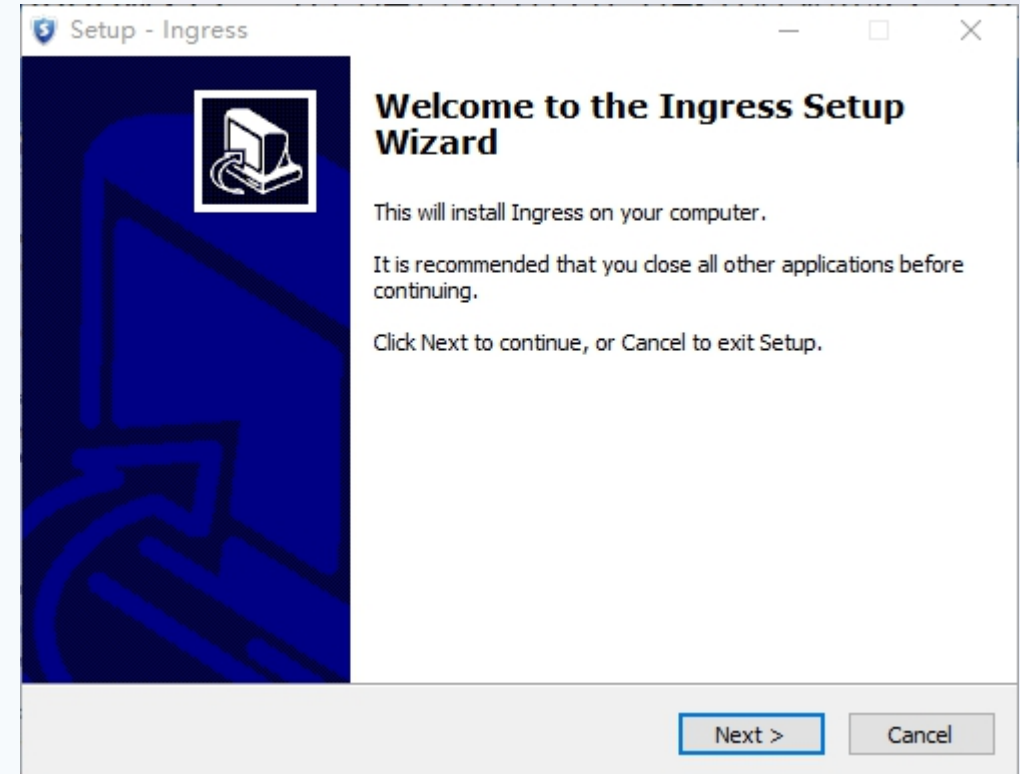
Expiration Date: 2022-06-09

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.



