SANGFOR

Sangfor NGAF

Security Enhancement Guide

Product Version	8.0.47
Document Version	1.0
Released on	Feb. 28, 2023

Disclaimer

Products, services or features described in this document, whether wholly or in part, may be not within your purchase scope or usage scope. The products, services or features you purchase must be subject to the commercial contract and terms as agreed by you and Sangfor. Unless otherwise provided in the contract, Sangfor disclaims warranties of any kind, either express or implied, for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Unless otherwise agreed, this document is used for reference only, and all statements, information, and recommendations therein do not constitute any express or implied warranties.

Technical Support

For technical support, please visit: https://www.sangfor.com/en/about-us/contact-us/technical-support

Send information about errors or any product related problem to tech.support@sangfor.com.

About This Document

This is the guide for the security enhancement of the Sangfor Next-Generation Application Firewall(NGAF).

Intended Audience

This document is intended for:

- NGAF Users.

Note Icons

English Icon	Description
	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
	Indicates a hazardous situation, which if not avoided, could result in minor or moderate injury.
	Indicates a hazardous situation, which if not avoided, could result in settings failing to take effect, equipment damage, or data loss. NOTICE addresses practices not related to personal injury.
	Calls attention to important information, best practices, and tips. NOTE addresses information not related to personal injury or equipment damage.

Change Log

Date	Change Description
Feb. 28, 2023	This is the first release of this document.

Contents

1 Ports

Port	Function
53/udp	DNS Server
67/udp4	DHCP Server
68/udp6	DHCP Server
80/tcp	HTTPS business user authentication and decryption
81/tcp	Bridge mode http business user authentication and page customization
100/tcp	Authentication IWA
179	BGP Route
442/tcp	HTTPS business user authentication and decryption
443	Web UI
500 4500	ipsec vpn
546/udp4	DHCP Server
547/udp6	DHCP Server
1774/udp	Authentication ADSSO
1775/udp	Authentication ADSSO
1813/udp	radius SSO
4009	ipsec vpn
4420/tcp	Bridge mode https business User Authentication and Decryption
4460	Use for Central Manager
7443	Use for Central Manager, Cyber Command
22345/tcp	SSH Port

