SANGFOR | SANGFOR SECURITY | Sangfor IAG

ENDPOINT COMPLIANCE SOLUTION FOR IOT

001101 00 01 100101
01 001101 00 01
001101 00 01 100101
01 00110
0 01 1001 01101 00
01101 00 100101 001
01 00110 0 01 1001
01 00 01 01 00110
01 00110
0 01 100101 001101 0

CONTENTS

Endpoint Security Inspection and Remediation

Inspection

Using a patented network access rules technology (Patent No. ZL200510037455.1), Sangfor IAG checks the security compliance of each employee's endpoint according to organizational policies. Checked items include antivirus software, login domain, operating system version, patch status, registry keys, scheduled tasks, endpoint processes, endpoint file path, endpoint registry, and Windows account rules. Endpoints that do not meet the required security compliance policies will be denied internet access or have restricted access privileges to improve the security and availability of the intranet.

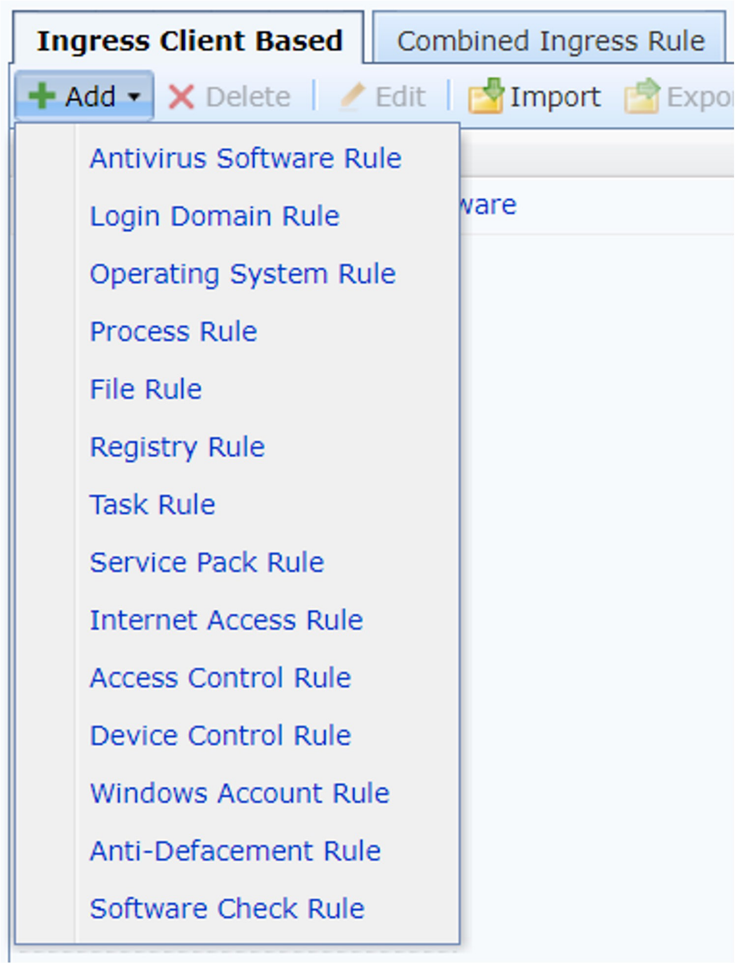
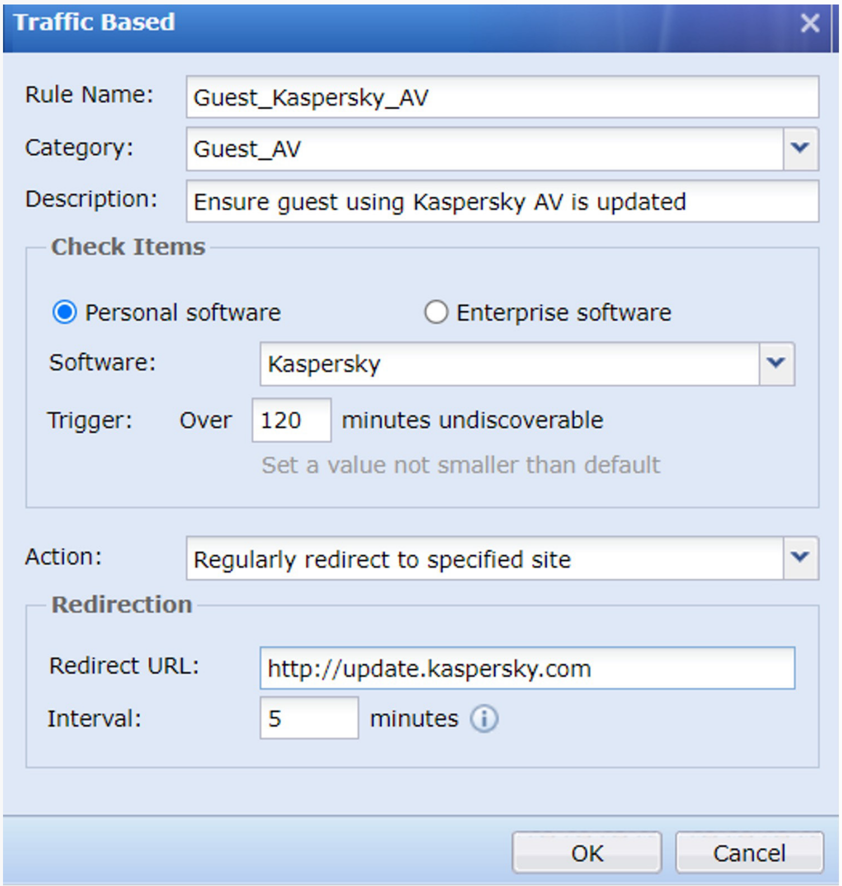


Figure 1: *Ingress Client Based*



Rule Name: Guest_Kaspersky_AV

Category: Guest_AV

Description: Ensure guest using Kaspersky AV is updated

Check Items

● Personal software ○ Enterprise software

Software: Kaspersky

Trigger: Over 120 minutes undiscoverable

Set a value not smaller than default

Action: Regularly redirect to specified site

Redirection

Redirect URL: http://update.kaspersky.com

Interval: 5 minutes

Figure 2: Traffic Based

Remediation

Sangfor IAG supports endpoint compliance checking and the isolation and remediation of incompliant endpoints. The built-in endpoint compliance checking strategy includes:

Routine Detection:

- Detects Windows patches according to specified levels or specified patches and reminds users to apply patches.
- Detects insecure registry items; supports automatic deletion of insecure items or prohibits network access and notifies users to repair.
- Detects suspicious files; supports automatic deletion of insecure files or prohibits network access with an alert, and reports to the administrator.

Detects whether specified processes are running; supports automatic process termination or prohibits network access with an alert.

Checks the operating system; prohibits network access with an alert.

Supports custom scheduled tasks; sets the time to execute customer-defined programs and checks the results.

Supports domain log in detection (checks compliance once a PC logs in to any domain account) and specified domain log ins (checks compliance once a PC logs into one of the specified domains with a domain account).

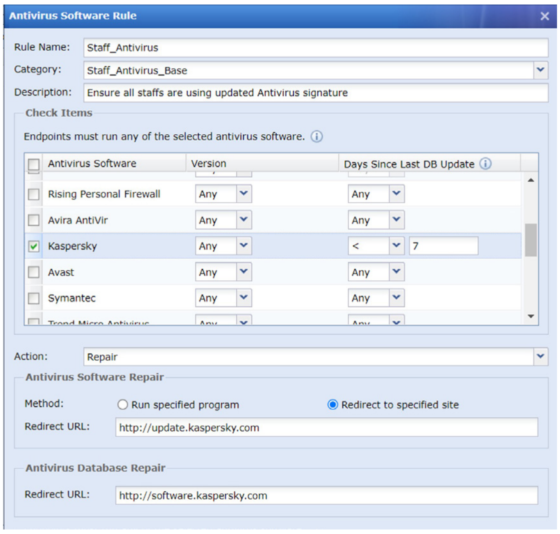
For non-compliant endpoints, four types of remediation processes are supported: prohibiting network access, prompting users, event logging, and restricting user privileges.

Antivirus Software Detection and Remediation

To ensure the security of endpoints accessing the network, Sangfor IAG supports antivirus software detection using a lightweight plug-in or traffic-based clientless detection.