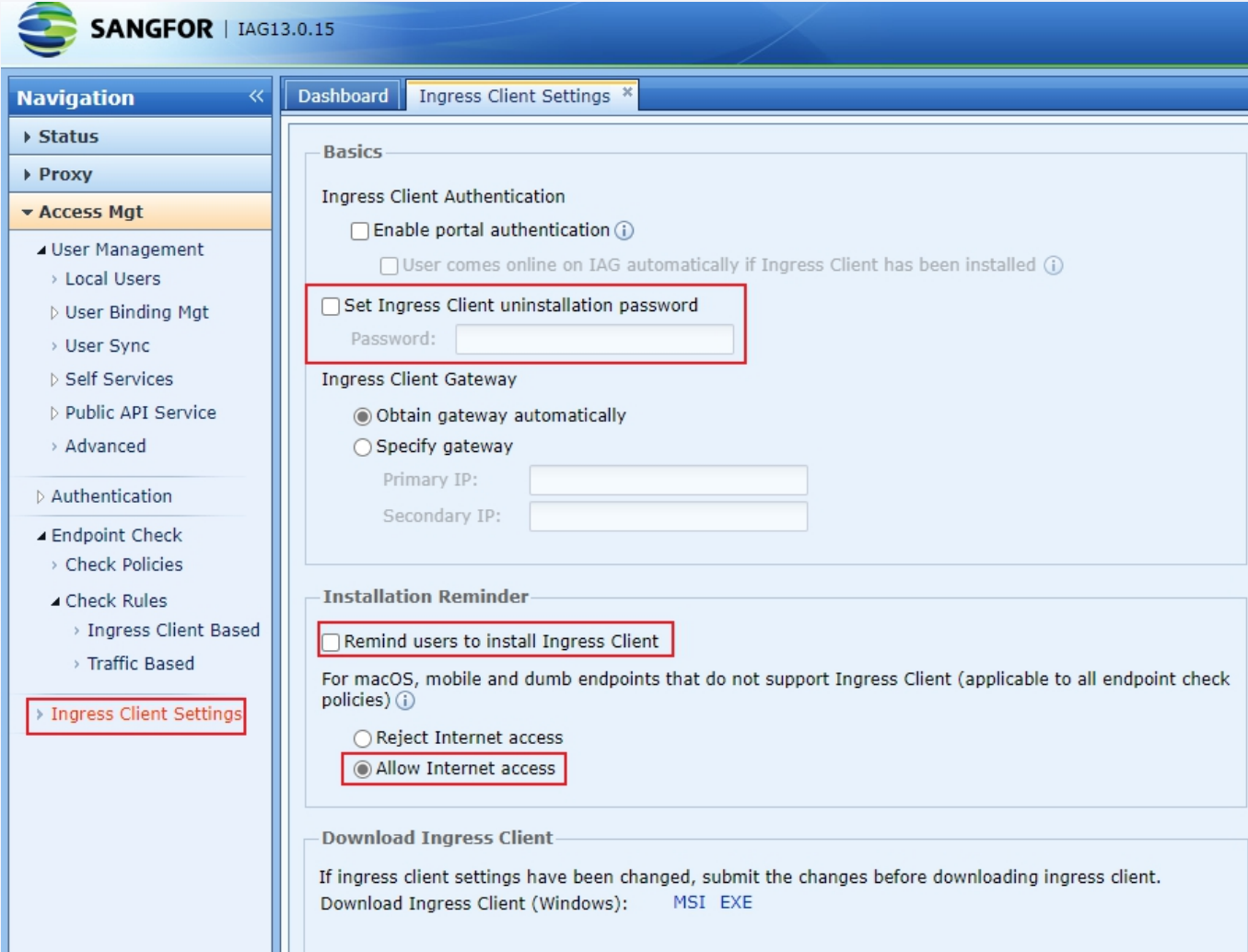
The screenshot displays the SANGFOR IAG13.0.15 web interface. The left navigation pane shows the 'Access Mgt' menu expanded, with 'Ingress Client Settings' selected. The main content area shows the 'Ingress Client Settings' configuration page. Under the 'Download Ingress Client' section, the text 'Download Ingress Client (Windows): MSI EXE' is visible, with 'MSI EXE' highlighted. A red arrow points from this link to a file named 'singress.exe' in the Windows taskbar at the bottom of the screen.



The screenshot shows the 'Setup - Ingress' window. The title bar reads 'Setup - Ingress'. The main content area contains the following text: 'Welcome to the Ingress Setup Wizard', 'This will install Ingress on your computer.', 'It is recommended that you close all other applications before continuing.', and 'Click Next to continue, or Cancel to exit Setup.' At the bottom right, there are two buttons: 'Next >' and 'Cancel'. The 'Next >' button is highlighted with a blue border.

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.



SANGFOR | IAG13.0.15

Navigation << Dashboard Ingress Client Settings *

- ▶ Status
- ▶ Proxy
- ▼ Access Mgt
 - ▲ User Management
 - ▶ Local Users
 - ▶ User Binding Mgt
 - ▶ User Sync
 - ▶ Self Services
 - ▶ Public API Service
 - ▶ Advanced
 - ▶ Authentication
 - ▲ Endpoint Check
 - ▶ Check Policies
 - ▲ Check Rules
 - ▶ Ingress Client Based
 - ▶ Traffic Based
 - ▶ Ingress Client Settings

Basics

Ingress Client Authentication

- Enable portal authentication ⓘ
- User comes online on IAG automatically if Ingress Client has been installed ⓘ
- Set Ingress Client uninstallation password
 - Password:

Ingress Client Gateway

- Obtain gateway automatically
- Specify gateway
 - Primary IP:
 - Secondary IP:

Installation Reminder

- Remind users to install Ingress Client

For macOS, mobile and dumb endpoints that do not support Ingress Client (applicable to all endpoint check policies) ⓘ