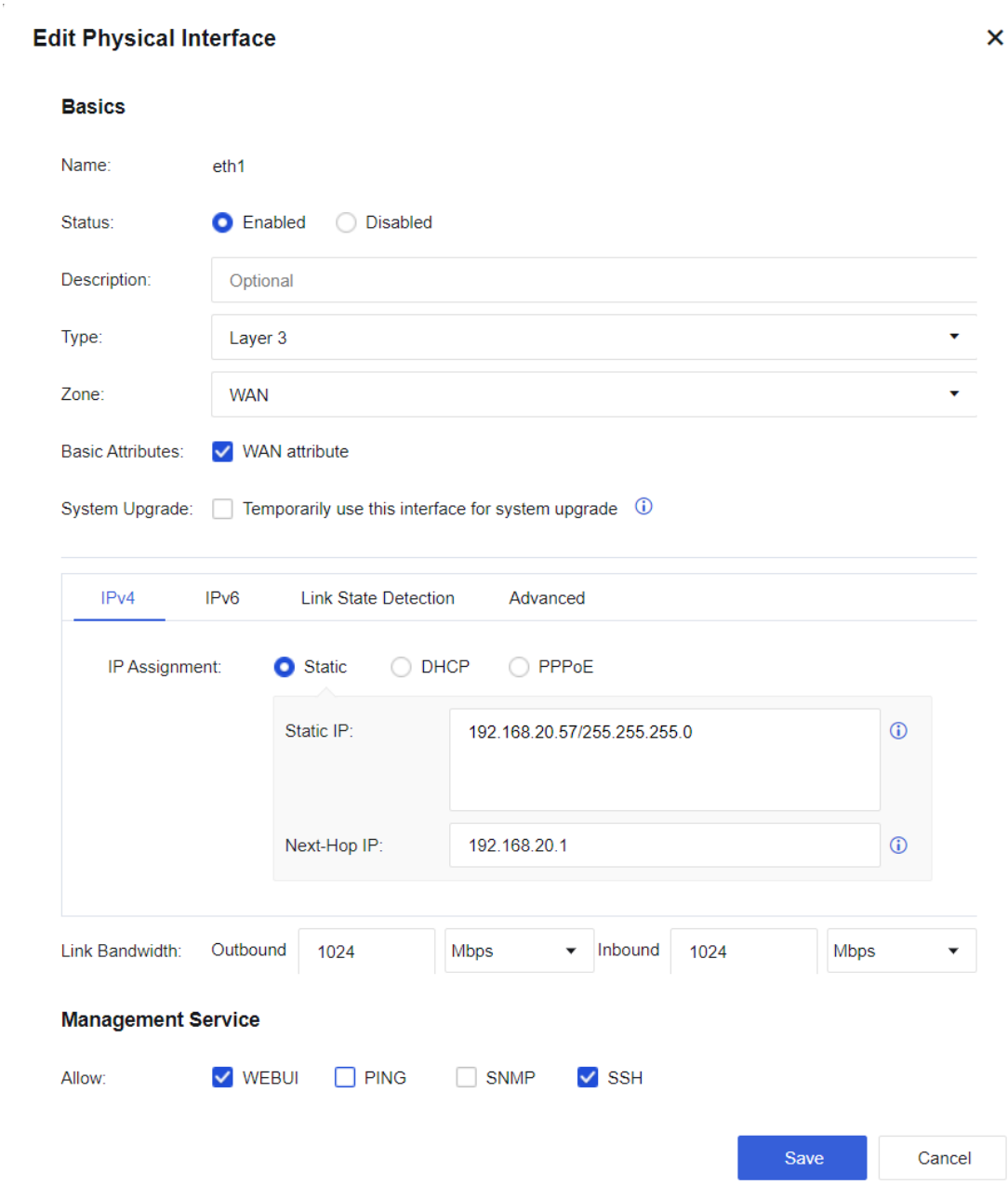
2 Domain Names

Domain Name	Port	Function
update1.sangfor.net	80 & 443	Database Upgrade
121.46.26.221	80 & 443	
update2.sangfor.net	80 & 443	
222.126.229.180	80 & 443	
update3.sangfor.net	80 & 443	
118.143.122.147	80 & 443	
download.sangfor.com	80 & 443	
download.sangfor.com.cn	80 & 443	
upd.sangfor.com	80 & 443	Database Upgrade and Neural-X File Feedback
upd.sangfor.com.cn	80 & 443	
intelligence.sangfor.com	80 & 443	
intelligence.sangfor.com.cn	80 & 443	
notify.sangfor.com	80 & 443	
tamper.sangfor.com	80 & 443	
tamper.sangfor.com.cn	80 & 443	
analysis.sangfor.com	80 & 443	
analysis.sangfor.com.cn	80 & 443	
auth.sangfor.com	80 & 443	Neural-X Authentication
clt.sangfor.com	80 & 443	Neural-X Integration
clt.sangfor.com.cn	80 & 443	
device.scloud.sangfor.com	80 & 443	Platform-X Integration
device.scloud.sangfor.com.cn	80 & 443	
license.sangfor.com	80 & 443	License Verification
saas.sangfor.com.cn	80 & 443	SAAS Service
gcs.sangfor.com	80 & 443	System Upgrade
sp.sangfor.com.cn sp.sangfor.com	80 & 443	SP Package Update

