SANGFOR

IAG

Endpoint Visibility Configuration Guide

Version 13.0.15

Change Log

Date	Change Description
Sep 25, 2020	Version 13.0.15 Release

CONTENT

Chapter 1 Endpoint Visibility Requirement Background 1
Chapter 2 Endpoint visibility function description 1
Chapter 2.1 Configuration Guide 2
Chapter 2.1.1 Endpoint Identification result 3
Chapter 2.1.2 Effect of IP ranges 4
Precaution: 5

Chapter 1 Endpoint Visibility Requirement Background

Network administrator unable to visible the Internal network hardware, including endpoint, server and other network devices, so the unknown device unable to be controlled and it will bring the security risk to the internal network.If network administrator doesn't know the IP usage, resulting in a waste of IP resources

At the same time cause difficulties in management and operation.

Endpoint visibility: auto detect the type of endpoint, system and the related information and auto sort.

Chapter 2 Endpoint visibility function description

Endpoint visibility: auto detect the type of endpoint, system and the related information and auto sort.

There are two ways to realize the terminal identification function: active and passive

1. The proactive is to extend the detection mechanism developed through the nmap framework, mainly as follows:

onvif: camera standard protocol, detect and identify other dumb terminal device types;

SMB detection: mainly for MSFT PC, which can obtain information such as the host name, operating system, and working group of the host

SNMP: Available equipment: routing table, arp table, machine type, system description, mac address operating system identification;

2. Passively identify the terminal information by identifying the UA field in http traffic and the option field in dhcp data;

The active mode is to scan which segment of the IP is configured, and the passive mode requires traffic to pass through the AC

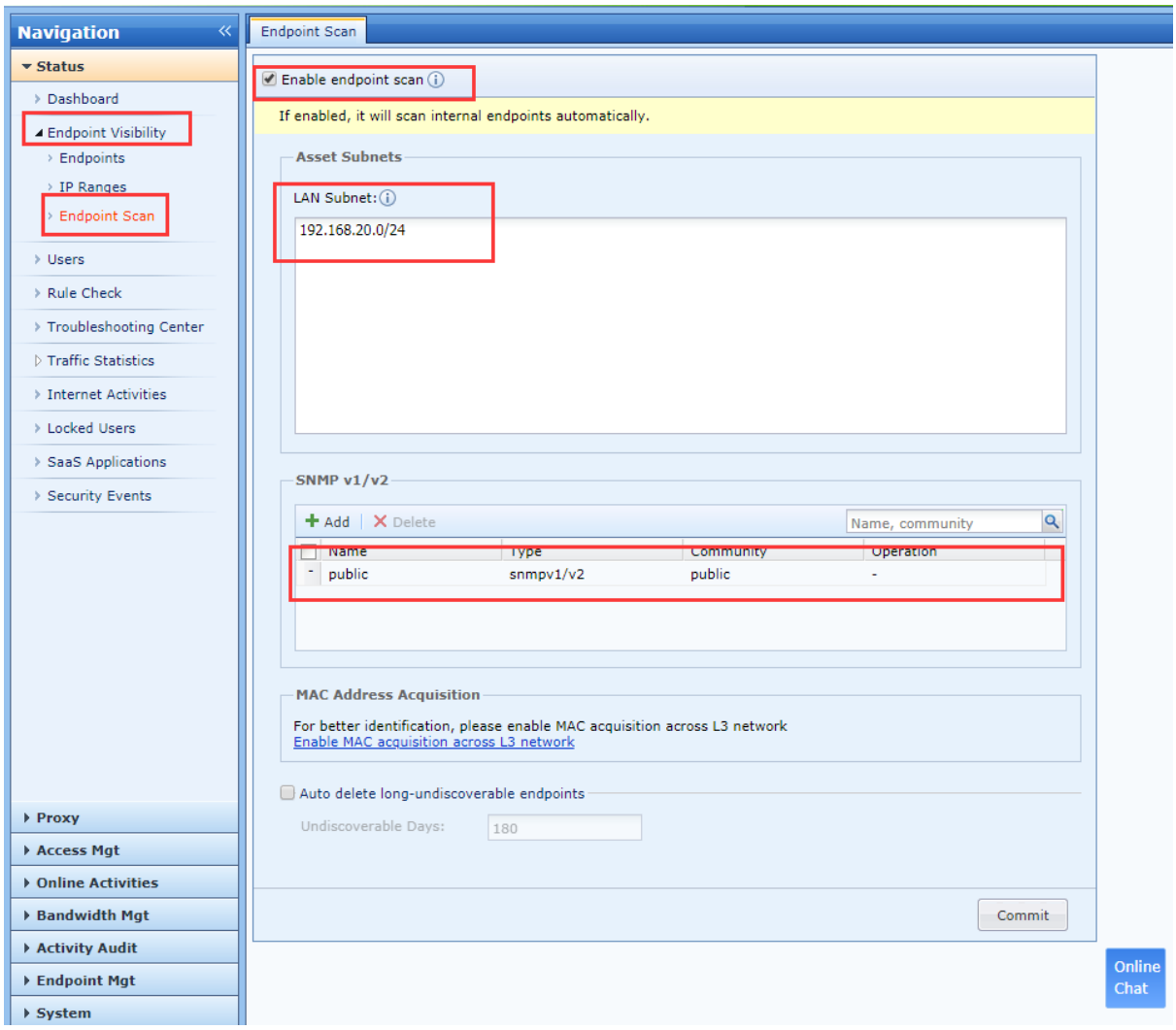
To accurately identify the MAC across the three-layer device, you need to enable the **MAC acquisition across L3 network**.