Plug-in detection detects whether any mainstream antivirus software is running on an endpoint and detects the version of the antivirus software. For incompliant endpoints, there are five types of remediation processes: restricting internet access (choice between access privileges or user quotas), prompting users, event logging, restricting user privileges, and running specified programs or redirecting to a remediation page.

Sangfor IAG can detect over 20 mainstream antivirus software, including their running status, software version, virus database update time. Other antivirus software detection strategies can be added in the "process check" section.



Rule Name: Staff_Antivirus

Category: Staff_Antivirus_Base

Description: Ensure all staffs are using updated Antivirus signature

Check Items

Endpoints must run any of the selected antivirus software. ⓘ

□	Antivirus Software	Version	Days Since Last DB Update ⓘ
□	Rising Personal Firewall	Any	Any
□	Avira AntiVir	Any	Any
☑	Kaspersky	Any	< 7
□	Avast	Any	Any
□	Symantec	Any	Any
□	Trend Micro Antivirus	Any	Any

Action: Repair

Antivirus Software Repair

Method: ○ Run specified program ● Redirect to specified site

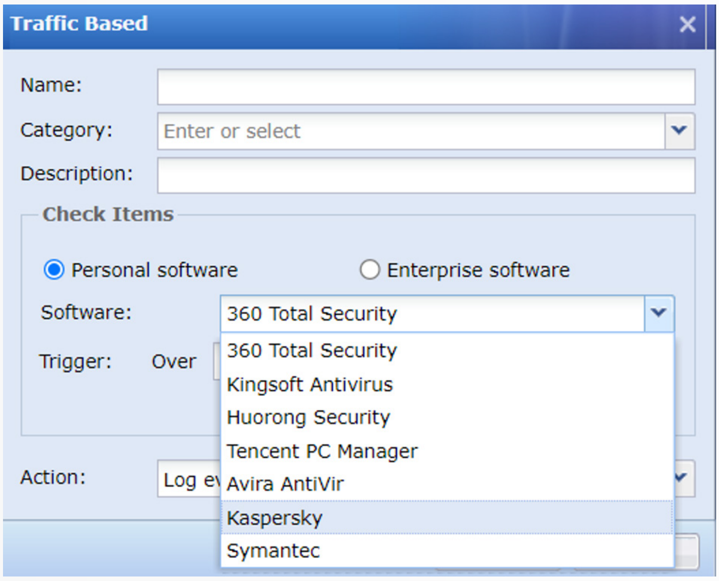
Redirect URL: http://update.kaspersky.com

Antivirus Database Repair

Redirect URL: http://software.kaspersky.com

Figure 3: Anti-Virus Software Based Rule Configuration

Sangfor IAG clientless detection detects the running status of more than 10 mainstream antivirus software through traffic conditions, delivering a lightweight software checking solution for customers. This function is implemented by identifying the heartbeat traffic packets between the antivirus software client and server. Incompliance remediation includes redirecting users to a remediation page and event logging.



Traffic Based

Name:

Category: Enter or select

Description:

Check Items

● Personal software ○ Enterprise software

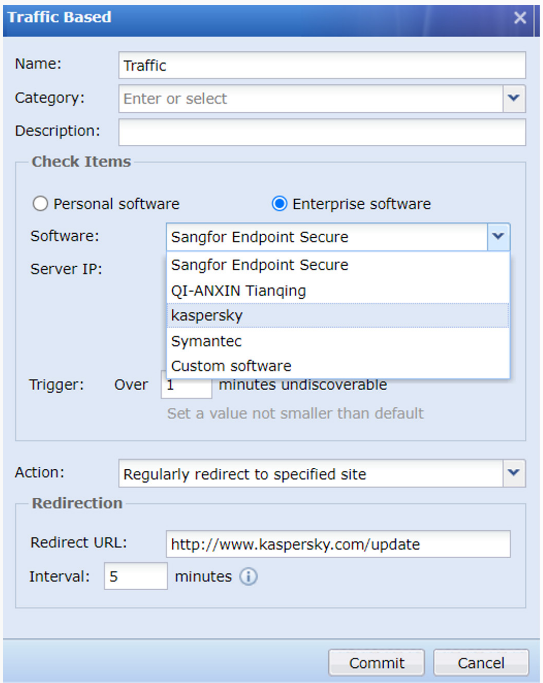
Software: 360 Total Security

- 360 Total Security
- Kingsoft Antivirus
- Huorong Security
- Tencent PC Manager
- Avira AntiVir
- Kaspersky
- Symantec

Trigger: Over

Action: Log ev

Figure 4: Traffic Based Configuration



Traffic Based

Name: Traffic

Category: Enter or select

Description:

Check Items

○ Personal software ● Enterprise software

Software: Sangfor Endpoint Secure

- Sangfor Endpoint Secure
- QI-ANXIN Tianqing
- kaspersky
- Symantec
- Custom software

Server IP:

Trigger: Over 1 minutes undiscoverable

Set a value not smaller than default

Action: Regularly redirect to specified site

Redirection

Redirect URL: http://www.kaspersky.com/update

Interval: 5 minutes

Commit Cancel

Figure 5: Traffic based configuration

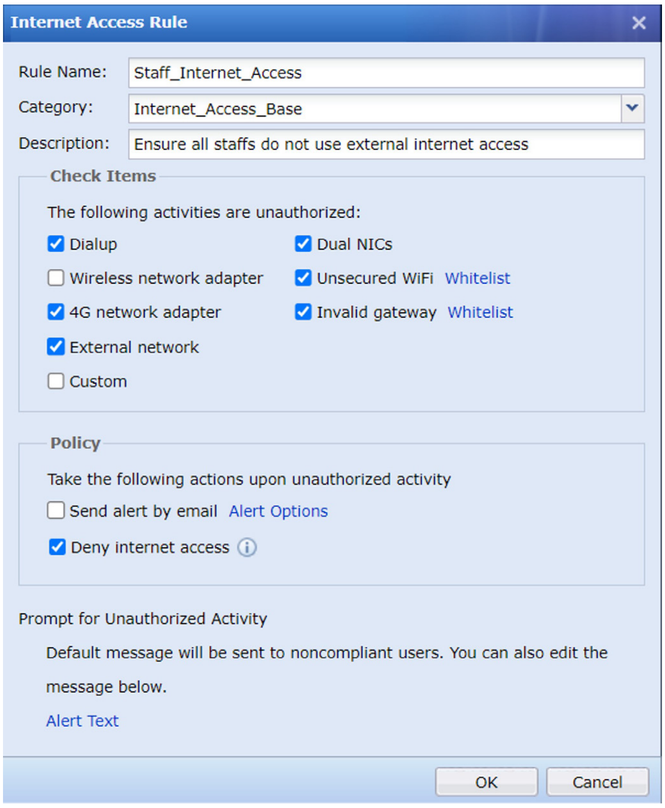
Endpoint Security Control

The number of security incidents is climbing sharply. Intranet disruption and instability directly affect users' network behavior. Sangfor IAG safeguards the gateway's security and strengthens intranet reliability and availability.

Unauthorized Peripheral Device Connection

Apart from securing network access through authentication, another problem that needs to be addressed is the unauthorized connection of peripheral devices. Sangfor IAG protects against the connection of unauthorized peripheral devices through peripheral device inspection and control.

IAG implements peripheral device management from three aspects: peripheral device connection configuration, incompliance remediation, and alerting users. Sangfor IAG provides eight types of checks, including dial-up connection, dual network card, wireless network card, unauthorized Wi-Fi connection, 4G network card, unauthorized gateways, external network connection, and custom peripheral device connection. The access client starts to enforce these checks once the configured policies are issued to it.