3 NGAF Security Enhancement

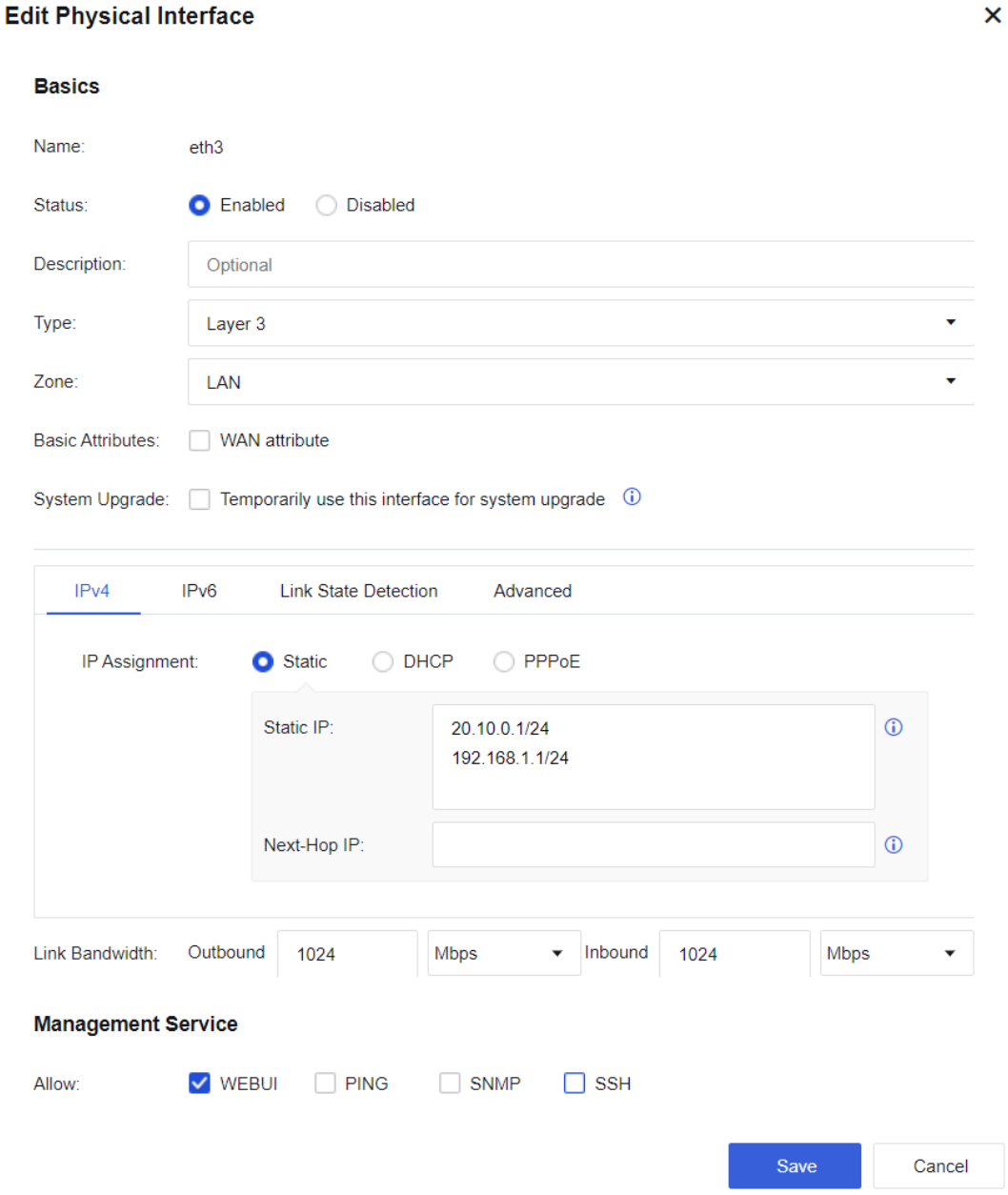
3.1 Remote Control

In the external network scenario, navigate to **Network > Interfaces > Physical Interfaces** and click **Edit** of WAN. It is recommended to disable **System Upgrade** and **SNMP**, enable **SSH** and **WEBUI.**

