SANGFOR | SANGFOR SECURITY | Sangfor IAG

ENDPOINT COMPLIANCE SOLUTION FOR IOT

CONTENTS

Access Authentication

Technical Overview of Network Access Authentication

To establish robust network access control, organizations have a range of authentication methods to choose from. These methods serve different needs and offer varying levels of control. The following are the primary authentication methods:

802.1X Authentication

802.1X is an IEEE standard for network access control that operates at the port level, enforcing authentication before granting network access. It is commonly used in LAN environments to enhance security. 802.1X uses the Extensible Authentication Protocol over LAN (EAPoL), which allows for various authentication methods, including passwords, tokens, certificates, and more.

When a device attempts to connect to a network, it is directed to an authentication server, which verifies the device's identity using the chosen authentication method. Once authenticated, the device is granted access to the network.

Portal Authentication

Portal authentication, or web authentication, is generally used to authorize public internet access in settings such as hotels, coffee shops, and fast-food chains. When a user attempts to access the internet through a browser, they are redirected to a captive portal webpage for authentication.

The authenticator only releases the data packet to authorize access after the user successfully logs in. This method requires no client installation and offers user-friendly portal webpages that are easy to maintain and operate. Businesses can also use portal webpages for digital marketing campaigns, such as advertisements, responsibility notices, and business promotions.

MAC Authentication Bypass (MAB)

MAC authentication bypass (MAB) is used to authorize network access to devices that do not support interactive authentication, such as printers, scanners, and self-service kiosks. This authentication method can also be used for devices that an organization wishes to exempt from authentication for fast and convenient network access. MAB can also be used as a fallback option when users fail to authenticate using 802.1X so long as MAB is enabled on the switch.

The following table provides a comparison of the three authentication methods.

Control Point	Authentication Method	Applicable Scenarios	Applicable to
Layer 2 Access Control	**802.1x Authentication**	1. Needs to be supported by the switch and a client application must be installed. ***a. Wired network*** Users need to use an ingress client or system login for authentication and internet access. ***b. Wireless network*** Users can use system login for authentication and internet access. 2. Strict control: Prevents access between devices connected to the same switch before successful authentication.	Employees and their devices
	MAB Authentication	1. Needs to be supported by the switch but does not require a client application. 2. Strict control; prevents access between devices connected to the same switch before successful authentication.	Devices that do not support interactive authentication, such as printers, dumb terminals, self-service kiosks, IoT devices
Layer 3 Access Control	**Portal Authentication**	1. Data is mirrored by the switch. This is generally only supported by Layer 3 core switches. It does not require a client application. 2. Supports various authentication methods, e.g., password authentication, active directory (AD) authentication, SMS authentication, and single sign-on authentication. 3. The authentication control point is deployed on the Layer 3 core switch. Access to the internet and business applications is restricted before successful authentication, but devices connected to the same layer 2 switch can interact with each other.	Employees, Guest, Devices that do not support interactive authentication (MAC binding to bypass authentication)

Comparison between 802.1x Authentication, MAB Authentication and Portal Authentication

Technical Overview of Sangfor Access Control

Effective user differentiation is the basis of implementing robust authorization and auditing policies to safeguard against identity impersonation, privilege escalation, and privilege abuse. Sangfor IAG offers a comprehensive range of authentication methods, enabling organizations to verify user identities and devices securely, including:

1. **Local authentication:** Supports username/password authentication, IP/MAC/IP-MAC binding, SMS authentication.

2. **Third-party authentication:** Supports LDAP, RADIUS, POP3, Proxy, database, etc.

3. **SMS authentication:** Users receive an authentication code via text message for verification.

4. **OA authentication:** Supports OAuth authentication using third-party OA applications, including DingTalk, Pocket Assistant, and WeCom.

5. **QR code authentication for virtual conferencing:** Users can either scan a QR code or enter the meeting ID for authentication. Real-name authentication is also supported via mobile number verification.

6. **QR code authentication for visitors:** Reception staff authenticate visitors by scanning a QR code on their mobile phones.

7. **Two-factor authentication:** Supports time-based one-time password (TOTP) verification via Microsoft Authenticator and Google Authenticator.

8 **USB-key authentication**

9 **Single sign-on (SSO) authentication:** Supports active directory (AD), POP3, proxy, web, and third-party systems.

10 **Force authentication:** Enforces single sign-on for users in specified IP segments.

11 **802.1x authentication:** Implements port-based authentication using a switch; achieves strong Layer 2 access control by blocking TCP and UDP packets before successful authentication.

12 **MAB authentication:** Based on 802.1x authentication and authorizes devices that do not support interactive authentication to the network using MAC authentication.

13 **CA authentication:** Supports external CA certificate authentication based on 802.1x authentication and the online certificate status protocol (OCSP).

802.1x Authentication

802.1X authentication is primarily used to authenticate devices to a local area network (LAN). It is used when strong intranet access control is required. Devices are restricted from accessing the intranet, including the Layer 2 network, until successful authentication. This means that traffic cannot pass through the Layer 2 switch.

802.1X authentication follows a typical client/server (C/S) architecture that comprises three entities: the client (supplicant), the authenticator, and the authentication server.

Features of 802.1x authentication:

High level of security: Authentication control points are deployed in the network access layer or aggregation layer, enhancing overall network security.

Requires the installation of an 802.1x authentication client (e.g., Sangfor IAG ingress client) or a built-in 802.1X client in the operating system.

The technology is mature and widely used for employee intranet access in various types of campus networks.

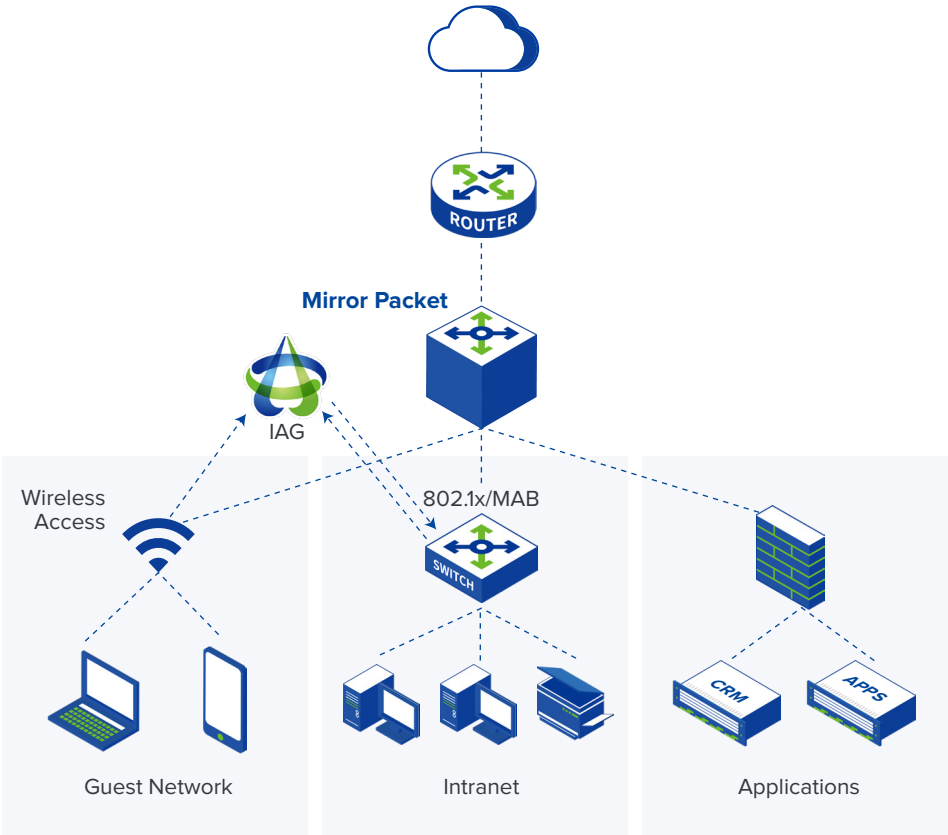


Figure 1: Secure Network using 802.1x Authentication and MAB

Sangfor IAG uses an ingress client to implement 802.1x authentication, ensuring secure Layer 2 access control in wired and wireless LAN environments. This authentication method requires 802.1x to be enabled on the Layer 2 switch or wireless controller, and users need to be authenticated to access the Layer 2 network. After successful authentication, users are granted an IP address to access intranet resources. Failure to authenticate restricts users from passing the Layer 2 switch and reaching the intranet.