Internet Access Rule

Rule Name: Staff_Internet_Access

Category: Internet_Access_Base

Description: Ensure all staffs do not use external internet access

Check Items

The following activities are unauthorized:

☑ Dialup ☑ Dual NICs

□ Wireless network adapter ☑ Unsecured WiFi Whitelist

☑ 4G network adapter ☑ Invalid gateway Whitelist

☑ External network

□ Custom

Policy

Take the following actions upon unauthorized activity

□ Send alert by email Alert Options

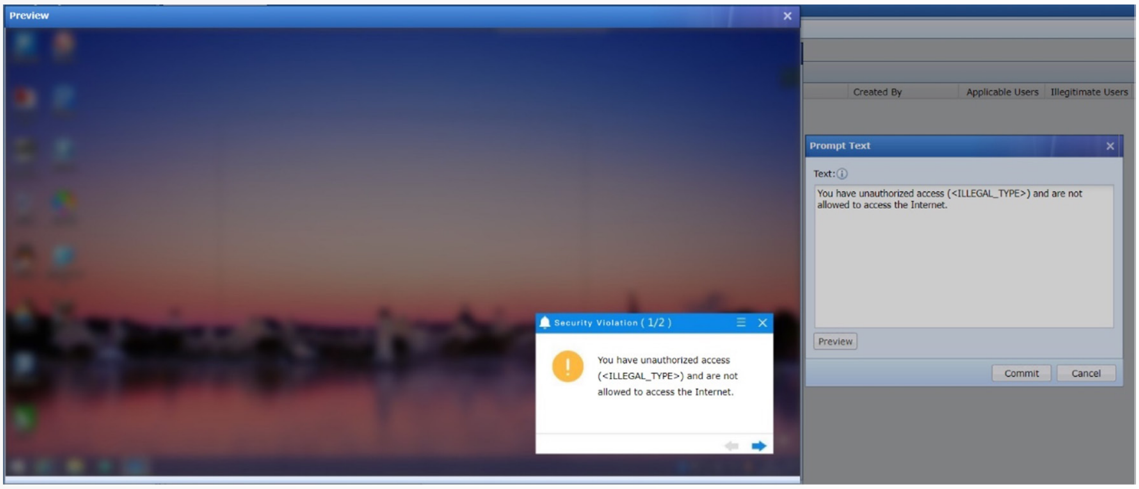
☑ Deny internet access

Prompt for Unauthorized Activity

Default message will be sent to noncompliant users. You can also edit the message below.

Alert Text

Figure 6: *Unauthorized Internet Access Check with prompt text setting*



You have unauthorized access (<ILLEGAL_TYPE>) and are not allowed to access the Internet.

You have unauthorized access (<ILLEGAL_TYPE>) and are not allowed to access the Internet.

Figure 7: Unauthorized Internet Access Check with security violation prompt.

Dial-up Detection

Dial-up connection is completed using the remote access service (RAS). Windows provides a complete set of APIs for RAS. Dial-up behavior is enumerated by calling the API RasEnumConnection. A dial-up behavior number of 0 means that there is no dial-up connection.

Dual Network Card Detection

Network card information is obtained by reading NIC info captured from the Windows system. The presence of multiple network cards is then determined by the MAC or IP address of the network cards.

Wireless Network Card Detection

The number of wireless network cards is determined by the detection of Windows API functions. A number greater than 0 means there is a/are wireless network card(s) on the PC.

4G Network Card Detection

The names (GUID) of all network cards on the host are obtained and matched to their corresponding IDs in the registry. If it is not with USB Wi-Fi adapter, it is a non-USB external network card (including wireless network card i.e., 2/3/4G wireless access). If it starts with USB, determine whether it is a wireless network card i.e., 2/3/4G wireless access.

Unauthorized Wi-Fi Connection Detection

Organizations that use a Wi-Fi whitelist can detect unauthorized Wi-Fi connections. Unauthorized connections are detected through the SSID and MAC addresses. This can help network administrators manage the Wi-Fi connections.

Unauthorized gateway Connection Detection

Configure a gateway whitelist. A local gateway on the whitelist is authorized, otherwise it is unauthorized.

External Network Connection Detection

Using the principle of a ping command: There are five built-in domain names. External connection is detected if one of the domain names is pinged (only one packet is sent each time).

Peripheral device control directly invokes Windows firewall rules to achieve strong control of unauthorized connections and strictly prohibits endpoint PCs from accessing the external network. Peripheral device control can be used in the following two scenarios.

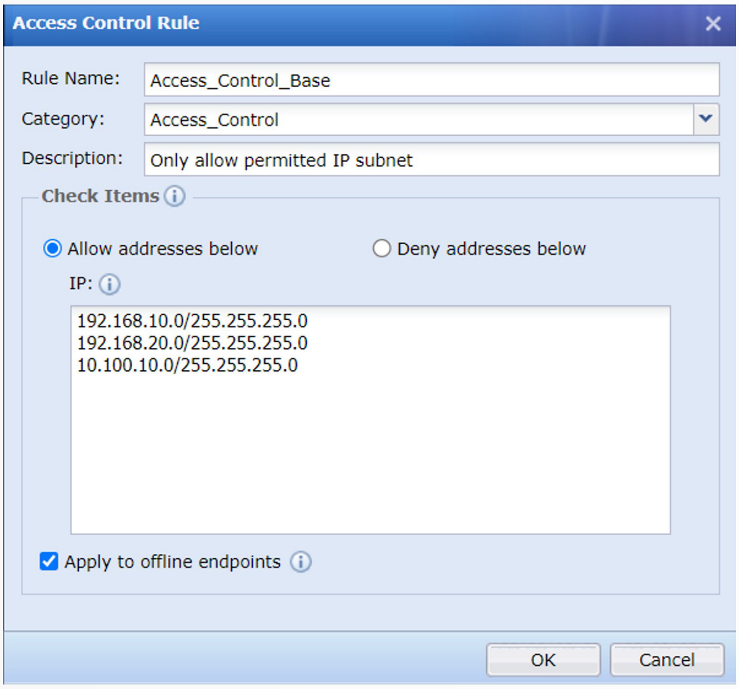
Problems with reporting unauthorized peripheral device connections

When an enterprise installs the security software and turns on the unauthorized peripheral device connection reporting function, all departments and regions will report unauthorized connection alerts.

Some enterprises may consider the number of alerts in a department or region’s performance assessment. Sangfor IAG provides control rules to configure alerts for certain departments or regions. For example, control rules can be configured to control the enormous number of alerts a testing department will inevitably generate during testing to not affect its performance evaluation.

Access Control Restriction

Controls the resources that can be accessed by endpoint PCs on the intranet. Achieves horizontal control in the network, and effectively protects information in the network according to the user's needs.



Access Control Rule

Rule Name: Access_Control_Base

Category: Access_Control

Description: Only allow permitted IP subnet

Check Items

● Allow addresses below ○ Deny addresses below

IP:

```
192.168.10.0/255.255.255.0
192.168.20.0/255.255.255.0
10.100.10.0/255.255.255.0
```

☑ Apply to offline endpoints

Figure 8: *Access Control Configuration*

Peripheral Device Management

Peripheral devices make work more convenient. However, the more peripherals, the more entry points there are for attack and infection. Sangfor IAG mitigates the risk of attack and infection and provides users with a safe and secure network environment.

Configure the inspection rules for peripheral device control, add them to the inspection policy, and issue the inspection policy to the access client. This enables the effective control the following types of peripherals:

Storage Devices
Prohibits endpoints from using portable storage devices, such as USB drives, cell phones, and tablets.

Network devices
Prohibits endpoints from using external network devices, such as mobile data network cards, wireless network cards, network-sharing Bluetooth adapters, and network-sharing functions of cell phones.

Bluetooth devices
Prohibits endpoints from using Bluetooth functions, such as notebooks with their own Bluetooth, Bluetooth adapters, and other related functions.

Cameras

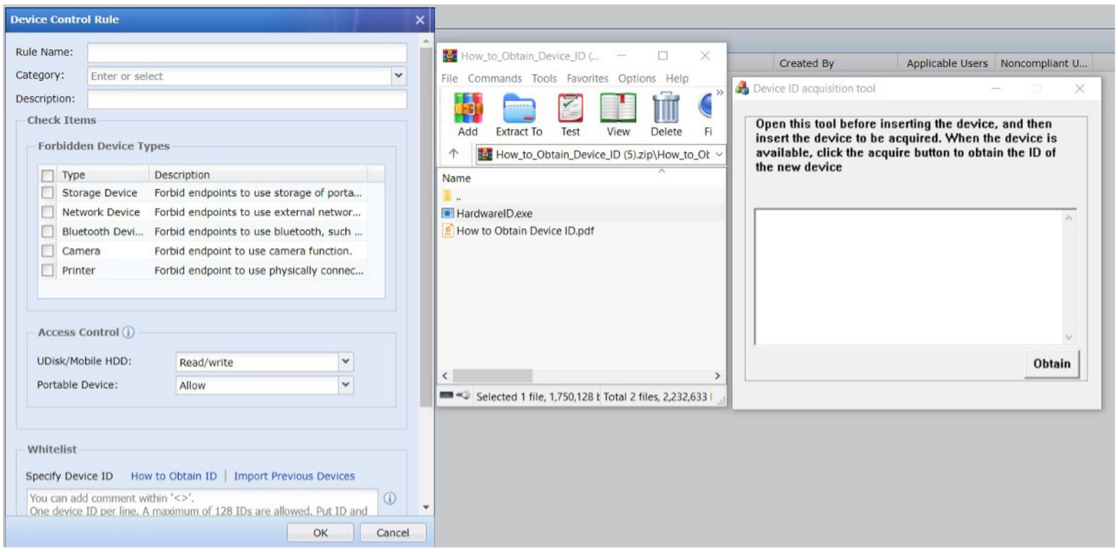
Prohibits endpoints from using their camera and other related functions.