- Reject Internet access
- Allow Internet access

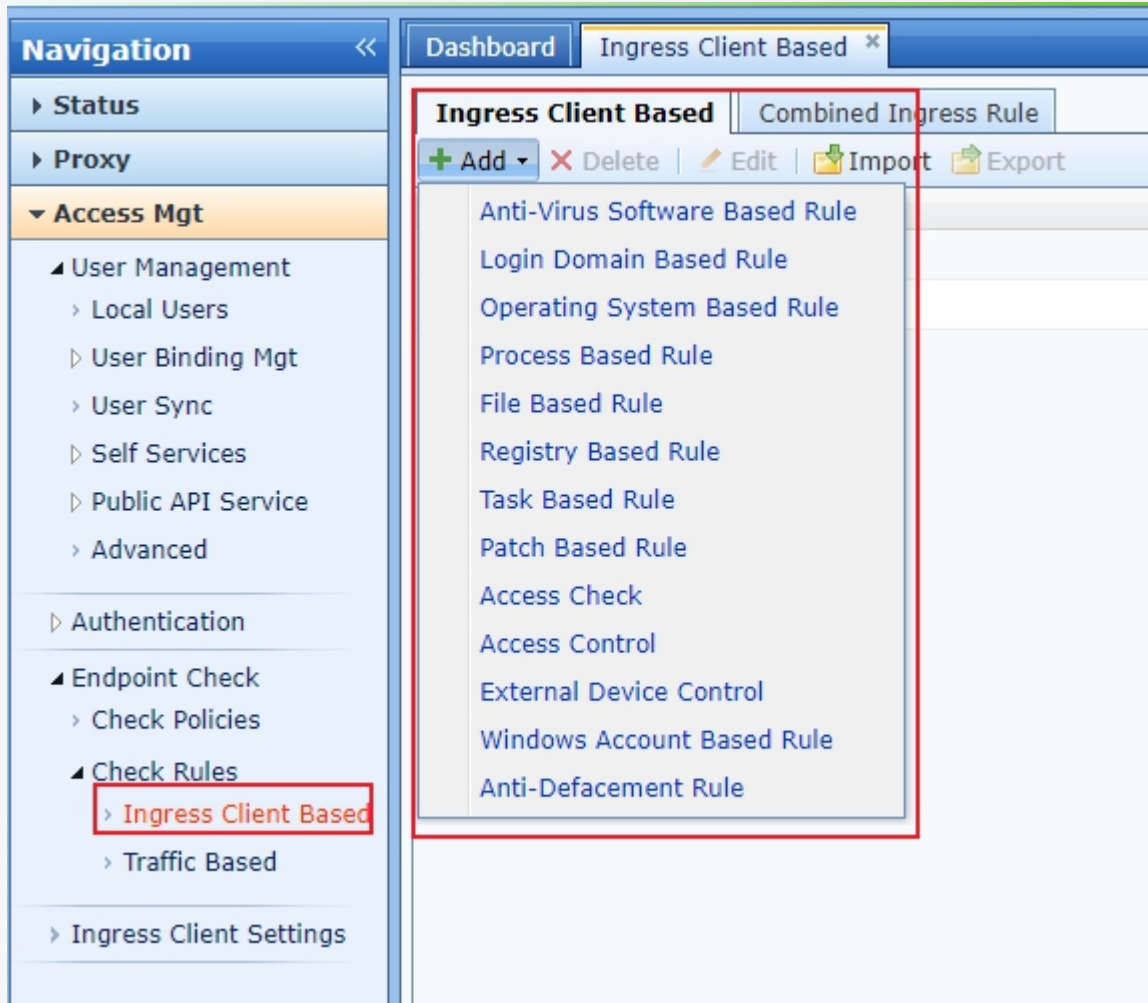
Download Ingress Client

If ingress client settings have been changed, submit the changes before downloading ingress client.

Download Ingress Client (Windows): [MSI](#) [EXE](#)