IP segment presentation mechanism in IP management

1. In the IP segment list, the 24-bit mask network segment where the IP is located will only be displayed when there is a surviving IP, or when it is recognized that the IP has traffic (the IP exists in online users or it is displayed in users who failed to access the network for 7 days) The network segment of the 24-bit mask where the IP is located will also be displayed;

Chapter 2.1 Configuration Guide

1. Navigate to the Endpoint visibility -> Endpoint scan and enable the endpoint scan function.
2. Configure the network segment that required to scan.
3. In order to improve the identification, it is required to enable the switch and enable the SNMP function and set the community string.
4. if required to enable the mac address in L3 environment, it required to enable the **MAC acquisition across L3 network** function

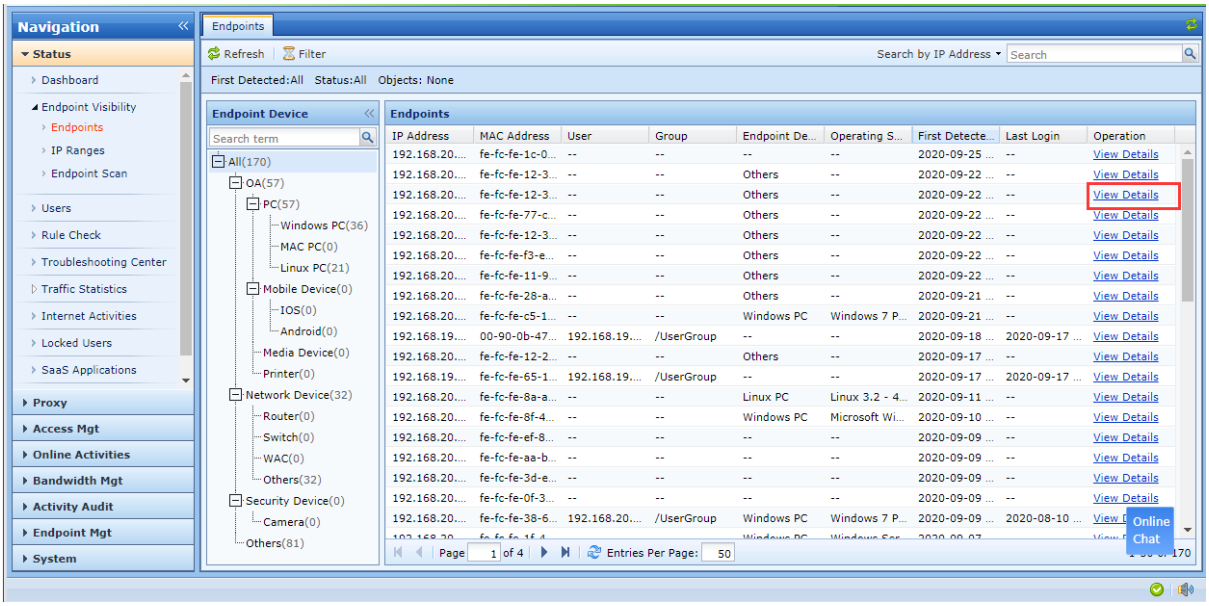


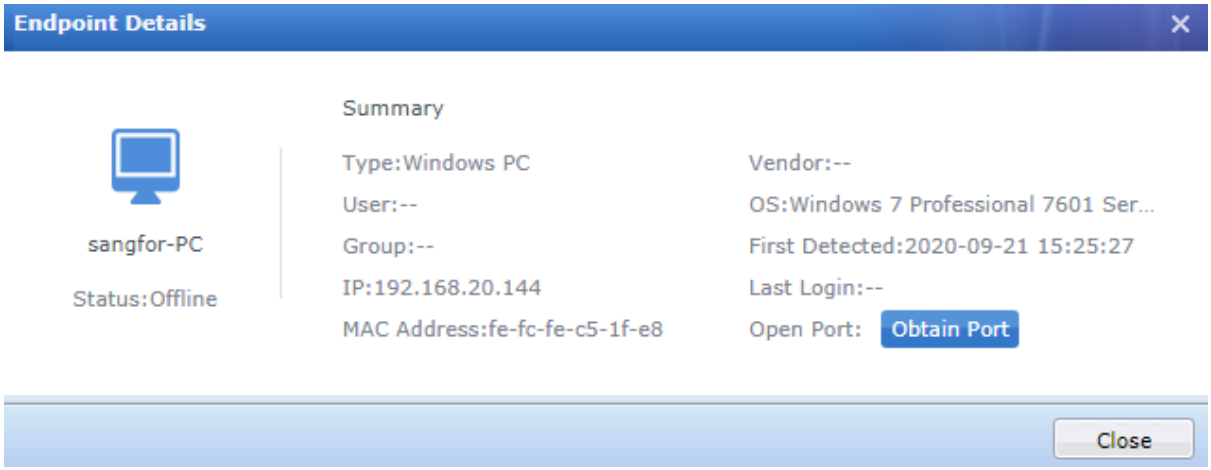
Chapter 2.1.1 Endpoint Identification result

Inside the endpoint list, you can see the type of endpoint, you can click on the detail to view the description

1. General endpoint and some network equipment will display names;

2. Online status: Online refers to whether there is the IP of the endpoint in the online user information. The presence of the IP indicates that the user has used the terminal to go online, and the user information and the status of the group will be displayed. Offline means that the endpoint IP is currently not used by users.