Printers

Prohibits endpoints from using physically connected printers and other related functions.

Other scenarios

Rules can be issued to the access client to disable the reporting of unauthorized connection alerts.



Device Control Rule

Rule Name:

Category: Enter or select

Description:

Check Items

Forbidden Device Types

☐	Type	Description
☐	Storage Device	Forbid endpoints to use storage of porta...
☐	Network Device	Forbid endpoints to use external networ...
☐	Bluetooth Devi...	Forbid endpoints to use bluetooth, such ...
☐	Camera	Forbid endpoint to use camera function.
☐	Printer	Forbid endpoint to use physically connec...

Access Control

UDisk/Mobile HDD: Read/write

Portable Device: Allow

Whitelist

Specify Device ID How to Obtain ID | Import Previous Devices

You can add comment within '<>'.
One device ID per line. A maximum of 128 IDs are allowed. Put ID and

How_to_Obtain_Device_ID (5).zip\How_to_Ot

Name
..
HardwareID.exe
How to Obtain Device ID.pdf

Selected 1 file, 1,750,128 t Total 2 files, 2,232,633 I

Device ID acquisition tool

Open this tool before inserting the device, and then insert the device to be acquired. When the device is available, click the acquire button to obtain the ID of the new device

Figure 9: External Device Configuration and Obtain Hardware ID

Granular Control

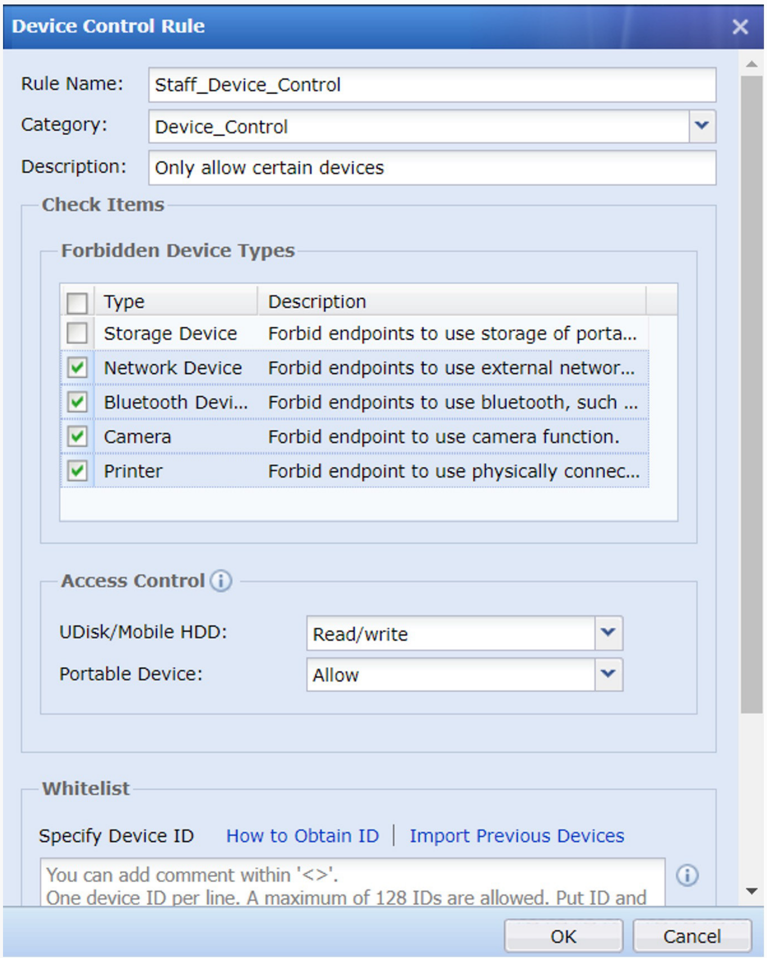
Install the access client on the PC and configure the inspection policy on Sangfor IAG to achieve granular control of portable devices.

Supported actions for portable devices include

1. Allow – Grant full control

2. Block
– Blocks the connection

3. Alert
– Generates an alert on connection



Device Control Rule

Rule Name: Staff_Device_Control

Category: Device_Control

Description: Only allow certain devices

Check Items

Forbidden Device Types

☐	Type	Description
☐	Storage Device	Forbid endpoints to use storage of porta...
☑	Network Device	Forbid endpoints to use external networ...
☑	Bluetooth Devi...	Forbid endpoints to use bluetooth, such ...
☑	Camera	Forbid endpoint to use camera function.
☑	Printer	Forbid endpoint to use physically connec...

Access Control ⓘ

UDisk/Mobile HDD: Read/write

Portable Device: Allow

Whitelist

Specify Device ID   How to Obtain ID | Import Previous Devices

You can add comment within '<>'.
One device ID per line. A maximum of 128 IDs are allowed. Put ID and

Figure 10: External Device Control Configuration

Policy Enforcement Results

When the peripheral device rules are added to the inspection policy and issued to the endpoint, the access client regularly checks whether a new policy has been issued and implements it. When a USB drive that is not listed on the device whitelist is inserted into an endpoint PC, the access client will block it according to the policy.

To determine that blocking was enforced by the access client and not due to hardware failure on the endpoint or the failure of the USB drive, perform the following steps:

Right-click My Computer --> Manage --> System Tools --> Device Manager --> Other Devices. If the prompt "The system policy prohibits the installation of this device, please contact your administrator" appears, the device installation failed due to a violation of the system policy, not a hardware or system failure.

Technical Principle

The access policy is issued by Sangfor IAG, and the access client executes the corresponding system script. This is equivalent to manually setting the system group policy and takes effect under the Windows system (supported in Win 7 and above).

Device ID Generation

One of the goals of Sangfor's products is to provide users with a secure network, but not at the cost of convenience. A blanket ban on peripheral devices would cause users a lot of inconvenience. Sangfor IAG provides a peripherals whitelist to allow users to use secure and trusted peripherals. Users can still enjoy the convenience of peripheral devices listed on the whitelist while ensuring a secure network environment.

To use the peripherals whitelist, download the ID generation tool from Sangfor IAG using the steps shown in the image below. Administrators need to use this tool to generate a device ID to configure the whitelist. Please refer to Figure 9: External Device Configuration and Obtain Hardware ID

Endpoint Security Configuration

This part will focus on the manual gateway configuration function. This function was developed to improve the implementation of the inspection policy based on actual needs in users' usage scenarios. This function can be used in the following scenarios:

Ensures that PCs can find the gateway

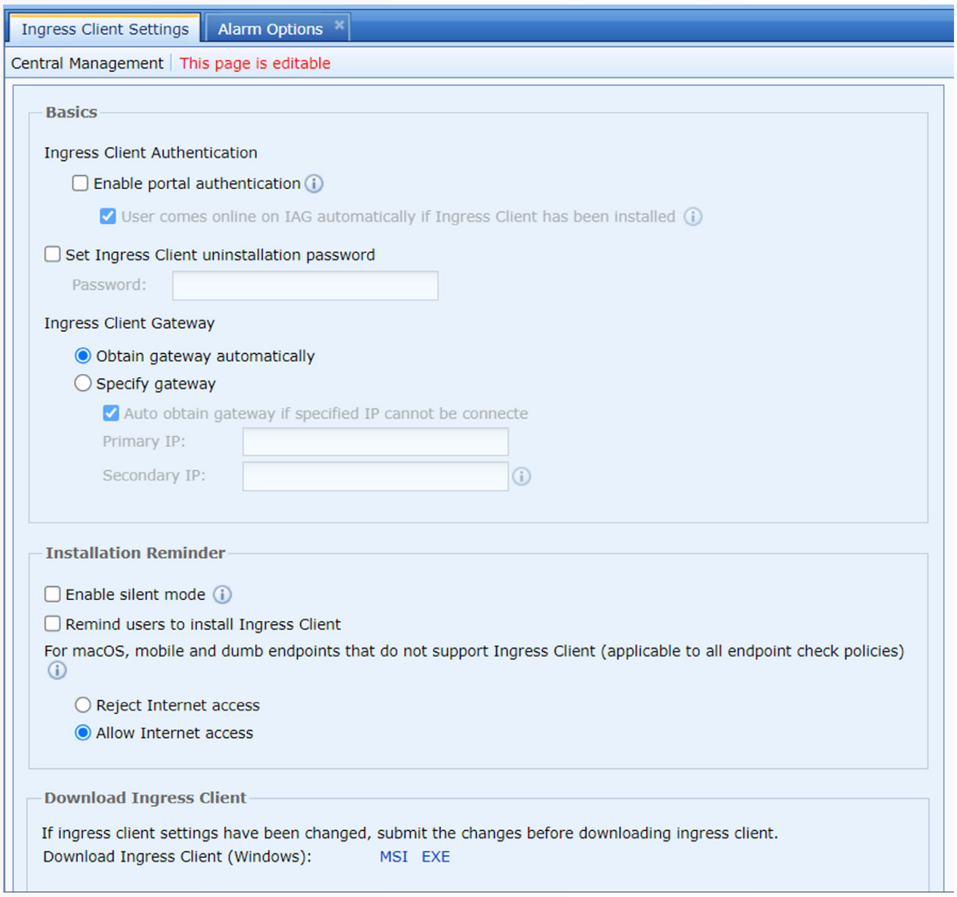
The access client automatically finds the gateway by default, which is a complex, time-consuming process and not necessarily accurate. If a gateway is designated, the access client will be able to accurately send business requests to the designated gateway.

Prevents incorrect gateway discovery when there are multiple products on the intranet

Sangfor IAG customers may also be users of previous Sangfor products. During a default automatic gateway search, the previous product may be found as the gateway, resulting in incorrect service requests.

Suggestion

Use the manual gateway configuration function to ensure the correct gateway is found.



Central Management | This page is editable

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

☑ Auto obtain gateway if specified IP cannot be connecte

Primary IP:

Secondary IP: ⓘ

Installation Reminder

□ Enable silent mode ⓘ

□ 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.

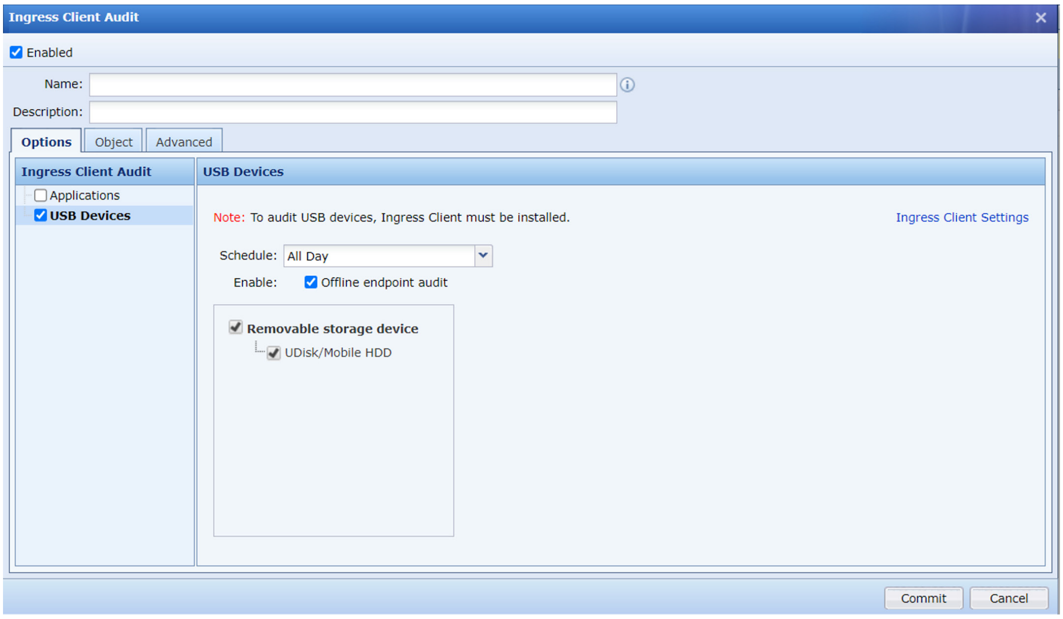
Download Ingress Client (Windows): MSI EXE

Figure 11: *Ingress Client Settings*

Offline Auditing

To meet the auditing requirements of mobile office and remote office scenarios, Sangfor IAG supports offline auditing when the access client is disconnected from the device. USB drive auditing can be implemented if employees take their laptops home.

The technical principles of offline auditing: When connection to the gateway fails or the heartbeat packet is not received within 2 minutes, offline mode will be switched on. If the offline audit switch is turned on in the cached policy file, file operations on USB drives will continue to be recorded: backs up the files to be audited, records the behavior in the local cache, supports a maximum cache size of 1GB, reports to IAG on the next connection, and supports auditing when the endpoint is offline.



☑ Enabled

Name:

Description:

□ Applications

☑ USB Devices

Note: To audit USB devices, Ingress Client must be installed.

Schedule: All Day

Enable: ☑ Offline endpoint audit

☑ Removable storage device

☑ UDisk/Mobile HDD

Figure 12: Ingress Client offline audit setting

Endpoint Asset Discovery

Company IT administrators often want an overview of the company's intranet to check the deployment and usage of endpoint devices, IP allocation, and the distribution and usage of network devices (switches, routers, firewalls, etc.). Sangfor IAG allows administrators to always keep track of network resource allocation and usage, and provide extensive, first-hand data for network optimization.