The 802.1x authentication process of Sangfor IAG is as follows:

- **STEP 1** Enable 802.1x authentication on the Layer 2 switch or wireless controller
- **STEP 2** Install the Sangfor IAG ingress client on the endpoint device
- **STEP 3** Only authenticated users are able to access the intranet
- **STEP 4** Unauthenticated users are restricted from accessing the intranet or only permitted access to the guest network for limited resources

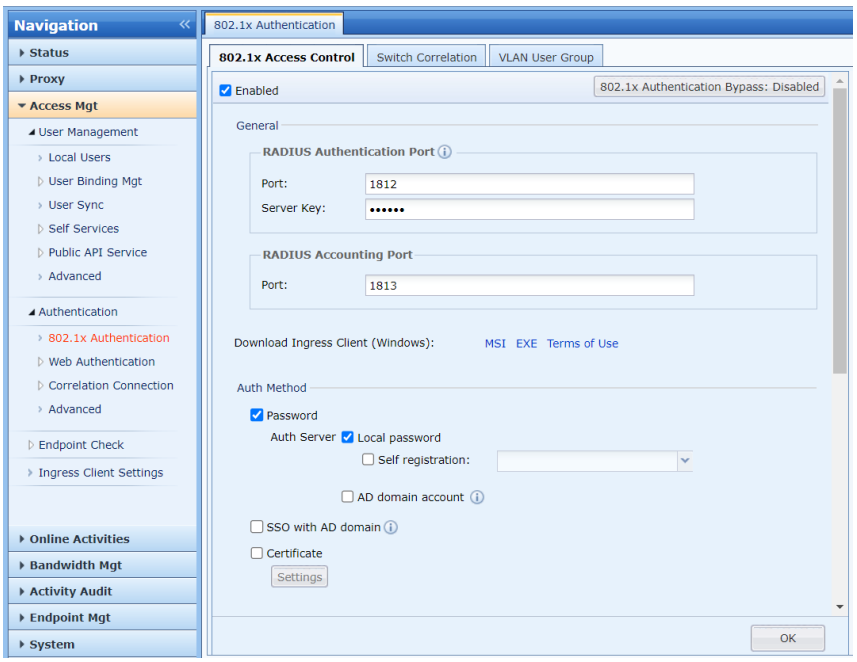


Figure 2: 802.1x Authentication Setting

Portal Authentication

Portal authentication typically does not require a dedicated client application other than a web browser. When a user accesses a URL, they are redirected to the captive portal webpage where they enter their username and password. After successful authentication, they are granted access to the corresponding network resources. Portal authentication is simple to implement and has little impact on the network environment. Portal authentication options on Sangfor IAG include password authentication, single sign-on authentication, SMS authentication, and authentication bypass through IP/MAC binding.

The portal authentication process of Sangfor IAG is as follows:

STEP 1 Internet or business application traffic passes through the switch. The data packets are mirrored from the switch to Sangfor IAG, which verifies if the endpoint device has been authenticated. If not, Sangfor IAG issues an HTTP response with the 302 status code, which is used for URL redirection.

STEP 2 The endpoint device receives the HTTP response and opens Sangfor IAG for authentication.

STEP 3 Access is granted after successful authentication. If authentication fails, a reset packet is sent to restrict access.

STEP 4 In addition to authentication, Sangfor IAG offers administrators the option to configure an endpoint compliance check policy. Users will have to complete both authentication and the endpoint compliance check to gain access to intranet resources.

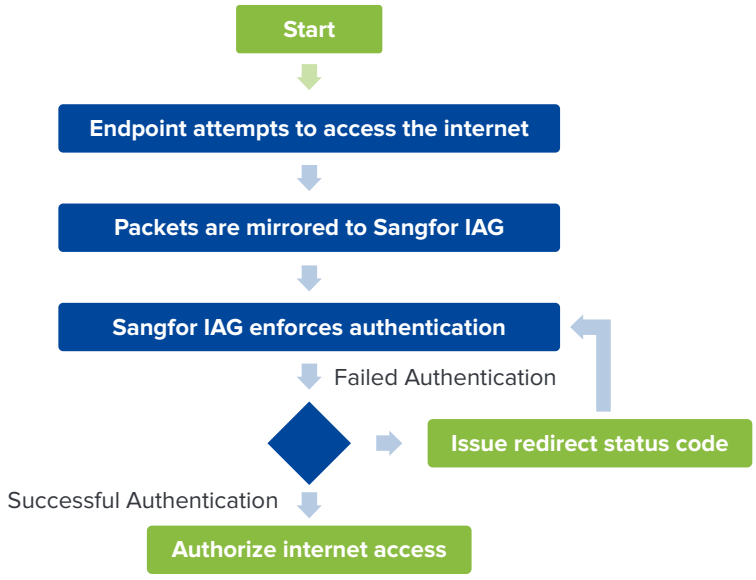


Figure 3: Decision Flow for using Portal Authentication Policy

Advantages of portal authentication	
• Supports bypass deployment / no client installation	• Achieves application access control
• Simple implementation	• Network-wide traffic visibility
• Low interference	• Supports internet and business application traffic auditing