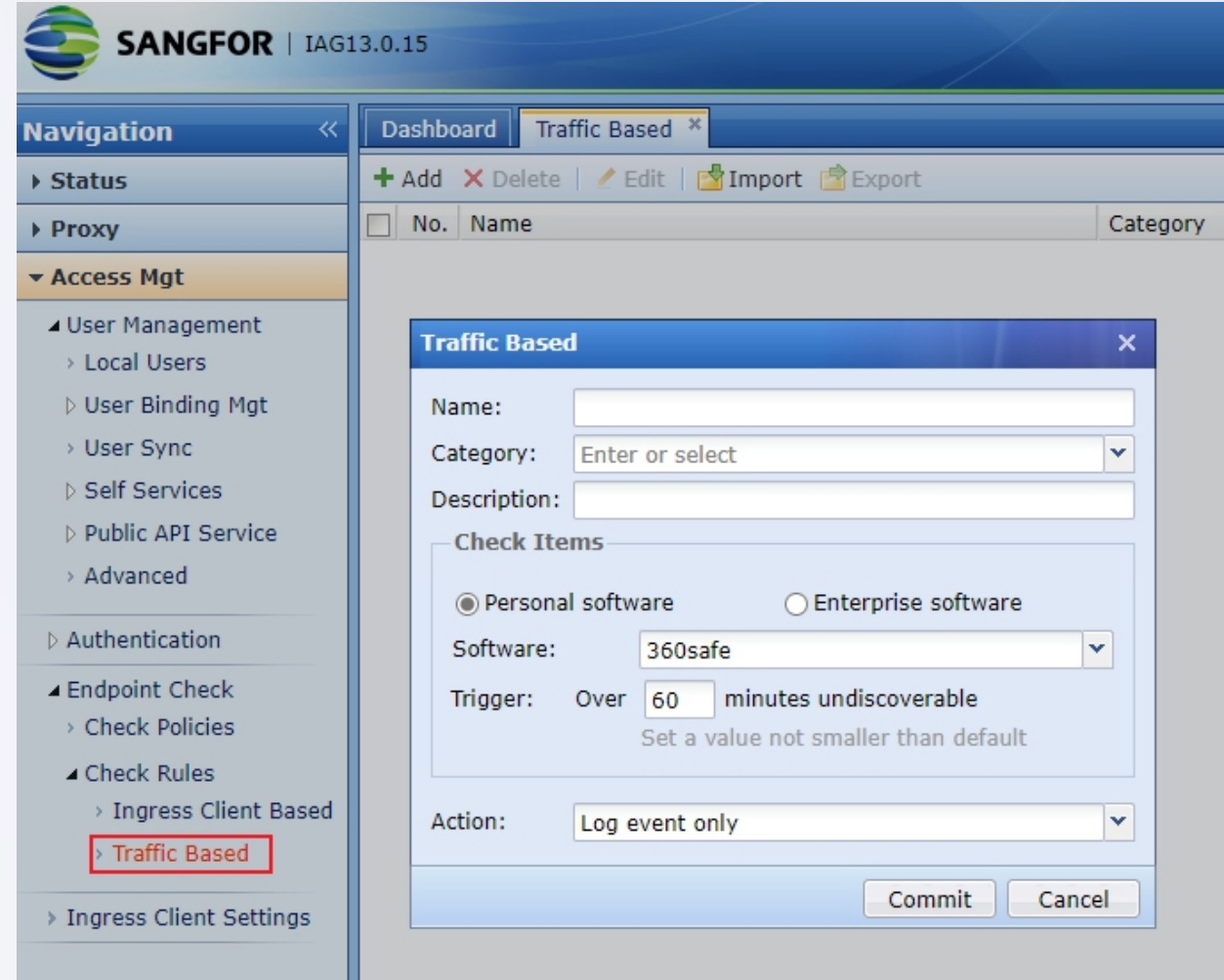
4.3 Checking Rule Description

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



The screenshot shows the Sangfor IAG13.0.15 interface. The left navigation pane is expanded to 'Access Mgt' > 'Check Rules' > 'Ingress Client Based', which is highlighted with a red box. The main content area is titled 'Ingress Client Based' and shows a list of rule types. A dropdown menu is open, listing the following rule categories:

- Anti-Virus Software Based Rule
- Login Domain Based Rule
- Operating System Based Rule
- Process Based Rule
- File Based Rule
- Registry Based Rule
- Task Based Rule
- Patch Based Rule
- Access Check
- Access Control
- External Device Control
- Windows Account Based Rule
- Anti-Defacement Rule



The screenshot shows the Sangfor IAG13.0.15 interface. The left navigation pane is expanded to 'Access Mgt' > 'Endpoint Check' > 'Check Rules' > 'Traffic Based', which is highlighted with a red box. The main content area is titled 'Traffic Based' and shows the configuration form for a 'Traffic Based' rule.

Traffic Based

Name:

Category:

Description:

Check Items

Personal software Enterprise software

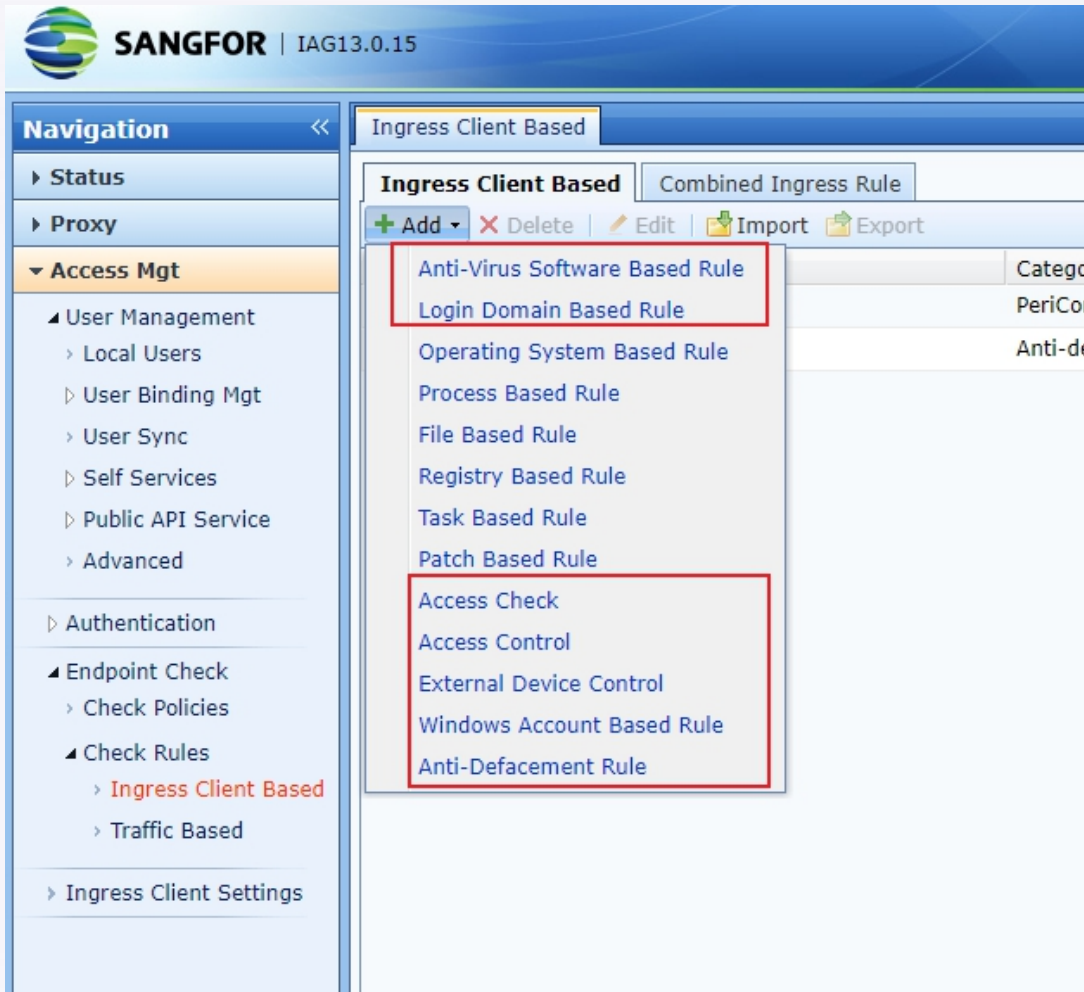
Software:

Trigger: Over minutes undiscoverable
Set a value not smaller than default

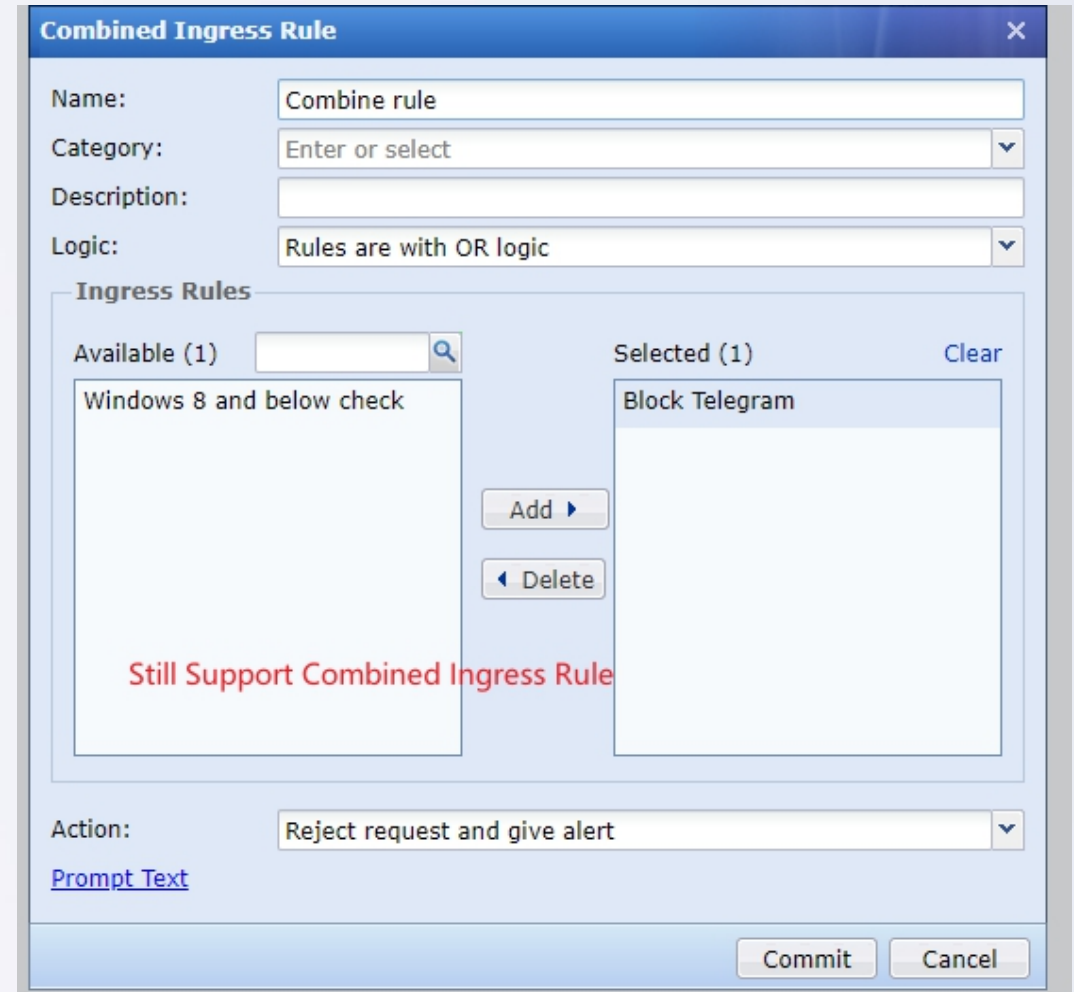
Action:

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.



The screenshot shows the SANGFOR IAG13.0.15 web interface. The left sidebar contains a navigation menu with sections: Status, Proxy, Access Mgt (expanded), Authentication, Endpoint Check, and Check Rules. Under Check Rules, 'Ingress Client Based' is selected. The main content area shows a tabbed interface with 'Ingress Client Based' and 'Combined Ingress Rule'. A dropdown menu is open under the 'Add' button, listing various rule types: Anti-Virus Software Based Rule, Login Domain Based Rule, Operating System Based Rule, Process Based Rule, File Based Rule, Registry Based Rule, Task Based Rule, Patch Based Rule, Access Check, Access Control, External Device Control, Windows Account Based Rule, and Anti-Defacement Rule. The first two and the last four items are highlighted with red boxes.



The screenshot shows the 'Combined Ingress Rule' configuration dialog box. It has the following fields and options:

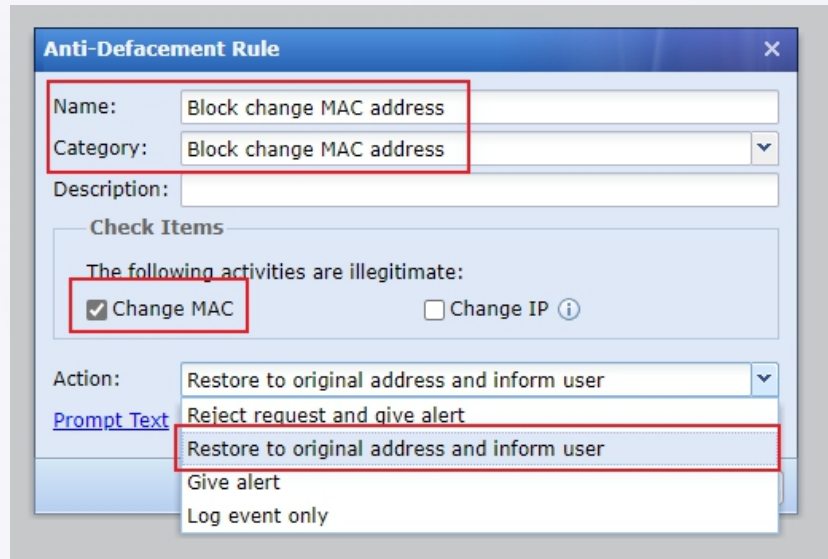
- Name: Combine rule
- Category: Enter or select
- Description: (empty)
- Logic: Rules are with OR logic
- Ingress Rules section:
 - Available (1): Windows 8 and below check
 - Selected (1): Block Telegram
 - Buttons: Add, Delete
- Action: Reject request and give alert
- Prompt Text: (empty)
- Buttons: Commit, Cancel

Red text at the bottom of the dialog reads: **Still Support Combined Ingress Rule**

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



Anti-Defacement Rule

Name: Block change MAC address
 Category: Block change MAC address

Description:

Check Items

The following activities are illegitimate:

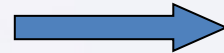
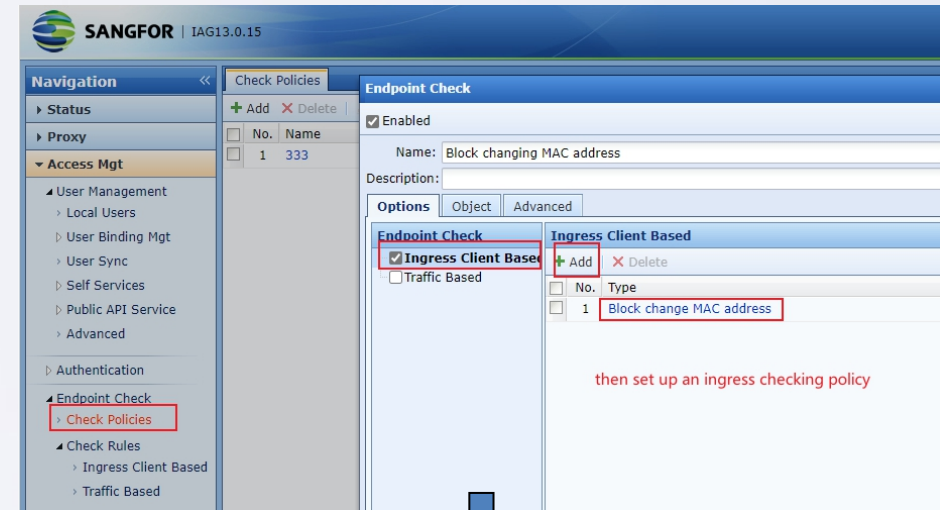
Change MAC Change IP

Action: Restore to original address and inform user

Prompt Text: Reject request and give alert

Restore to original address and inform user
 Give alert
 Log event only

Set ingress check rule

SANGFOR | IAG13.0.15

Navigation: Check Policies

Endpoint Check

Enabled

Name: Block changing MAC address

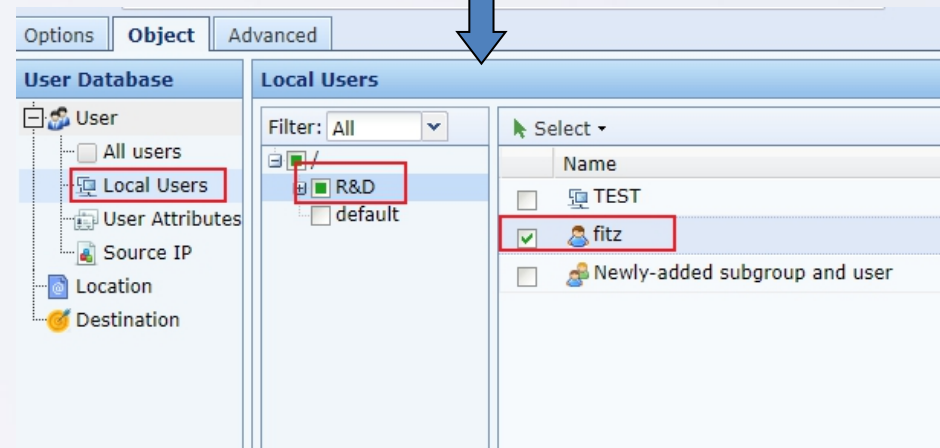
Description:

Options: Object Advanced

Ingress Client Based

No.	Type
1	Block change MAC address

then set up an ingress checking policy

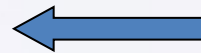
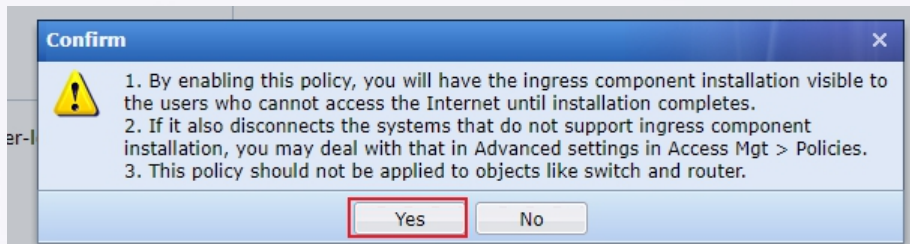
Options: Object Advanced

User Database

Local Users

Filter: All

Name
<input type="checkbox"/> TEST
<input checked="" type="checkbox"/> fitz
<input type="checkbox"/> Newly-added subgroup and user

Confirm

1. By enabling this policy, you will have the ingress component installation visible to the users who cannot access the Internet until installation completes.

2. If it also disconnects the systems that do not support ingress component installation, you may deal with that in Advanced settings in Access Mgt > Policies.