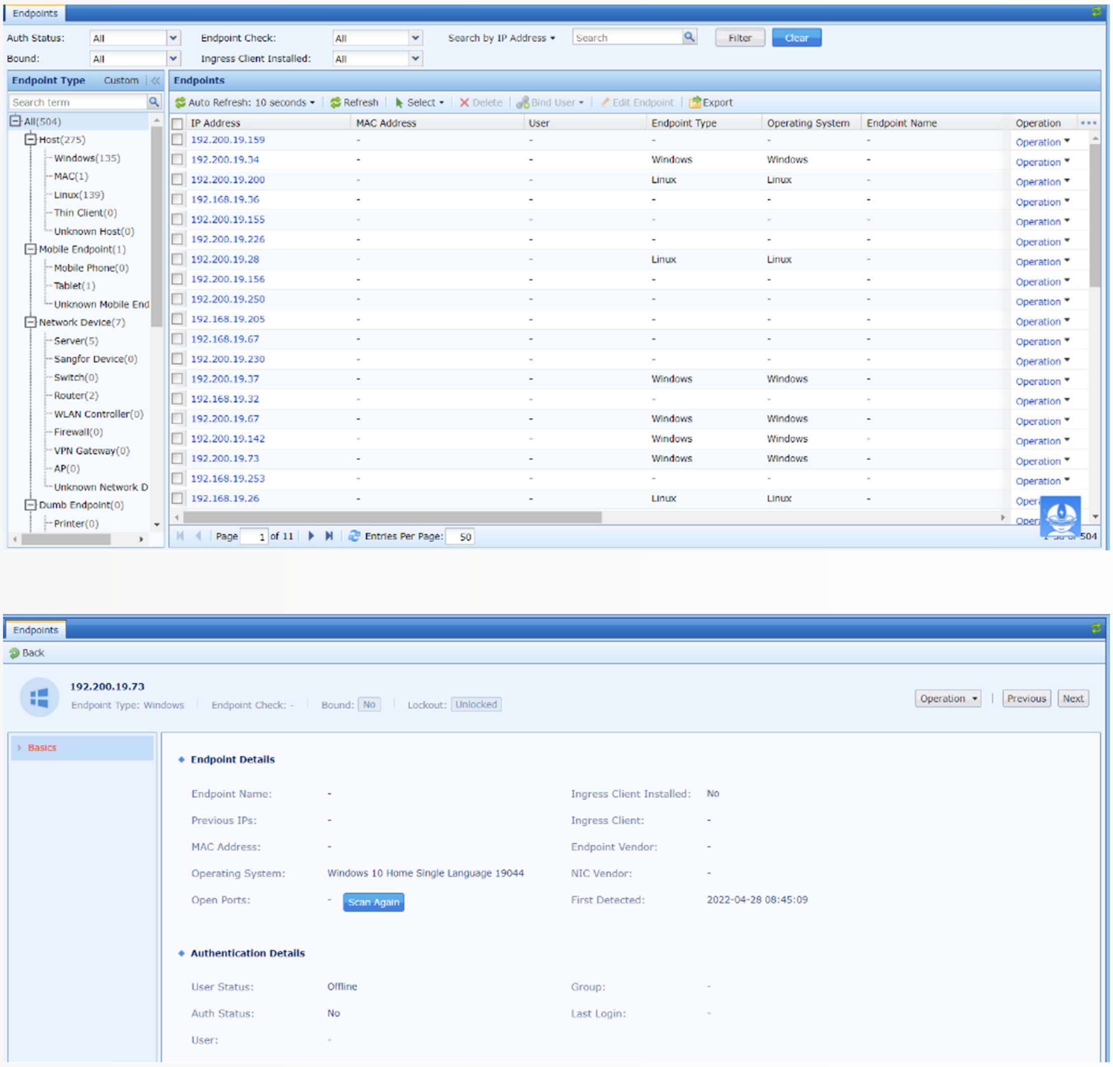
Endpoint Discovery

Sangfor IAG can scan specified network segments on the intranet for endpoint devices and identify the type of device. The endpoint fingerprint information (device type, IP, MAC, operating system, online status, open ports, manufacturer, and other basic details) gets mirrored to Sangfor IAG and is analyzed.

Sangfor IAG can identify an endpoint’s characteristics through protocols such as TCP, DHCP, ARP, HTTP (HTTPS), and DICOM. Discovery and identification rates under real environment testing are much higher than those of other Chinese manufacturers.

Sangfor IAG supports the discovery and model identification of PCs, mobile devices, dumb terminals, and custom devices; Supports Windows, Linux, macOS, and thin clients; Supports mobile devices such as cell phones and tablets; Supports over seven categories of network devices, including servers, switches, and wireless controllers; Supports over ten categories of dumb terminals, including printers, projectors, TVs, cameras, and access control systems.

Due to gaps in between device scans, perform regular scanning (such as a network-wide scan every day or scan for detected but unresolved devices every two hours) to ensure that devices have been scanned before accessing the network.



Endpoints

Auth Status: All | Endpoint Check: All | Search by IP Address | Search | Filter | Clear

Bound: All | Ingress Client Installed: All

Endpoint Type | Custom

- All(504)
  - Host(275)
    - Windows(135)
    - MAC(1)
    - Linux(139)
    - Thin Client(0)
    - Unknown Host(0)
  - Mobile Endpoint(1)
    - Mobile Phone(0)
    - Tablet(1)
    - Unknown Mobile End
  - Network Device(7)
    - Server(5)
    - Sangfor Device(0)
    - Switch(0)
    - Router(2)
    - WLAN Controller(0)
    - Firewall(0)
    - VPN Gateway(0)
    - AP(0)
    - Unknown Network D
  - Dumb Endpoint(0)
    - Printer(0)

Endpoints

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

IP Address	MAC Address	User	Endpoint Type	Operating System	Endpoint Name	Operation
192.200.19.159	-	-	-	-	-	Operation
192.200.19.34	-	-	Windows	Windows	-	Operation
192.200.19.200	-	-	Linux	Linux	-	Operation
192.168.19.36	-	-	-	-	-	Operation
192.200.19.155	-	-	-	-	-	Operation
192.200.19.226	-	-	-	-	-	Operation
192.200.19.28	-	-	Linux	Linux	-	Operation
192.200.19.156	-	-	-	-	-	Operation
192.200.19.250	-	-	-	-	-	Operation
192.168.19.205	-	-	-	-	-	Operation
192.168.19.67	-	-	-	-	-	Operation
192.200.19.230	-	-	-	-	-	Operation
192.200.19.37	-	-	Windows	Windows	-	Operation
192.168.19.32	-	-	-	-	-	Operation
192.200.19.67	-	-	Windows	Windows	-	Operation
192.200.19.142	-	-	Windows	Windows	-	Operation
192.200.19.73	-	-	Windows	Windows	-	Operation
192.168.19.253	-	-	-	-	-	Operation
192.168.19.26	-	-	Linux	Linux	-	Oper

Page 1 of 11 | Entries Per Page: 50 | 504

Endpoints

Back

192.200.19.73

Endpoint Type: Windows | Endpoint Check: - | Bound: No | Lockout: Unlocked | Operation | Previous | Next

Basics

Endpoint Details

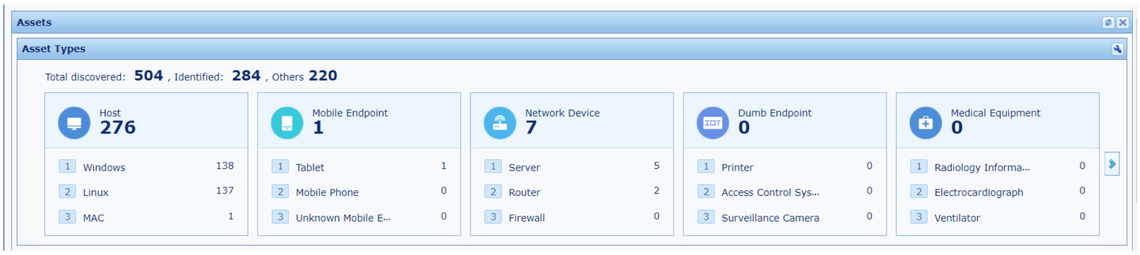
Endpoint Name:	-	Ingress Client Installed:	No
Previous IPs:	-	Ingress Client:	-
MAC Address:	-	Endpoint Vendor:	-
Operating System:	Windows 10 Home Single Language 19044	NIC Vendor:	-
Open Ports:	- Scan Again	First Detected:	2022-04-28 08:45:09

Authentication Details

User Status:	Offline	Group:	-
Auth Status:	No	Last Login:	-
User:	-		

Figure 13: Endpoint Visibility and Endpoint Info

Sangfor IAG can also discover trends in newly discovered devices, rank incompliant check items, and rank incompliant users to help administrators intuitively grasp the security status of endpoint access.



Assets

Asset Types

Total discovered: 504 , Identified: 284 , Others 220

Host	276	Mobile Endpoint	1	Network Device	7	Dumb Endpoint	0	Medical Equipment	0
1 Windows	138	1 Tablet	1	1 Server	5	1 Printer	0	1 Radiology Informa...	0
2 Linux	137	2 Mobile Phone	0	2 Router	2	2 Access Control Sys...	0	2 Electrocardiograph	0
3 MAC	1	3 Unknown Mobile E...	0	3 Firewall	0	3 Surveillance Camera	0	3 Ventilator	0

Figure 14: Asset Dashboard

Sangfor IAG can provide administrators with such important endpoint information and network visibility using active identification and passive identification mechanisms.

Passive Identification

Passive identification does not rely on sending packets but analyzes traffic to obtain device information. Passive identification is achieved using the following methods:

HTTP: The model of the endpoint device can be obtained from the field information of http traffic.