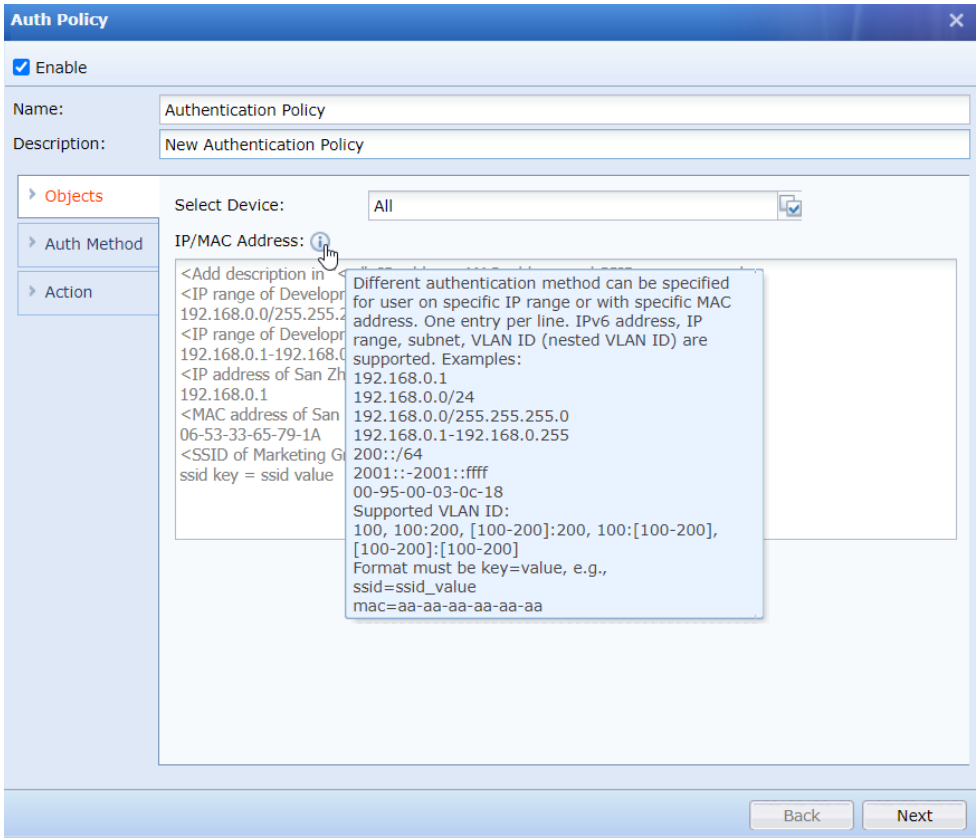


Figure 4: *Objects configuration from Authentication Policy Setting*

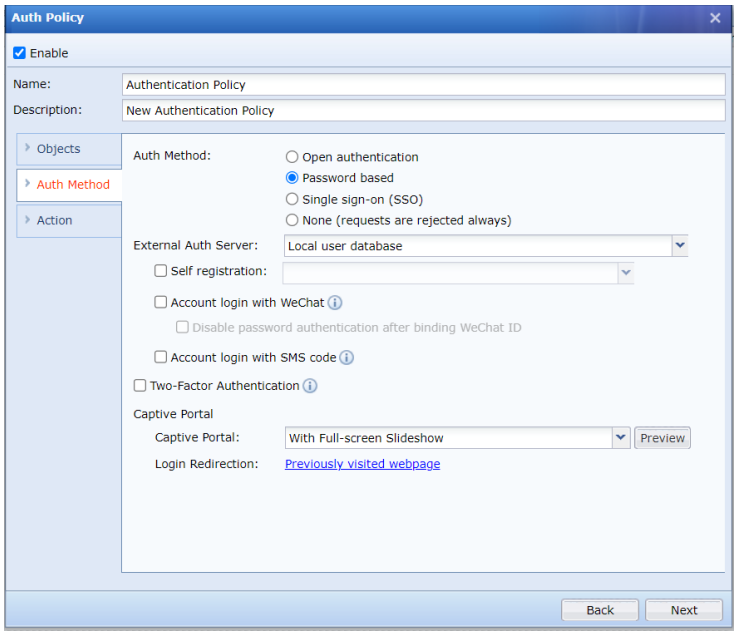


Figure 5: *Authentication method configuration from Authentication Policy Setting*

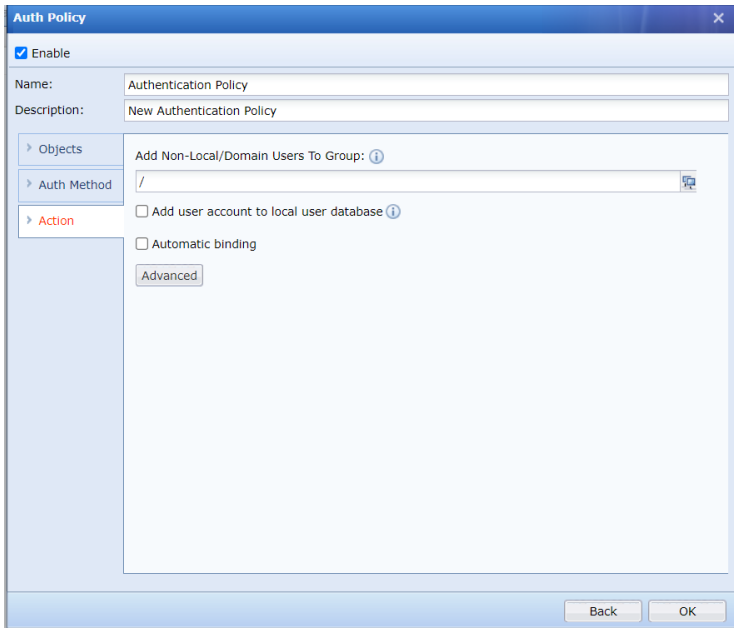


Figure 6: *Action configuration from Authentication Policy Setting*

MAB Authentication

MAC Address Bypass (MAB) is used when the device connected to an 802.1x authentication-enabled switch port does not support interactive authentication, such as a printer. If the switch times out waiting for the device to return the EAPoL response packet for 802.1x authentication, it will attempt to identify the device using its MAC address. The MAC address serves as the device's identity token, which is sent to the authentication server as its username.

Advantages of MAB authentication:

- No client installation required
- Supports the authentication of IoT devices
- Supports the authentication of devices that do not support interactive authentication
- Achieves Layer 2 access control by denying intranet access before successful authentication
- Used as a fallback authentication method for devices that fail to authenticate to the network

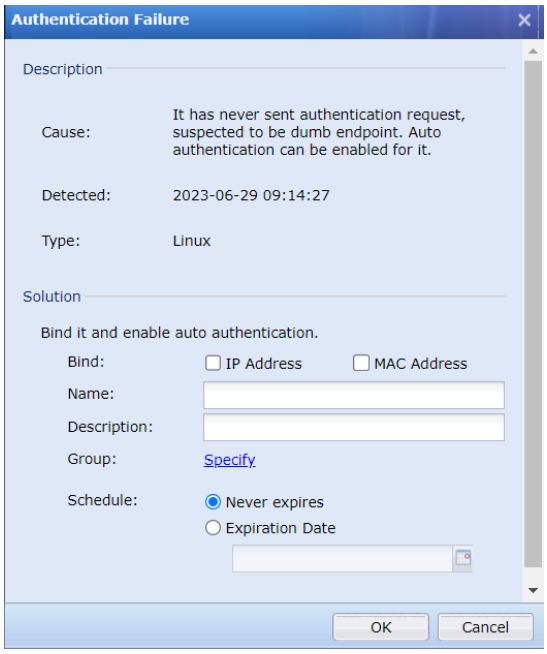


Figure 7: Authentication Failure Setting Dialog Box from Failed to Get Online (7 Days)

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.