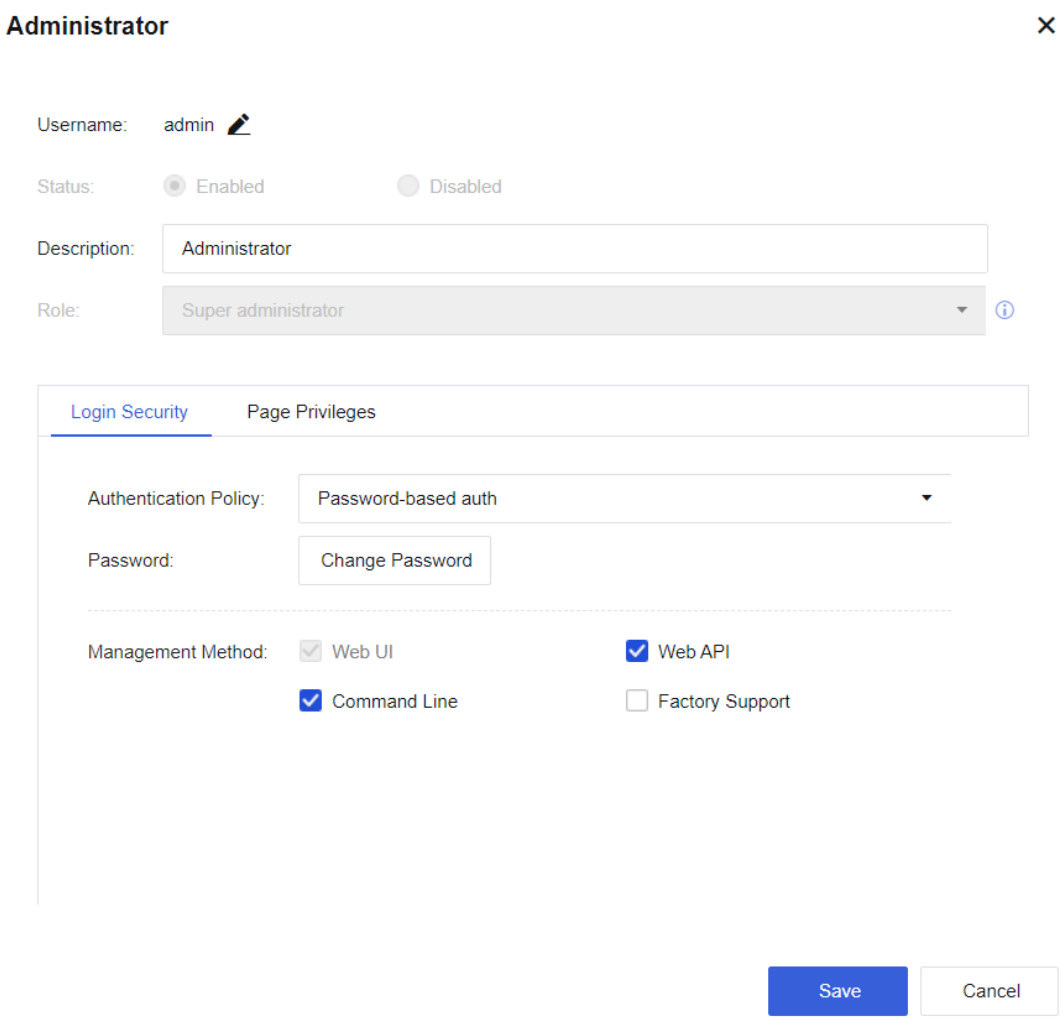


In the Intranet scenario, navigate to **Network > Interfaces > Physical**

Interfaces and click **Edit** of LAN. It is recommended to enable **WEBUI** only and disable the **System Update, SSH**, and **SNMP**.



When you have multiple accounts to manage NGAF, please manage the permissions of all Administrator accounts, and ensure to allow **WEBUI** as the **Management Method** only.