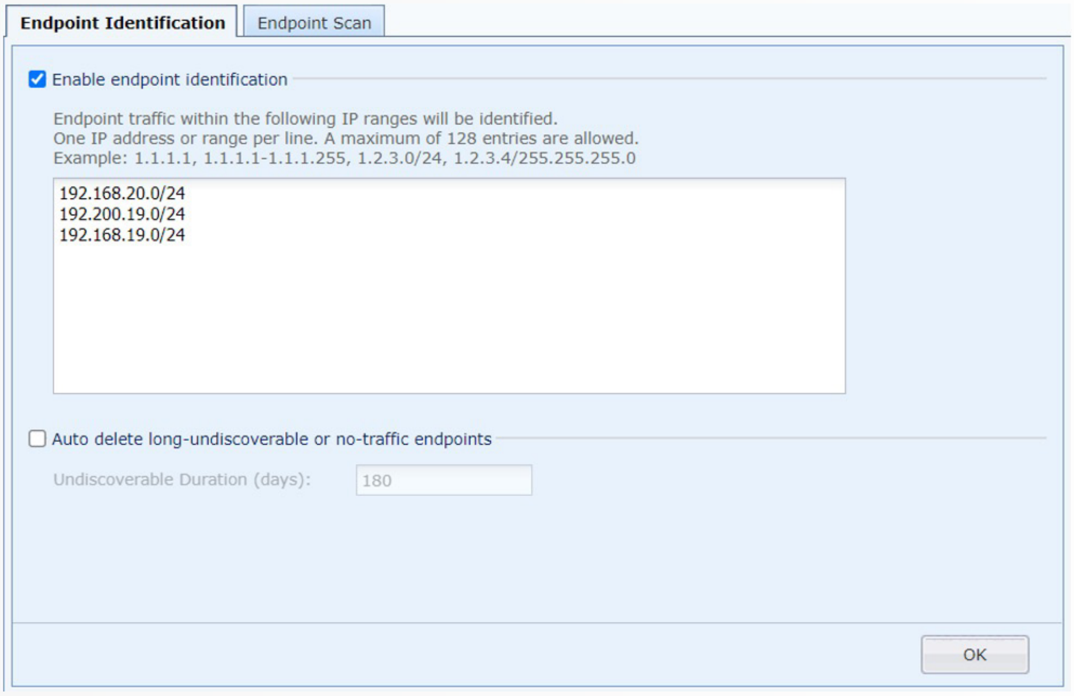
DHCP: The vendor and host name can be obtained by analyzing specified field information in DHCP request packets. This information can be used as the fingerprint to identify the endpoint type and matched with an endpoint vendor identification library to determine the endpoint vendor and host name.

Device Deployment

Layer 2 deployment: Nmap can identify the MAC address from ARP packets.

Layer 3 deployment: Uses cross-layer 3 MAC data and SNMP protocol to identify the MAC address by retrieving the APR table from the switch.

Other sniffing methods (smb, onvif, snmp) support Layer 3 scenarios.



☑ Enable endpoint identification

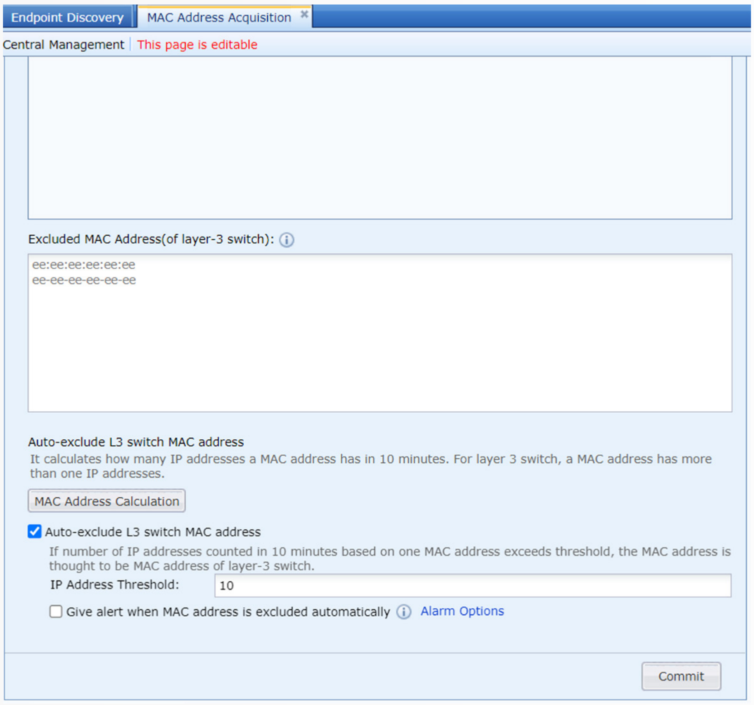
Endpoint traffic within the following IP ranges will be identified.
One IP address or range per line. A maximum of 128 entries are allowed.
Example: 1.1.1.1, 1.1.1.1-1.1.1.255, 1.2.3.0/24, 1.2.3.4/255.255.255.0

```
192.168.20.0/24
192.200.19.0/24
192.168.19.0/24
```

□ Auto delete long-undiscoverable or no-traffic endpoints

Undiscoverable Duration (days): 180

Figure 15: Endpoint Discovery setting



Excluded MAC Address(of layer-3 switch):

```
ee:ee:ee:ee:ee:ee
ee-ee-ee-ee-ee-ee
```

Auto-exclude L3 switch MAC address

It calculates how many IP addresses a MAC address has in 10 minutes. For layer 3 switch, a MAC address has more than one IP addresses.

☑ Auto-exclude L3 switch MAC address

If number of IP addresses counted in 10 minutes based on one MAC address exceeds threshold, the MAC address is thought to be MAC address of layer-3 switch.

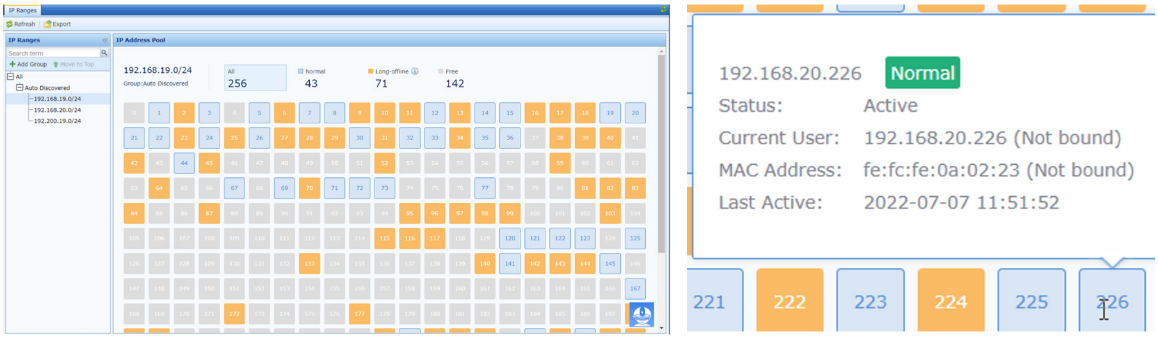
IP Address Threshold: 10

□ Give alert when MAC address is excluded automatically

Figure 16: MAC Address Acquisition Setting

IP Sorting

Sangfor IAG supports actively scanning the IPs of specified segments on the intranet, and by resolving the IPs of devices that mirror to the traffic. This gives administrators an overview of the intranet's IP usage, providing first-hand information for IP allocation and management (normal IPs, long-term offline IPs, and unused IPs, as well as the online status, users, MAC addresses, and active time of normal IPs).



192.168.19.0/24
Group:Auto Discovered

All	Normal	Long-offline	Free
256	43	71	142

192.168.20.226 Normal

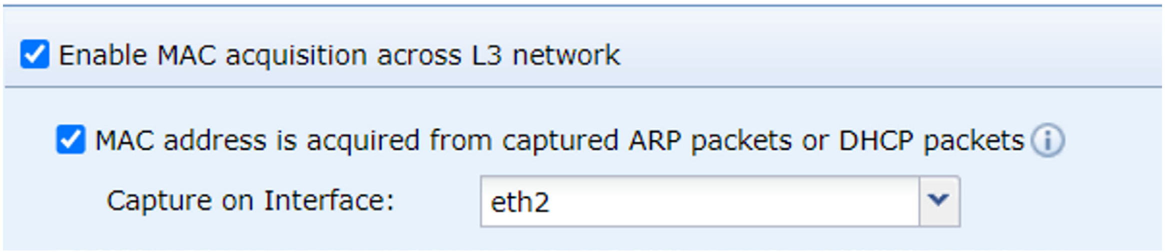
Status:	Active
Current User:	192.168.20.226 (Not bound)
MAC Address:	fe:fc:fe:0a:02:23 (Not bound)
Last Active:	2022-07-07 11:51:52

Figure 17: *IP Range Info*

Cross-Layer 3 MAC Address Identification

When an intranet user is bound to a MAC address or the user's MAC address range is limited, MAC identification across three layers must be enabled to achieve MAC authentication bypass in a Layer 3 intranet environment. Sangfor IAG identifies a MAC address across three layers in two different ways.