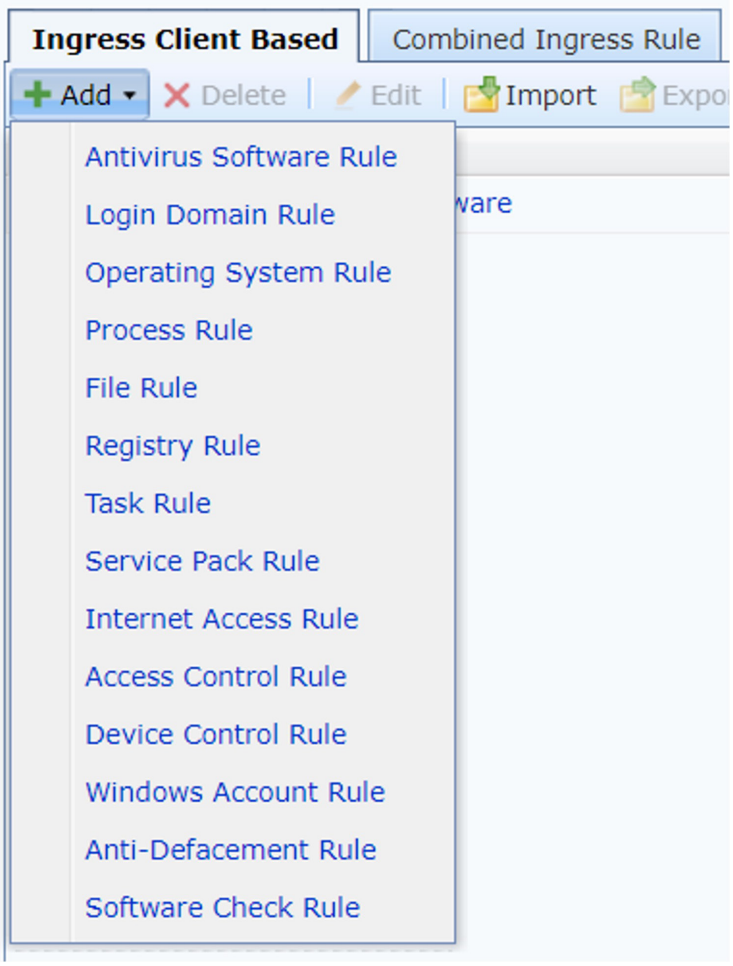


Figure 8: *Ingress Client Based*

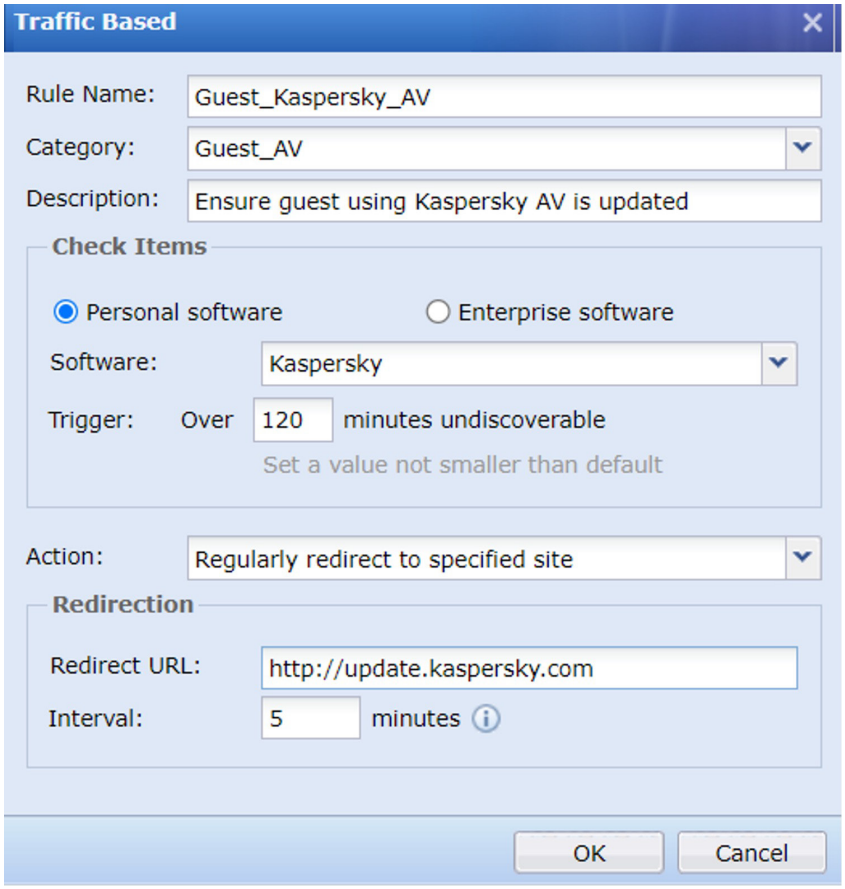


Figure 9: *Traffic Based*

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.

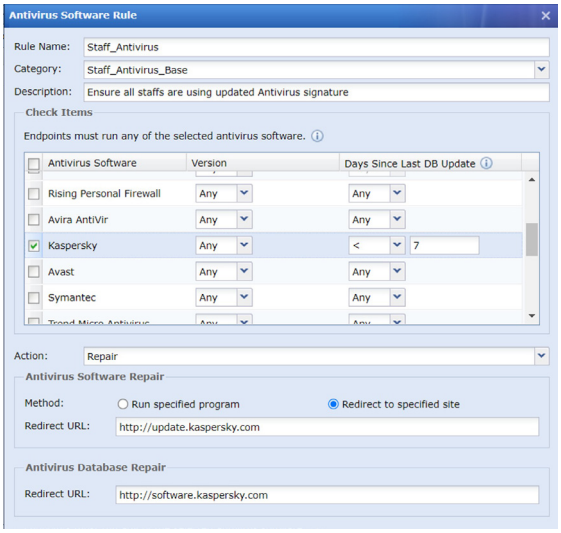


Figure 10: *Anti-Virus Software Based Rule Configuration*

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.

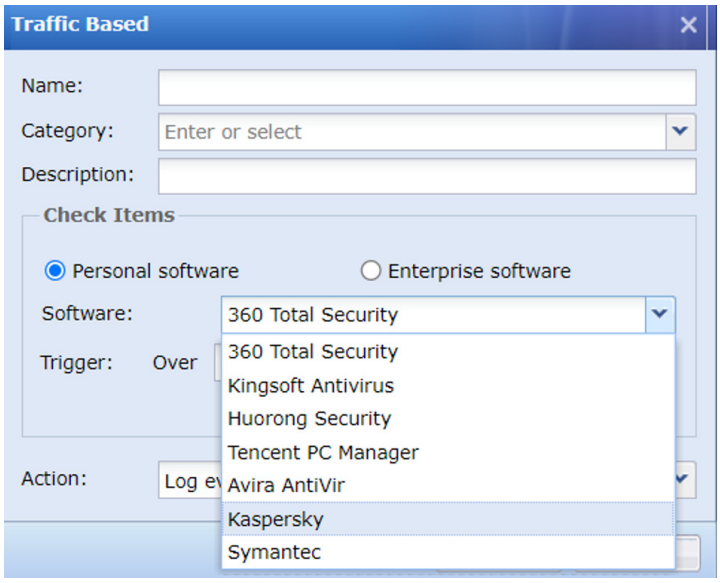


Figure 11: Traffic Based Configuration

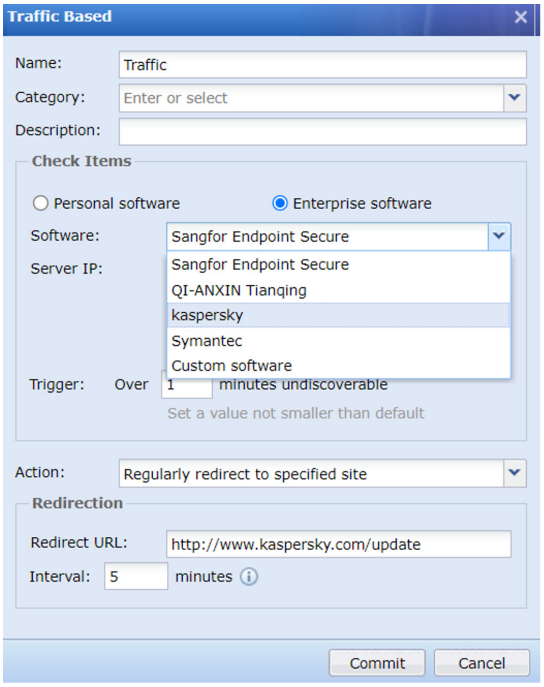


Figure 12: Traffic based configuration

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.