3.2 Administrator Account

Change the administrator's default account password and ensure that the password is stored securely. For a network with multiple administrators, create different levels of accounts for different roles or administrators.

Super Administrator: Has full permissions.

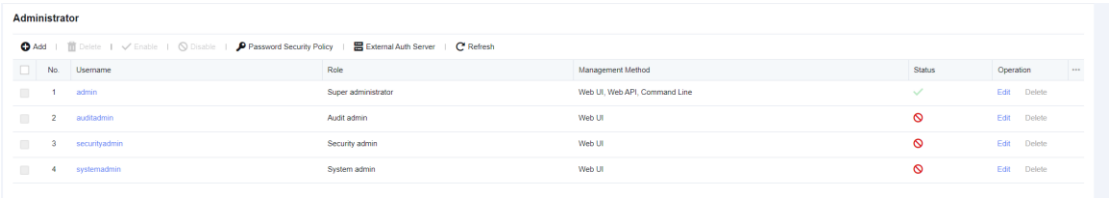
System Admin: Has the permission to manage basic network configuration, user management, and other non-security policies.

Security Admin: Has permission to view and modify security policies and view logs.

Audit Admin: Has permission to view and modify built-in data centers.

Three things need attention and action:

1. Confirm with the user whether there are redundant accounts. If yes, it is recommended to delete the unused accounts.
2. Check and confirm with the user whether the existing account has a weak password. If yes, it is necessary to assist the user in modifying the password.
3. If needed, you can modify or rename the Super Administrator account to meet a stricter management requirement.



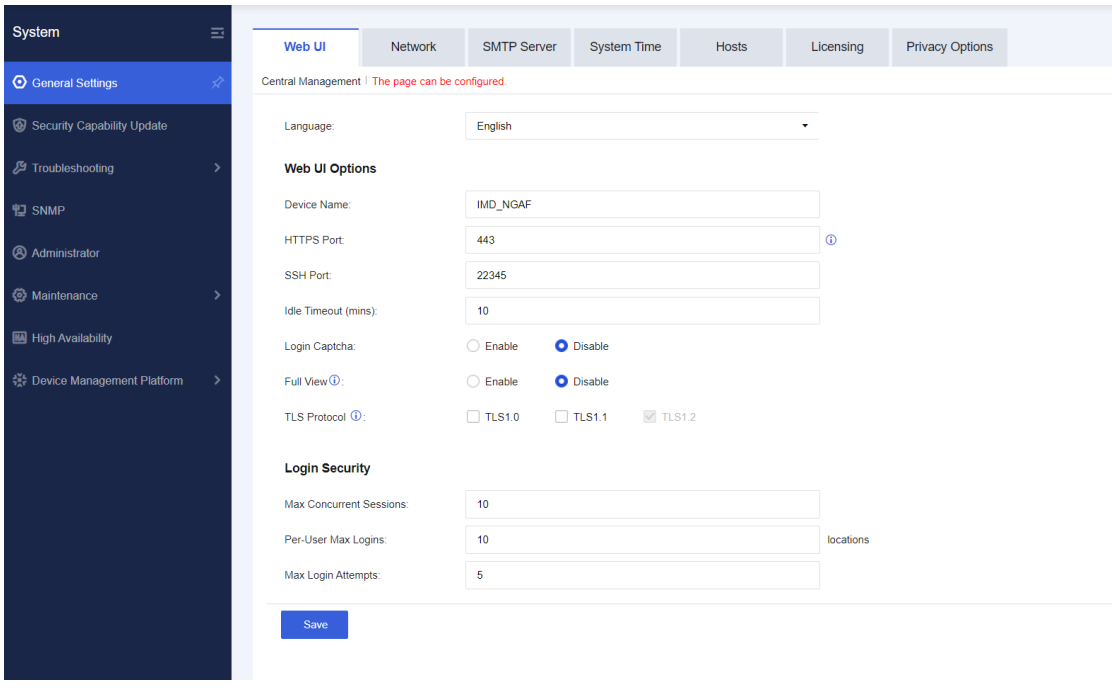
3.3 Use More Secure Login Method

Navigate to **System > General Settings > Web UI** for the following settings:

It is recommended to enable **TLS 1.2**, and disable traditional TLS1.0 and TLS1.1.