Chapter 2.1.2 Effect of IP ranges

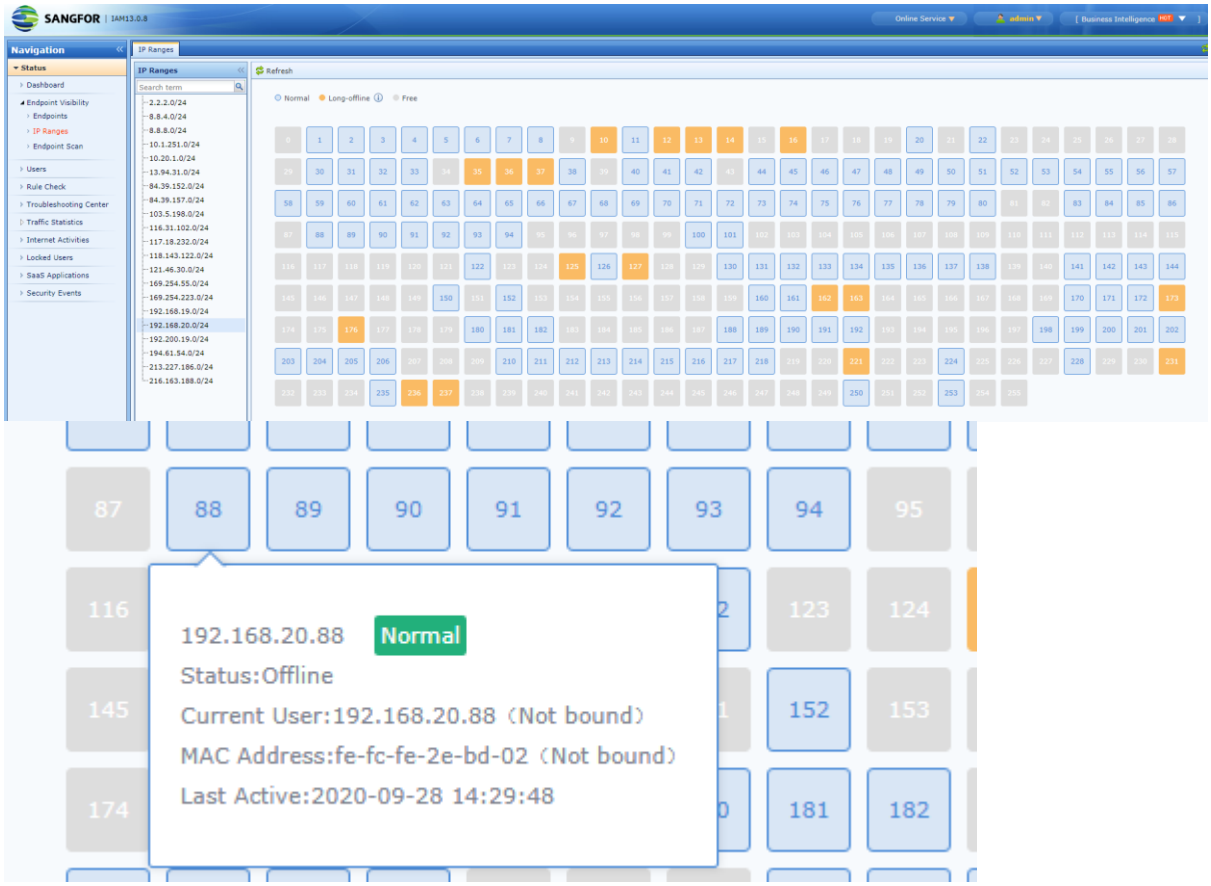
Navigate into the IP ranges,

click on each network segment to see the current IP segment address usage, click on a box to view the detailed usage

Normal use: refers to a period of time (the default is 30 days, configurable) to scan the IP to active, the online status is the same as previous chapter.

Free: Refers to the IP didn't use

Long offline: Refers to the IP that has been scanned for active before, and it is defined as offline if it is not scanned for a period of time (the default is 30 days, configurable).



Precaution:

1. Endpoint identification list only support to show maximum of 200, 000 IP addresses.
2. IAM will actively scan the Local network, If a firewall exists in the environment, it will affect the idenfication result, it also need to ensure customer allow to do endpoint scanning inside the encironment.
3. IP ranges support 1024 IP segments.
4. In L3 environment, it required to enable the mac address in L3 environment, it required to enable the MAC acquisition across L3 network function.
5. The endpoint type in the online user is not related to the operating system information in the endpoints of the entire network, two modules are independent
6. The endpoint scanning function of the entire network is enabled. If arp protection is enabled at the same time, the arp protection module will continue to alarm;