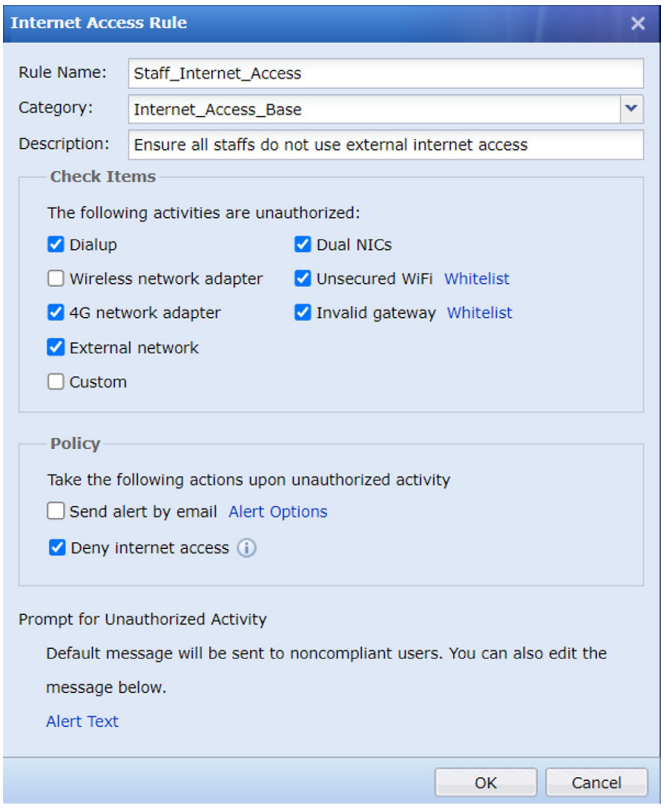


Figure 13: Unauthorized Internet Access Check with prompt text setting

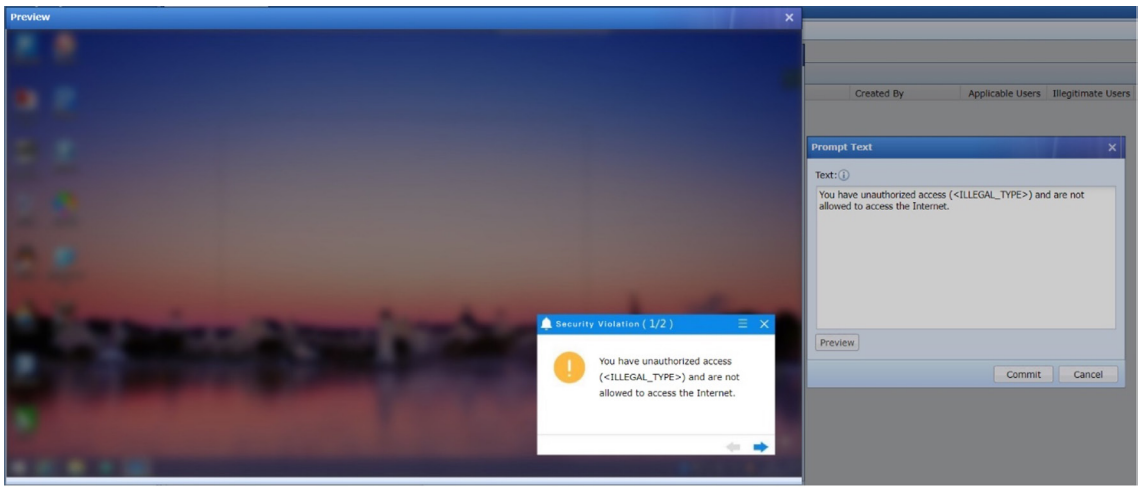


Figure 14: Unauthorized Internet Access Check with security violation prompt.

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.

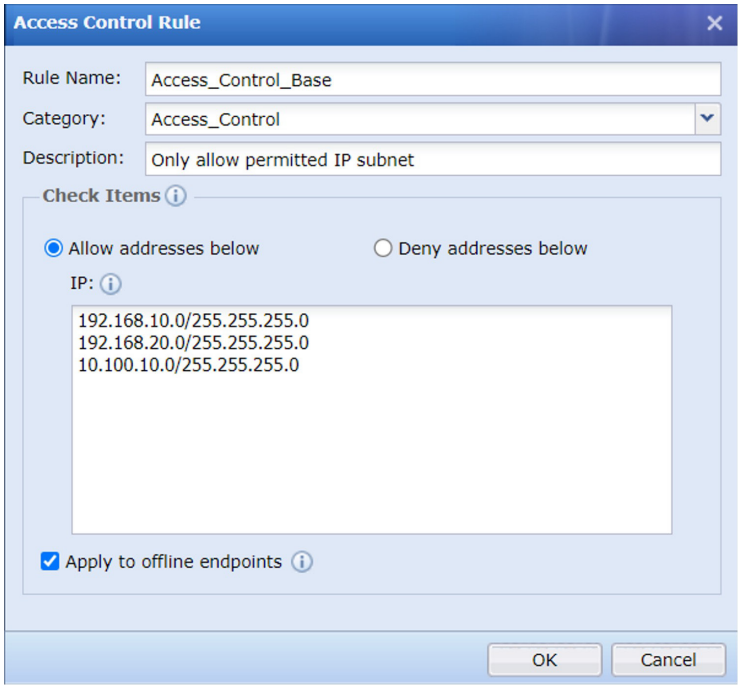


Figure 15: Access Control Configuration

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.

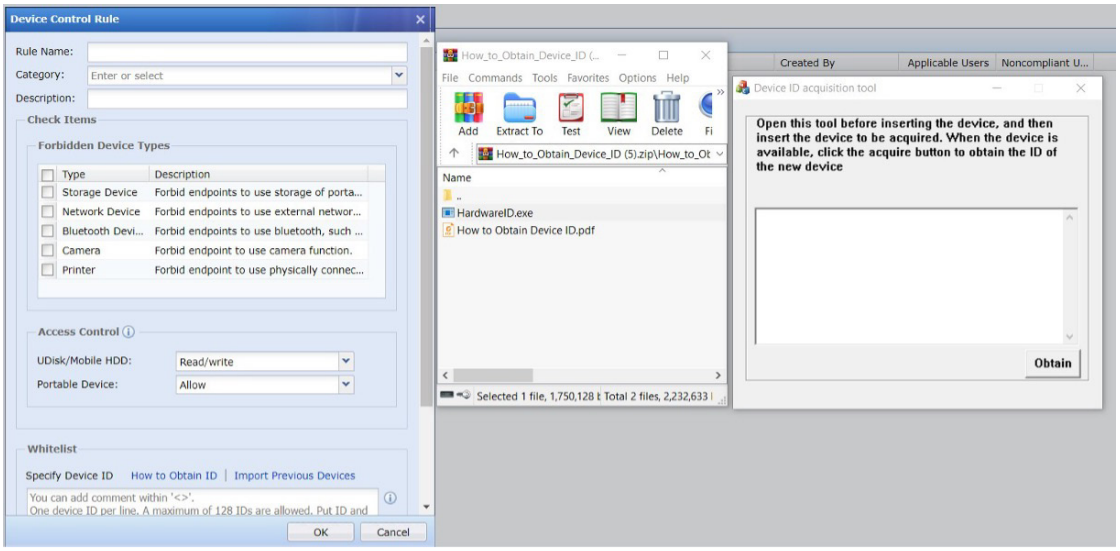


Figure 16: External Device Configuration and Obtain Hardware ID

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

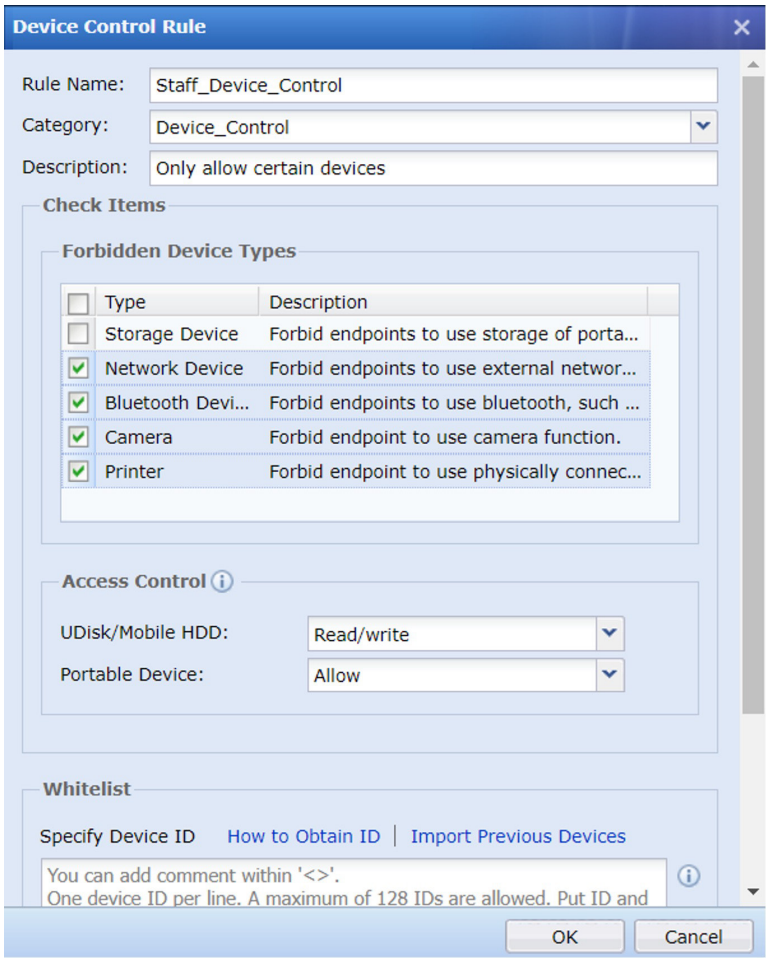


Figure 17: External Device Control Configuration

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).