It is recommended to enable **Login Captcha**, which will increase the security of the console login.

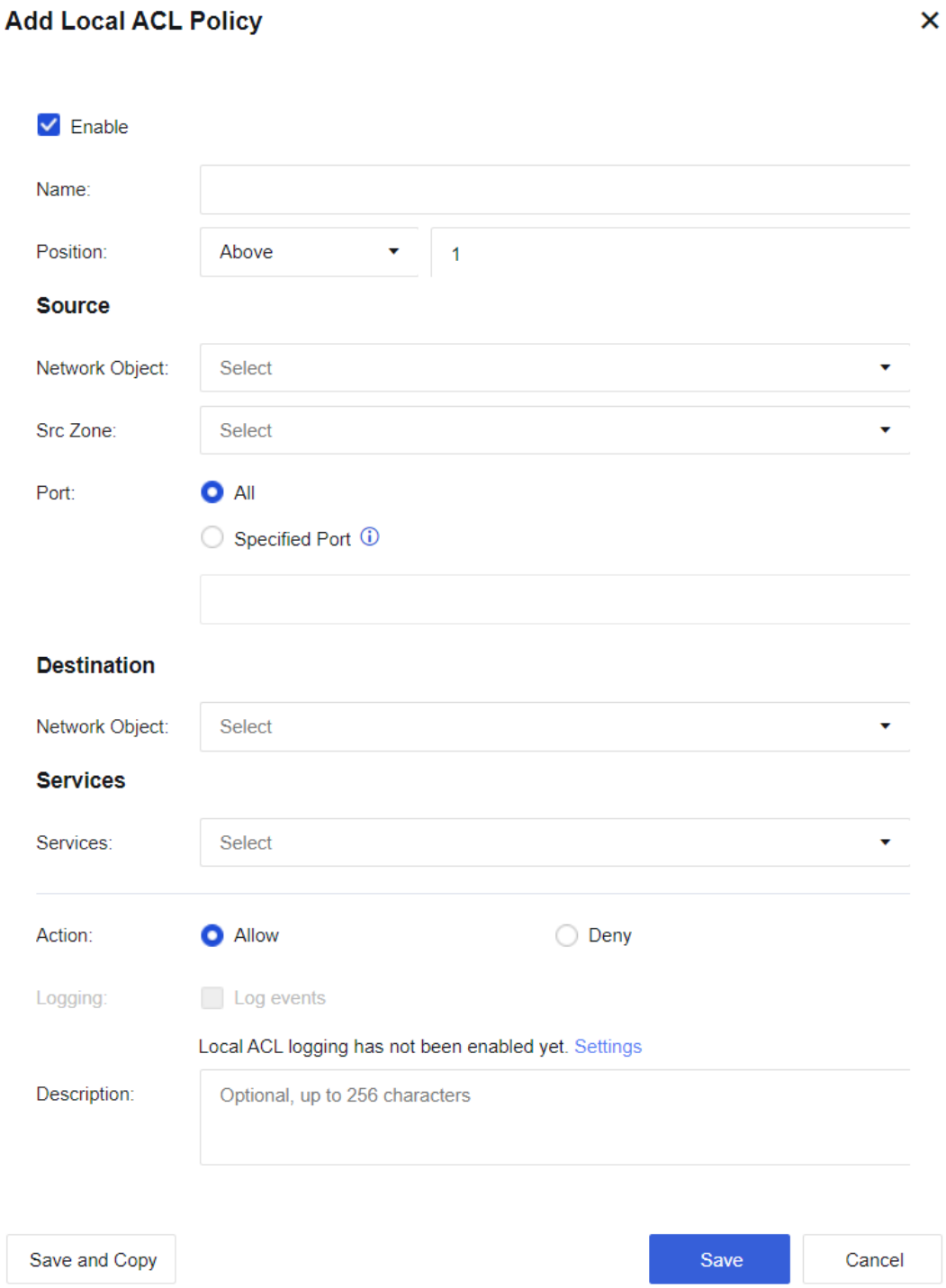
It is recommended to use **Max Login Attempts**, which will help prevent brute force cracking of console login accounts and passwords.