3. This policy should not be applied to objects like switch and router.

Yes No

4.6 Ingress Client Check Results

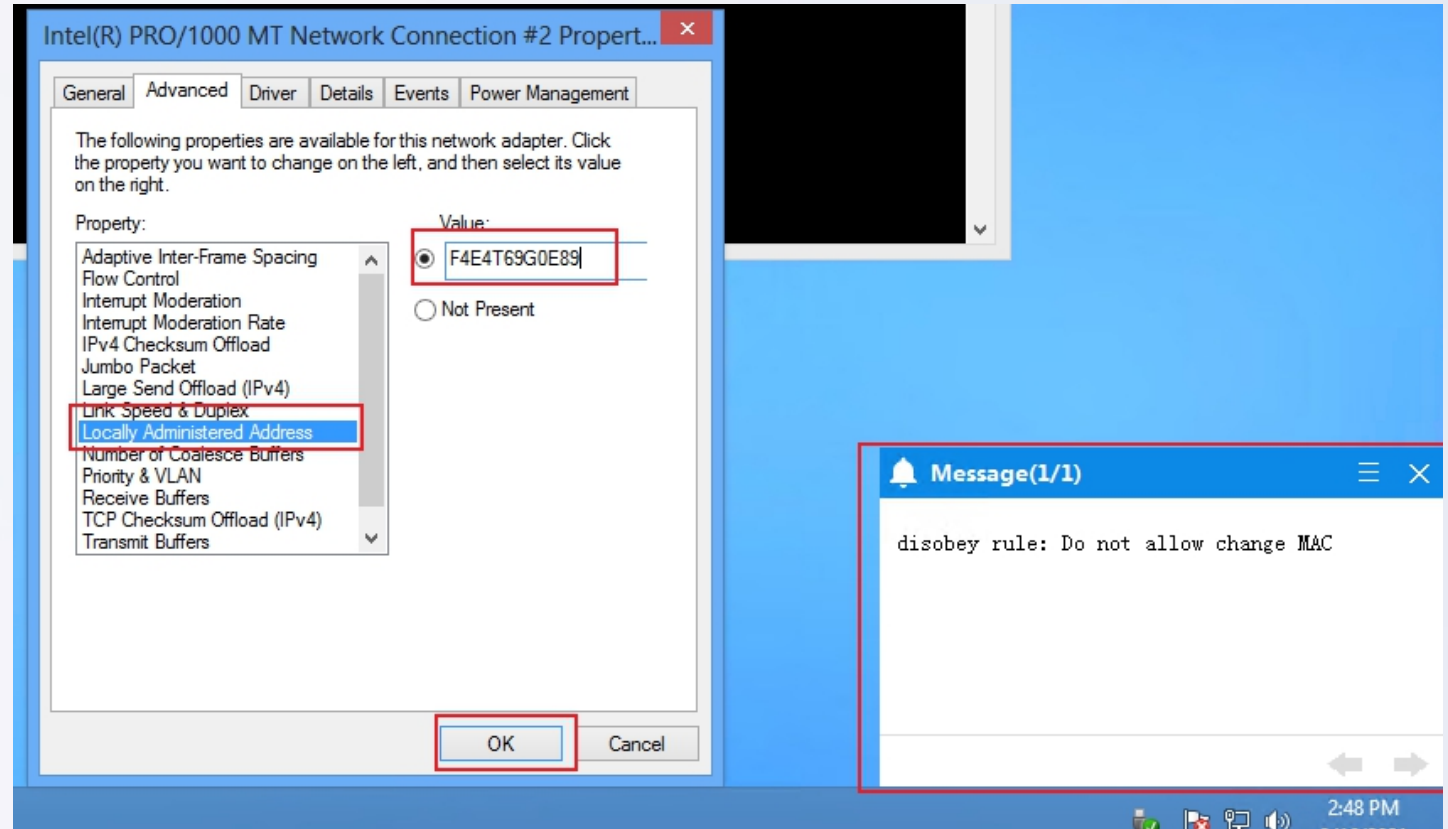
We tried to modify the MAC address on Fitz's computer, and we found that the modification failed, and we also received a prompt.

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

Details

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](#)



The screenshot shows a Windows network adapter properties window for an Intel(R) PRO/1000 MT Network Connection #2. The 'Advanced' tab is selected, and the 'Locally Administered Address' property is highlighted in the list. The value 'F4E4T69G0E89' is entered in the 'Value' field. A system message box is overlaid on the bottom right, displaying the text 'disobey rule: Do not allow change MAC'.

Intel(R) PRO/1000 MT Network Connection #2 Propert... x

General Advanced Driver Details Events Power Management

The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property: Value:

- F4E4T69G0E89
- Not Present

Adaptive Inter-Frame Spacing
Flow Control
Interrupt Moderation
Interrupt Moderation Rate
IPv4 Checksum Offload
Jumbo Packet
Large Send Offload (IPv4)
Link Speed & Duplex
Locally Administered Address
Number of Coalesce Buffers
Priority & VLAN
Receive Buffers
TCP Checksum Offload (IPv4)
Transmit Buffers

OK Cancel

Message(1/1)

disobey rule: Do not allow change MAC

2:48 PM

Thanks