The first is reading the MAC address of intranet users through mirroring without SNMP enabled on the switch: Connect any idle network port of Sangfor IAG to the switch, enable mirroring on the corresponding interface of the switch, and mirror the relevant data packets to Sangfor IAG. Obtain the MAC address from ARP packets or DHCP packets.



☑ Enable MAC acquisition across L3 network

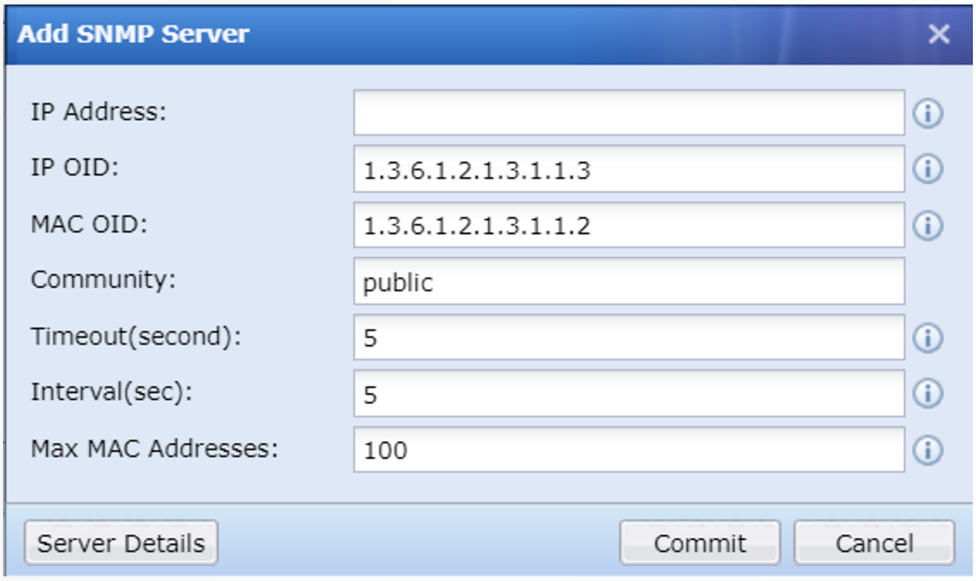
☑ MAC address is acquired from captured ARP packets or DHCP packets ⓘ

Capture on Interface: eth2

Figure 18: *MAC Acquisition Capture on Different Interface*

The second is using the SNMP function of the intranet switch to identify the real MAC address of intranet users. The device will periodically send SNMP requests to the Layer 3 switch to request the MAC table of the switch and save it in the device memory.

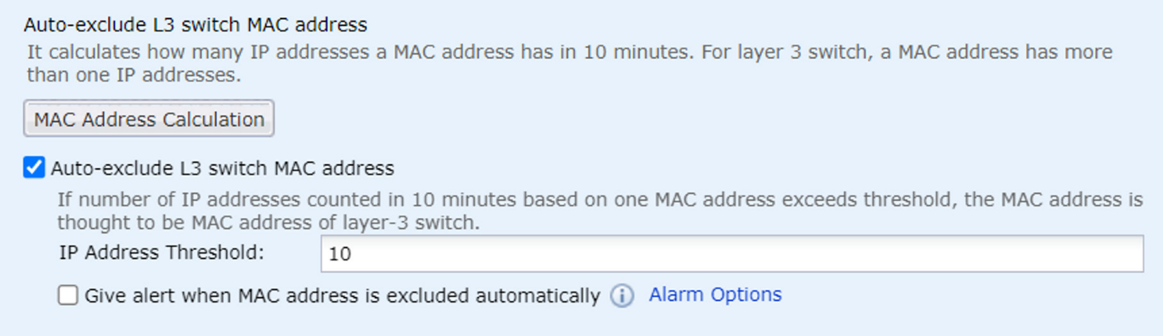
When computers on other network segments of the Layer 3 switch pass through the switch, such as a 192.168.1.2 PC (which is not on the same network segment as the device's LAN port), the switch verifies that the MAC of this data packet belongs to the switch. This MAC is not processed, and the real MAC address is searched in the memory according to the IP 192.168.1.2 to verify user's real MAC.



Add SNMP Server

IP Address:	
IP OID:	1.3.6.1.2.1.3.1.1.3
MAC OID:	1.3.6.1.2.1.3.1.1.2
Community:	public
Timeout(second):	5
Interval(sec):	5
Max MAC Addresses:	100

Figure 19: *SNMP Server Setting*



Auto-exclude L3 switch MAC address

It calculates how many IP addresses a MAC address has in 10 minutes. For layer 3 switch, a MAC address has more than one IP addresses.

☑ Auto-exclude L3 switch MAC address

If number of IP addresses counted in 10 minutes based on one MAC address exceeds threshold, the MAC address is thought to be MAC address of layer-3 switch.

IP Address Threshold: 10

☐ Give alert when MAC address is excluded automatically

Figure 20: *Auto-Exclude L3 Switch MAC Address setting*

Make Your Digital Transformation Simpler and Secure

SANGFOR INTERNATIONAL OFFICES

SANGFOR SINGAPORE
8 Burn Road # 04-09, Trivex,
Singapore (369977)
Tel: (+65) 6276-9133

SANGFOR HONG KONG (CHINA)
Unit 1612-16, 16/F, The Metropolis Tower, 10 Metropolis
Drive, Hung Hom, Kowloon, Hong Kong
Tel: (+852) 3845-5410

SANGFOR INDONESIA
MD Place 3rd Floor, Jl Setiabudi No.7, Jakarta Selatan
12910, Indonesia
Tel: (+62) 21-2966-9283

SANGFOR MALAYSIA
No.47-10 The Boulevard Offices, Mid Valley City, Lingkaran
Syed Putra, 59200 Kuala Lumpur, Malaysia
Tel: (+60) 3-2702-3644

SANGFOR THAILAND
141 Major Tower Thonglor (Thonglor10) Floor 11 Sukhumvit
Road, Kholngtan Nuea Wattana BKK, Thailand 10110
Tel: (+66) 02-002-0118

SANGFOR PHILIPPINES
7A, OPL Building, 100 Don Carlos Palanca, Legazpi, Makati,
122 Metro, Manila, Philippines.
Tel: (+63) 917-117-9346

SANGFOR VIETNAM
4th Floor, M Building, Street C, Phu My Hung,
Tan Phu Ward, District 7, HCMC, Vietnam
Tel: (+84) 287-1005018

SANGFOR SOUTH KOREA
Floor 17, Room 1703, Yuwon bldg. 116, Seosomun-ro,
Jung-gu, Seoul, Republic of Korea
Tel: (+82) 2-6261-0999

SANGFOR EMEA
D-81 (D-Wing), Dubai Silicon Oasis HQ Building, Dubai, UAE.
Tel: (+971) 52855-2520

SANGFOR PAKISTAN
44, Navy Housing Scheme, ZamZamma, Karachi, Pakistan
Tel: (+92) 333-3365967

SANGFOR ITALY
Floor 8, Via Marsala, 36B, 21013 Gallarate VA, Italia
Tel: (+39) 3395-7110-78

VAILABLE SOLUTIONS

IAG	Simplify User & Network Management
NGAF	Smarter Security Powered By AI
Endpoint Secure	The Future of Endpoint Security
Cyber Command	Powerful Intelligent Threat and Detection Platform
TIARA	Threat Identification, Analysis and Risk Management
Incident Response	Closed-loop Incident Response Service Solution
HCI	Driving Hyperconvergence to Fully Converged
MCS	Your Digital Infrastructure Exclusive Store
VDI	Ultimate User Experience that Beats PC
SD-WAN	Boost Your Branch Business With Sangfor
SIER	Simplify & Intelligence Your Branch Network
ACCESS	Cloud-based SASE for Branch Offices & Remote Users
WANO	Enjoy a LAN Speed on your WAN

SANGFOR

Sales: sales@sangfor.com

Marketing: marketing@sangfor.com

Global Service Center: +60 12711 7129 (or 7511)

www.sangfor.com

OUR SOCIAL NETWORKS

https://twitter.com/SANGFOR

https://www.linkedin.com/company/sangfor-technologies

https://www.facebook.com/Sangfor

https://www.instagram.com/sangfortechnologies/

https://www.youtube.com/user/SangforTechnologies