3.4 Login IP Restriction

Restrict the login IP of the console account

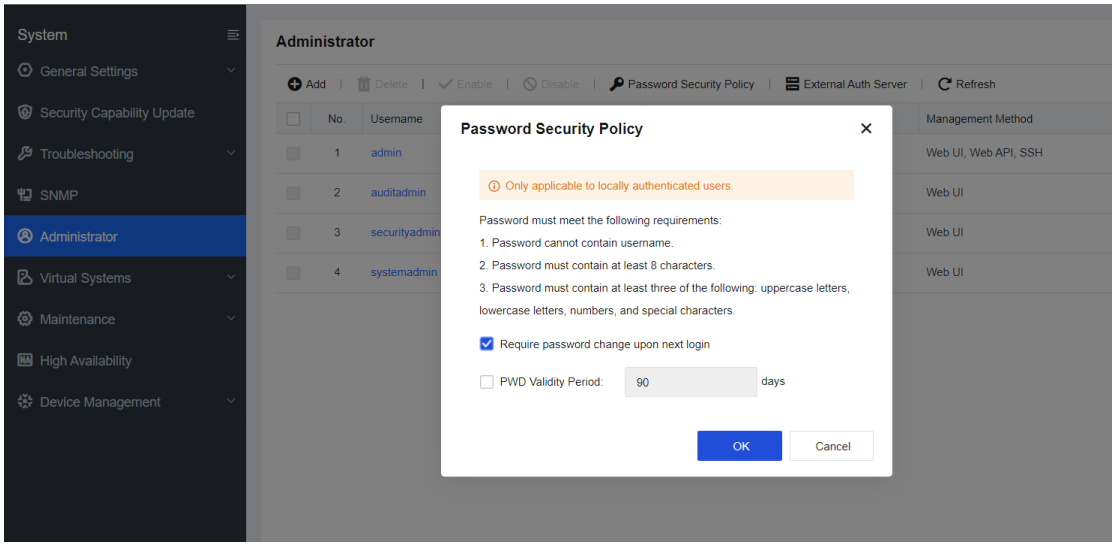
Ensure only the IP address configured in the **Network Object** can log in to the NGAF, as shown below. Navigate to **Policies** > **Access Control** > **Local ACL** page, and configure the Network Object that is allowed to log in.



3.5 Console Password Security Policy

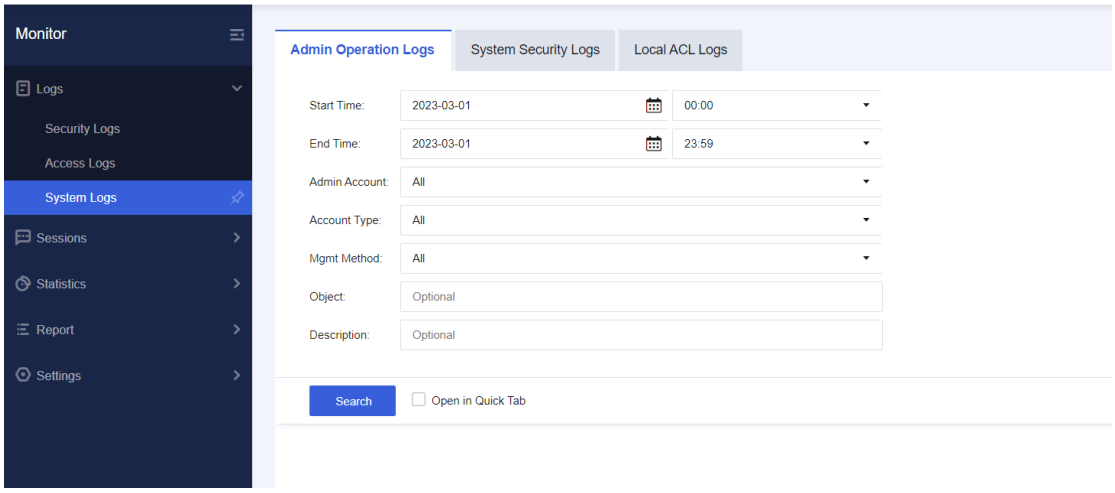
Navigate to the **System > Administrator** and click **Password Security Policy** to configure the password security policy.