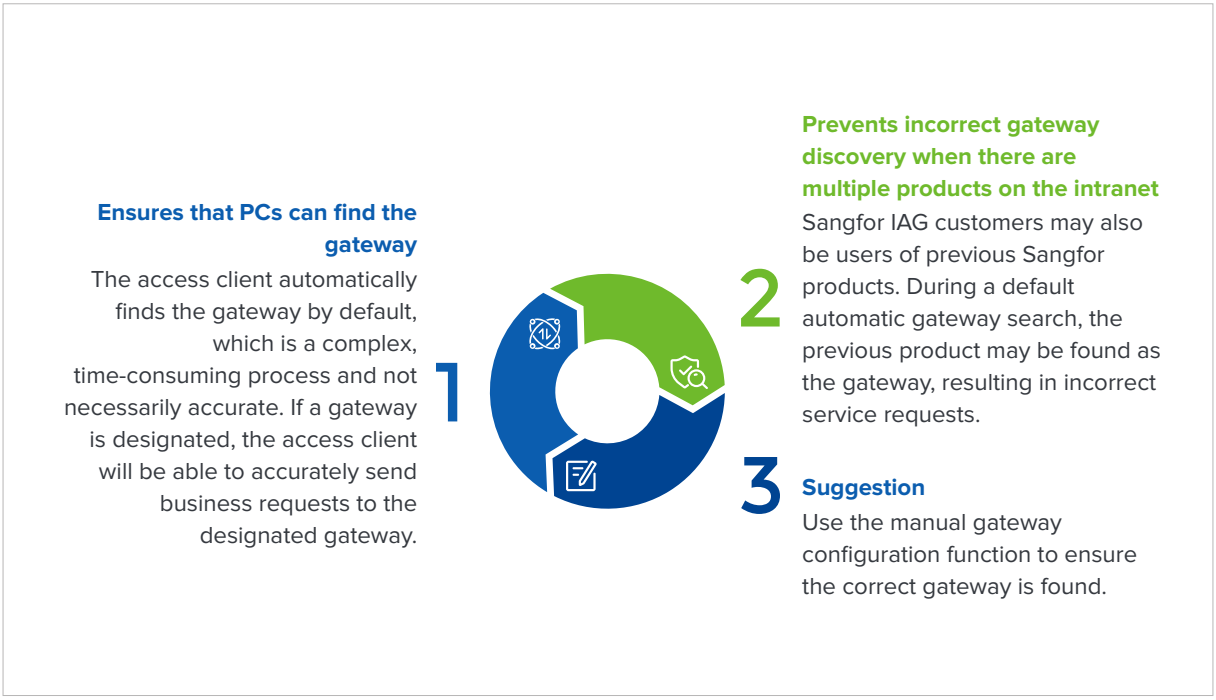
Device ID Generation

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:



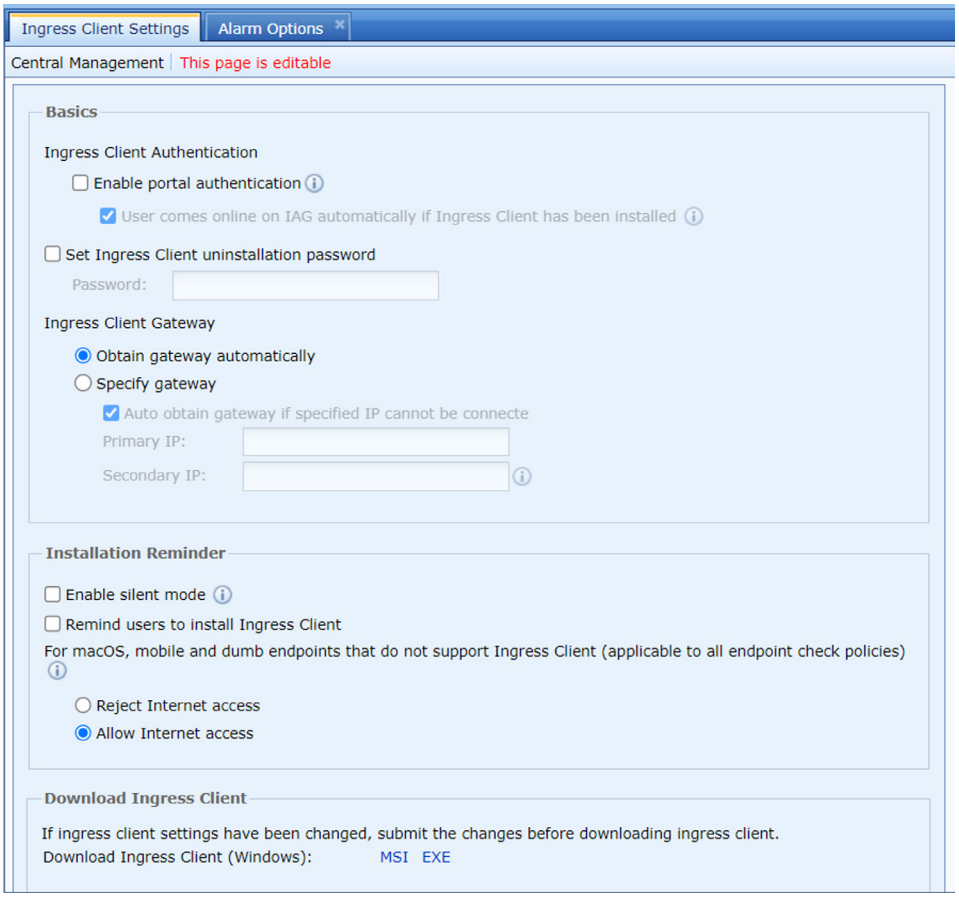


Figure 18: *Ingress Client Settings*

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.

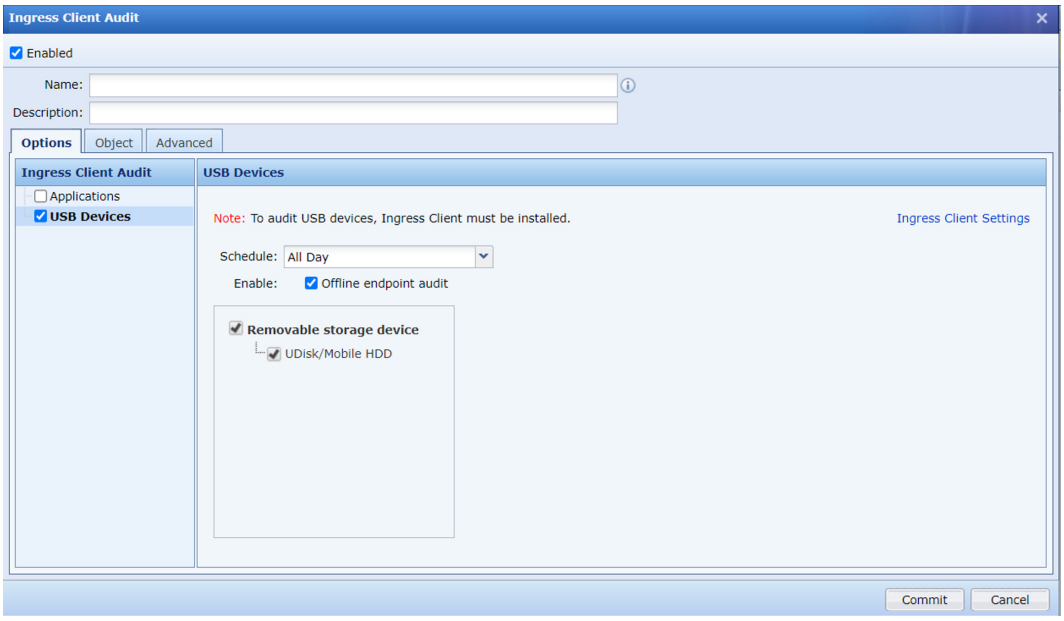


Figure 19: Ingress Client offline audit setting

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.

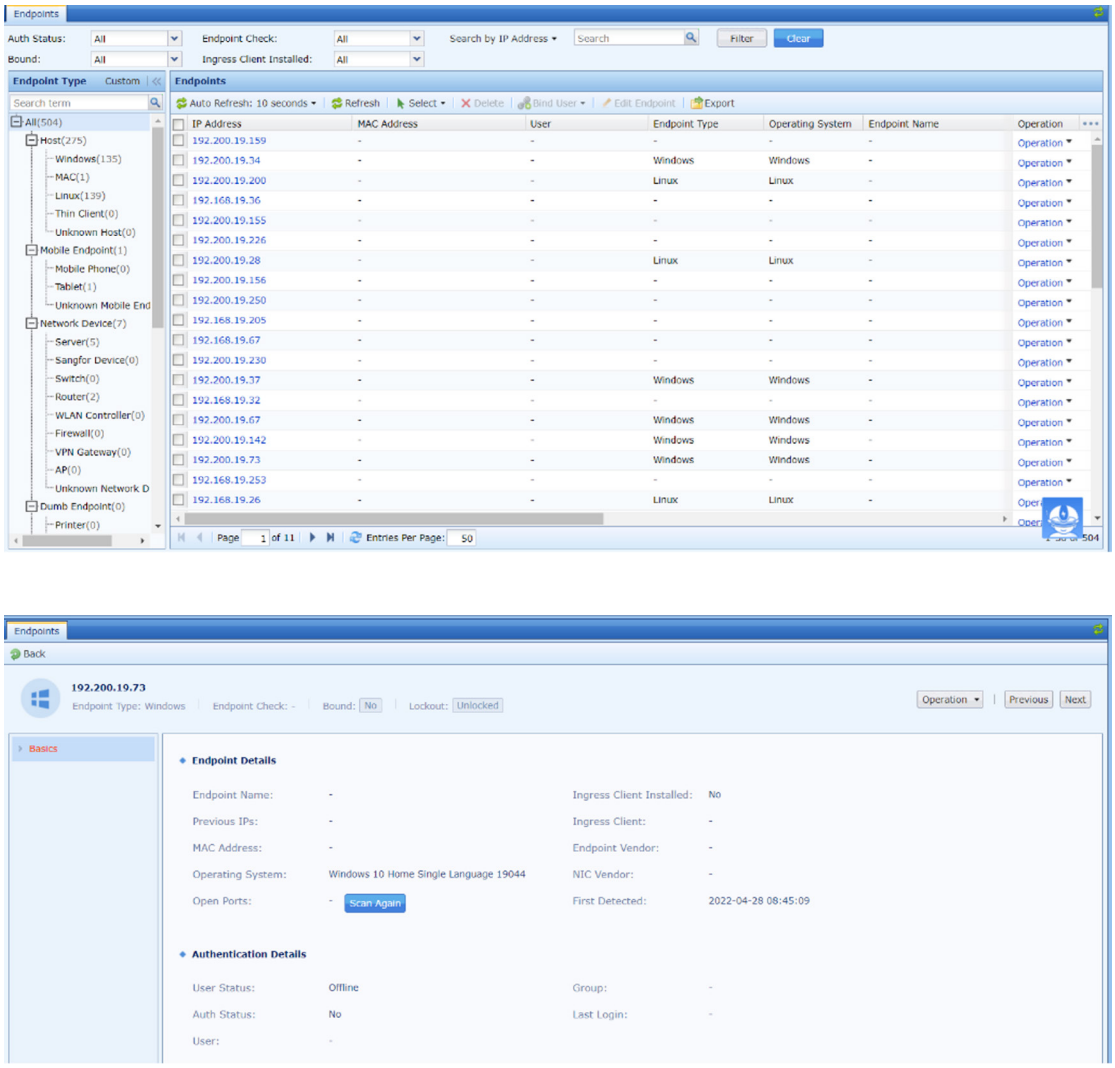


Figure 20: *Endpoint Visibility and Endpoint Info*

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.

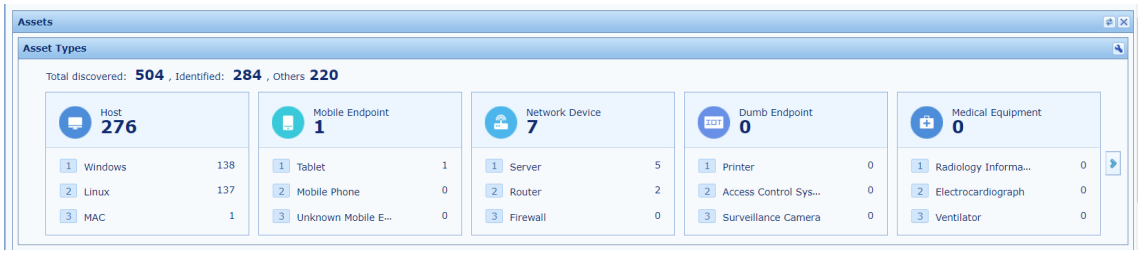


Figure 21: Asset Dashboard

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.

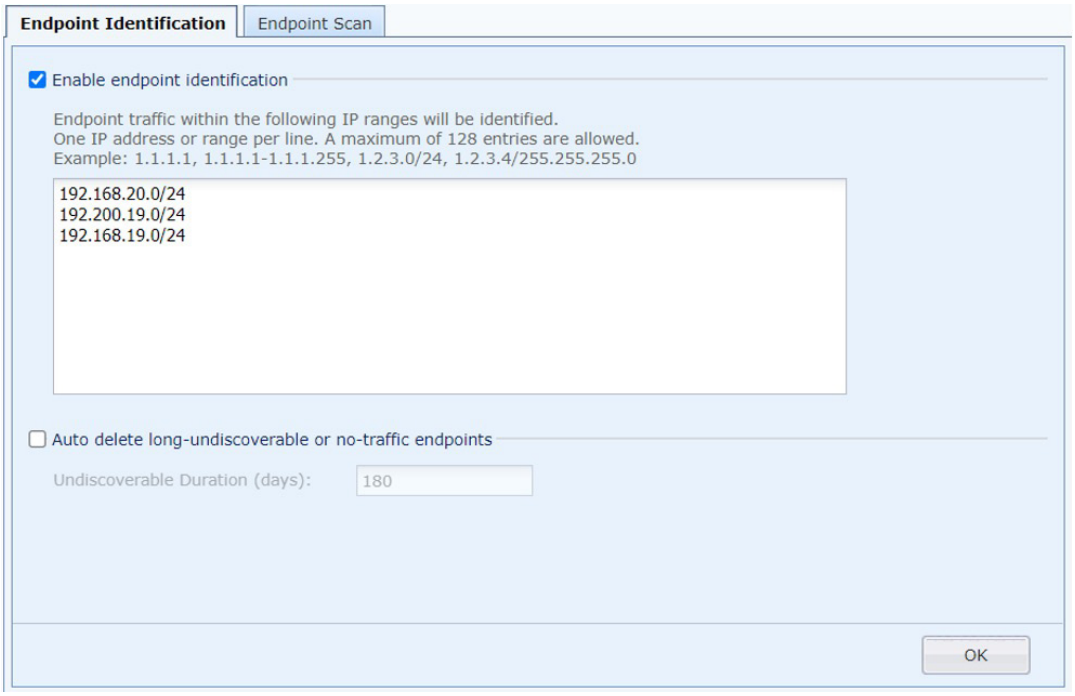


Figure 22: Endpoint Discovery setting

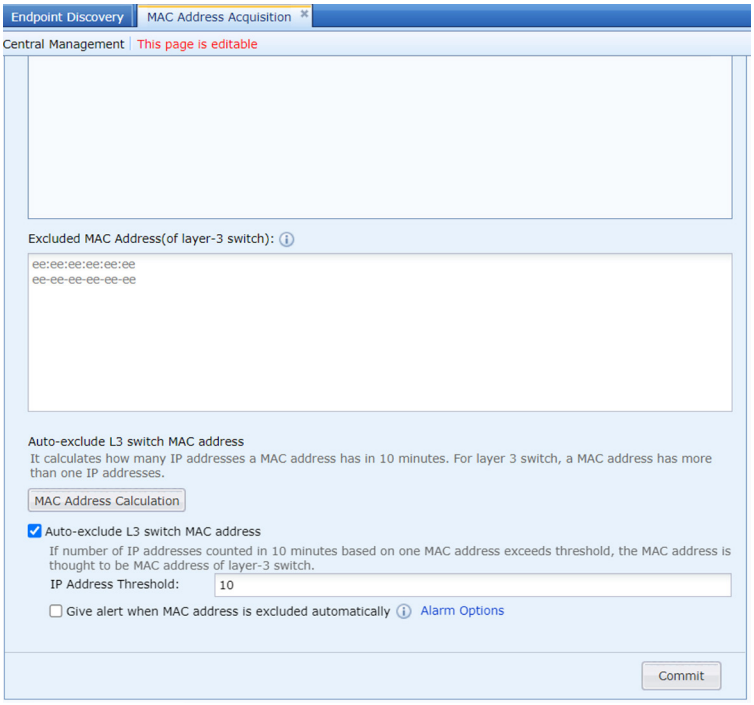


Figure 23: MAC Address Acquisition Setting

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).