It is recommended to tick the **PWD Validity Period** and set the value to **90** days.



3.6 Monitor Administrator Operation Logs

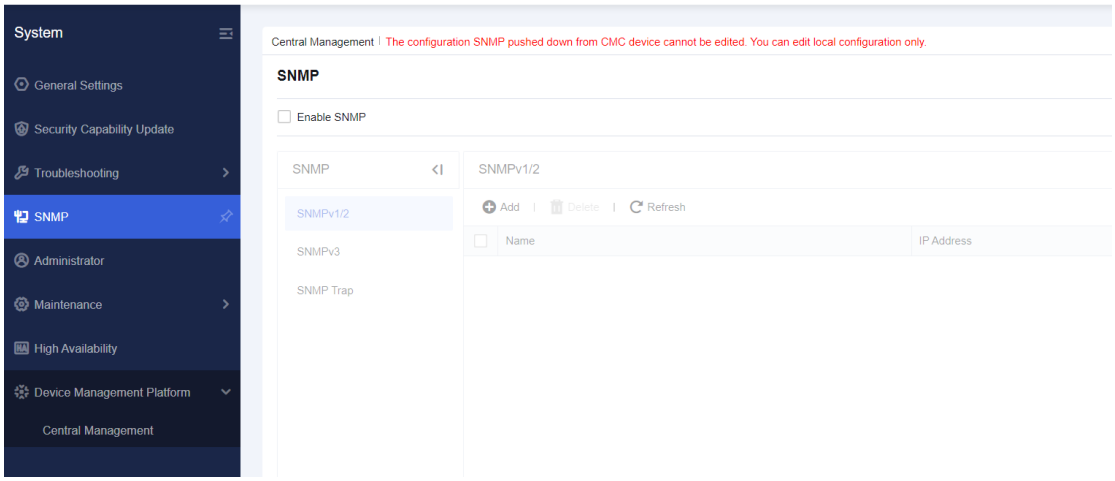
In the daily maintenance of NGAF, it is important to check the administrator operation log. You can check whether there are multiple errors in accessing the console and the operation records of different administrators. This information will give you a more comprehensive understanding of **Who** uses NGAF. Path: **Monitor > Logs > System Logs > Admin Operation Logs**.



3.7 SNMP Monitoring

Navigate to the **System > SNMP** to see whether NGAF is connected to the SNMP device to monitor the status of the NGAF.

Suppose your NGAF is not connected to the SNMP device to monitor the Running Status. **Do not** configure any SNMP policies.



3.8 Firmware Upgrade

Please visit Sangfor Community to get the latest NGAF firmware; updating your NGAF firmware to the latest version is recommended. The most recent version is the most stable and has the most bugs fixed and vulnerabilities removed.

3.9 Follow PSIRT Information

Please pay attention to various notifications, such as emails from Sangfor staff. For security incidents that seriously affect Sangfor products, Sangfor engineers will take the initiative to notify you by email and other means and assist you in fixing these security incidents.

SANGFOR