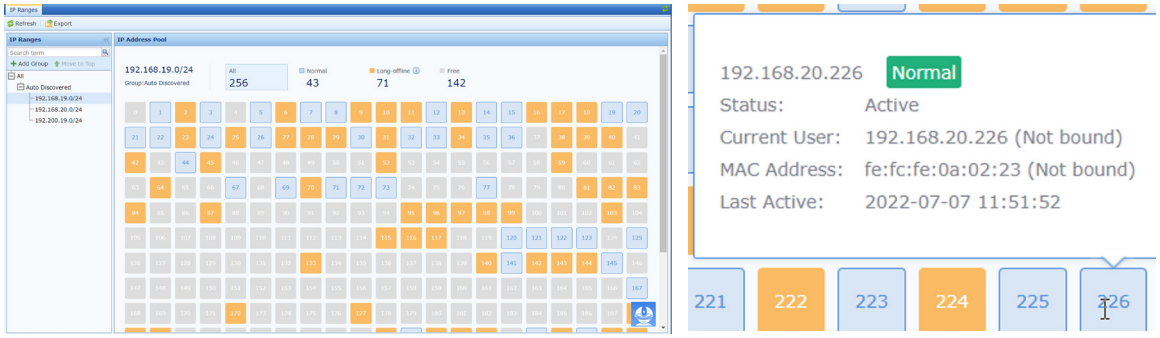


Figure 24: IP Range Info

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.

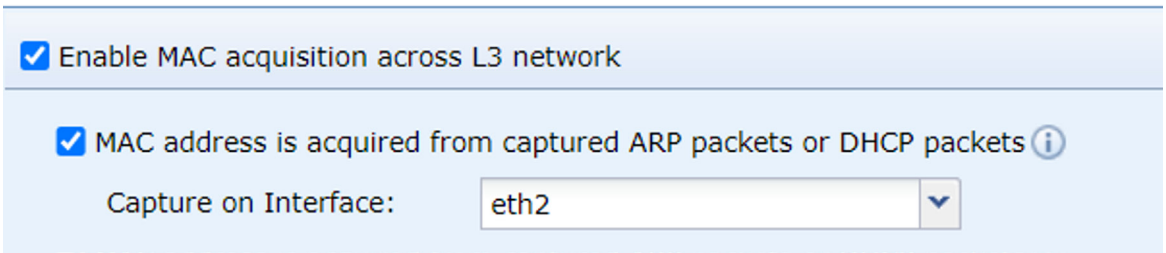


Figure 25: MAC Acquisition Capture on Different Interface

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.

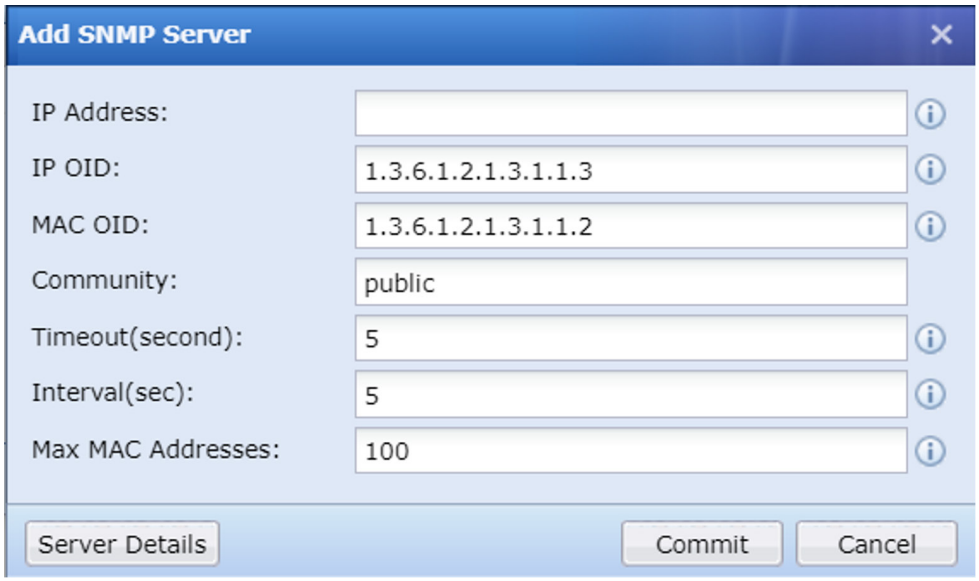


Figure 26: SNMP Server Setting

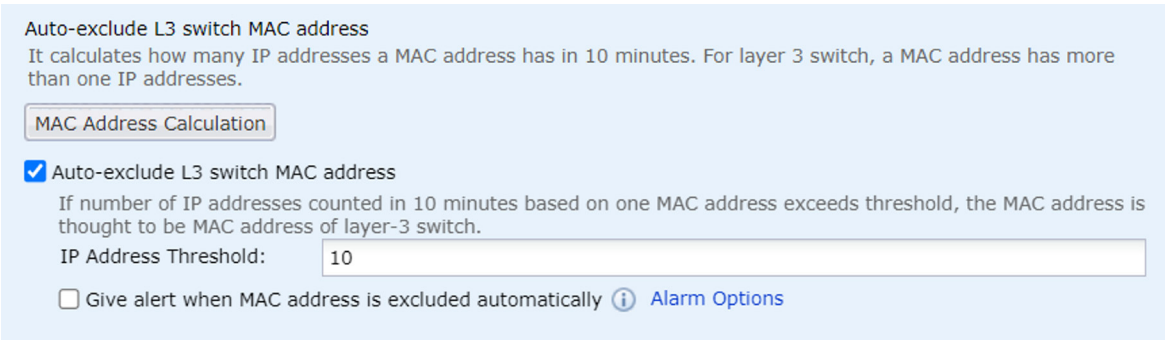


Figure 27: Auto-Exclude L3 Switch MAC Address setting

Make Your Digital Transformation Simpler and Secure

INTERNATIONAL OFFICES

SANGFOR SINGAPORE
10 Ubi Crescent, #04-26 Ubi Techpark (Lobby B),
Singapore 408564
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.45-10 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) 0916-267-7322

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
D44, Navy Housing Scheme, ZamZamma, Karachi, Pakistan
Tel: (+92) 333-3365967

SANGFOR ITALY
Floor 8, Via Marsala, 36B, 21013 Gallarate VA, Italia
Tel: (+39) 0331-648773

SANGFOR TURKEY
Turgut Ozal Street, Zentra Istanbul, First Floor, Office.
20 Çekmeköy / İstanbul, Postal Code: 34788
Tel:(+90) 546-1615678

AVAILABLE SOLUTIONS

IAG - Internet Access Gateway
Secure User Internet Access Behaviour

NGAF - Next Generation Firewall
Smarter AI-Powered Perimeter Defence

Endpoint Secure - Endpoint Security
The Future of Endpoint Security

Cyber Command - Network Detection and Response
Smart Efficient Detection and Response

TIARA - Threat Identification, Analysis and Risk Assessment
Smart Threat Analysis and Assessment

IR - Incident Response
Sangfor Incident Response – One Call Away

Cyber Guardian - Managed Threat Detection & Response Service
Faster Response Through Human/AI Collaboration

HCI - Hyper-Converged Infrastructure
Fully Converge Your Data Center

MCS - Managed Cloud Services
Your Exclusive Digital Infrastructure

VDI - aDesk Virtual Desktop Infrastructure
Seamless Experience, Secure and Efficient

Access - Secure Access Service Edge
Simple Security for Branches & Remote Users

EDS - Enterprise Distributed Storage
The Only Secured Data Storage You Need

SD-WAN
Boost Your Branch with Sangfor

SANGFOR

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

Sales: sales@sangfor.com

Marketing: marketing@sangfor.com

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

www.sangfor.com