GRUNDIG

Network Security Hardening Guide for Smart Line Series

Table of contents

Applicable products: Smart Line cameras and NVRs
Target groups: end users, integrators

1. Introduction

To improve the network security of user devices and prevent illegal access, malicious attacks or data leakage risks, we recommend that users perform comprehensive security configuration reinforcement before deploying devices. This guide will introduce recommended configuration items for accounts, passwords, services, remote access, etc. to help you reduce network security risks.

2. Security Features Overview
2.1 Fixed security features
2.2 Configurable security features
2.3 Password Encryption
2.4 Configuration Parameter Encryption
2.5 Editing and backup video encryption

2. Initial access and device activation

When the device is powered on for the first time or restored to factory settings, the user needs to activate the device and set an administrator password. Before activation, the device cannot perform any functions.

2.1 Strong password setting

Passwords are the most important security factor for network devices. Please use strong passwords that are difficult to predict and keep them safe to prevent them from being leaked.
Recommended password strength: no less than 8 characters, including a combination of uppercase and lowercase letters, numbers, and special characters.

- **Recommended update cycle:** once every 6 months for normal business scenarios and once a month or week for high-security scenarios.
- **Avoid using:** default passwords, usernames with the same username, consecutive characters (such as " 123 “, "321”), repeated characters (such as "aaa", "555"), and weak password dictionaries (such as admin123).
- **Minimum password strength requirement:** no less than 8 characters, including any combination of uppercase and lowercase letters, numbers, and special characters

✅ Example: Gd3se!A9

2.2 Security Questions & GUID File

- **Certificate file:** It is recommended to export the certificate file immediately after activation so that it can be used to retrieve the password when it is forgotten.
- **Security questions:** It is recommended to configure 3 questions as a backup verification method. The answers must be kept properly and cannot be repeated with commonly used information.

2.3 Password Reset Options

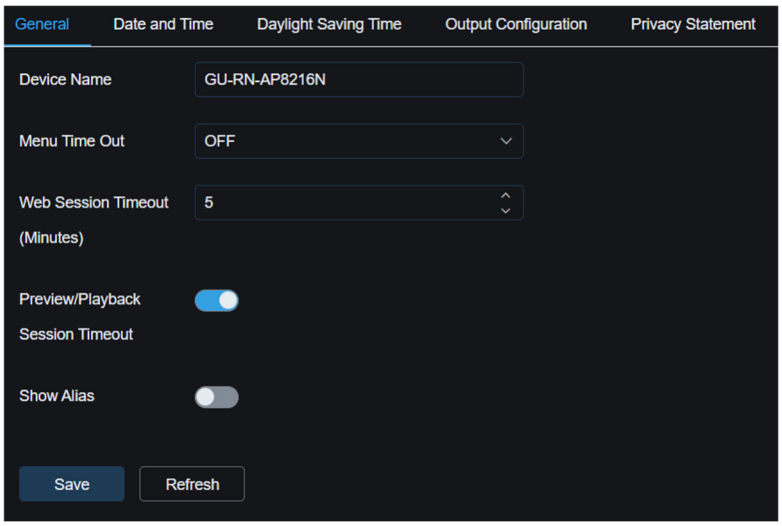
If the administrator forgets the password, he can reset it in the following ways:

Reset method	Prerequisites	Recommended level
Importing certificate files	Exported on activation	✅ Recommend
Answer security questions	Configured Issues	✅ Recommend
Local factory reset	Have physical access	⚠ Last resort only

2.4 Auto Logout Configuration

For the device UI, it is recommended to enable the "Auto Lock" function, which will automatically log out the current user after a period of inactivity in the system, effectively preventing the risk of the console being left in use.
Recommended time: 5 minutes
Path: **System > General > Auto Lock**

For WEB browsers, it is recommended to enable the " Web Session Timeout " function, which will automatically log out the current user after a period of no operation in the setting menu.



If not check Preview Session Timeout, the system will retain the session when there is a stream on

the Preview and Playback pages, and the automatic logout function will be invalid during this period. If check it, even if the user is previewing the stream on the Preview page, if not operate the mouse, it will automatically log out of the system after the timeout.

IPC currently does not have an open settings page, and the default is to automatically time out and log out after 5 minutes.

3. User Account & Permission Management

To avoid risks such as account abuse and unauthorized access, it is recommended to properly configure account and permission levels based on user usage scenarios.

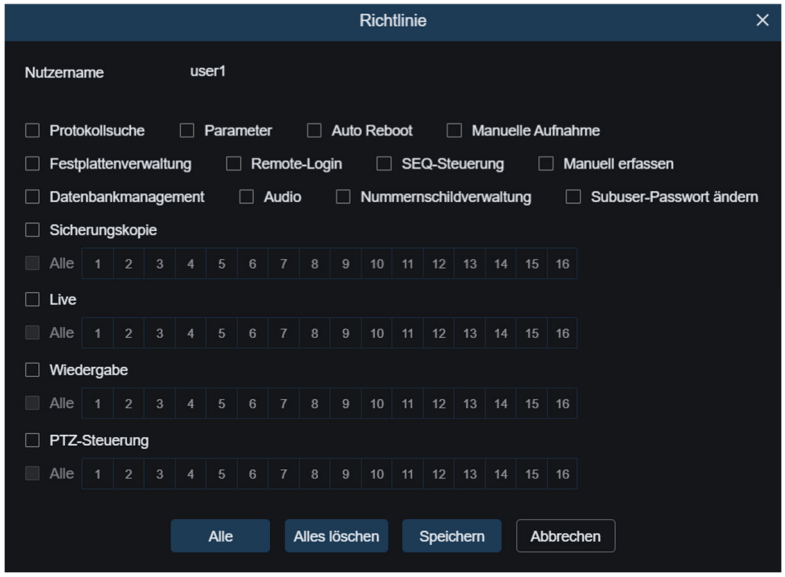
3.1 User Roles

The system supports the following two types of users by default:

User Type	Permission levels	Typical Uses
Administrator	Full permissions	Installation, Configuration, and Upgrade
Ordinary user (User)	Medium permissions	Viewing and Portion Control

3.2 Permission configuration and local preview settings

Administrators can set refined operation permissions and preview ranges for different users to prevent irrelevant personnel from accessing key screens.
Recommended operation path:
System > Multi-user > Policy

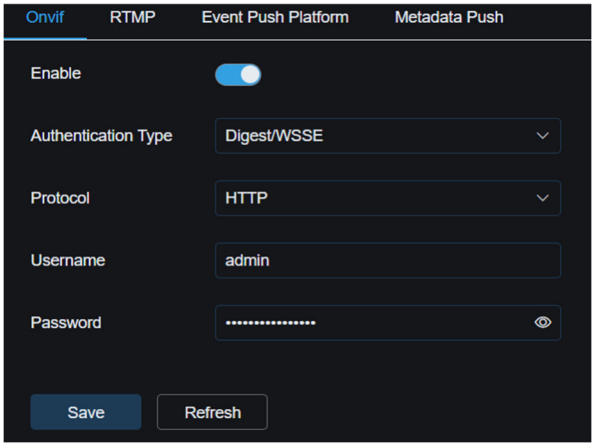


3.3 Deleting Idle or Unused Accounts

It is recommended to regularly clean up user accounts that have not been logged in for a long time or are invalid to reduce the potential attack surface.

3.4 ONVIF third-party access user management

If you need to use the ONVIF protocol to connect to a third-party platform, it is recommended to create a special account with limited permissions and rotate the password regularly. Currently, there is a separate account designed for the ONVIF protocol on the NVR.
Recommended operation path:
Network > Platform Access > ONVIF



Camera devices do not have the function of separate ONVIF accounts.

4. Remote Access Control

Remote access is one of the main targets of network attacks, and it is recommended to adopt multiple methods to limit unauthorized remote connections.

4.1 Login Failure Lockout

To prevent brute force attacks, the device has a default "login failure lock" function.

Maximum number of failures	**Lock Time**
5 times	5 minutes

There is currently no UI page for user settings.

4.2 Disable Unused Remote Services

If cloud access, mobile access and other functions are not enabled, it is recommended to disable the relevant protocols:

- **UPnP automatic port mapping** (strongly recommended to turn off)

4.3 IEEE 802.1x

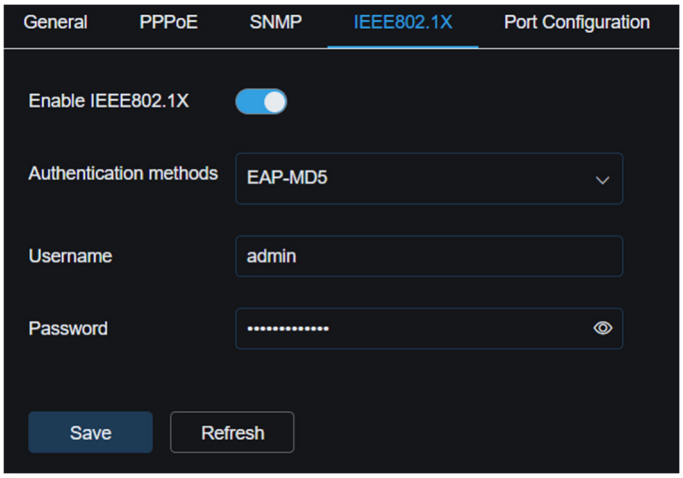
The role of IEEE 802.1X network authentication service is to strictly verify the network access rights of users or devices through a port-based access control mechanism, ensuring that only legitimate identities can access network resources after passing authentication, controlling the access of illegal devices, and improving the overall security performance of the network.

The camera device supports the IEEE 802.1X standard. After enabling this function, user authentication is required when connecting the camera to a network protected by IEEE 802.1X. Users can configure 802.1X settings, including authentication method, EAPOL version, user name, password, etc. Some authentication methods require importing client certificates and root certificates.

If you are not familiar with the network environment, it is recommended not to select EAP-MD5 and EAP- MSCHAPv2, which are two authentication methods with security risks.

Recommended operation path:

Network > General > IEEE802.1X



5. Network Service Hardening

Network services are the window for devices to interact with the outside world, and are also the entry point for attacks. It is recommended to enable only necessary services and limit their authentication methods and access scope.

5.1 Disable Unused Services

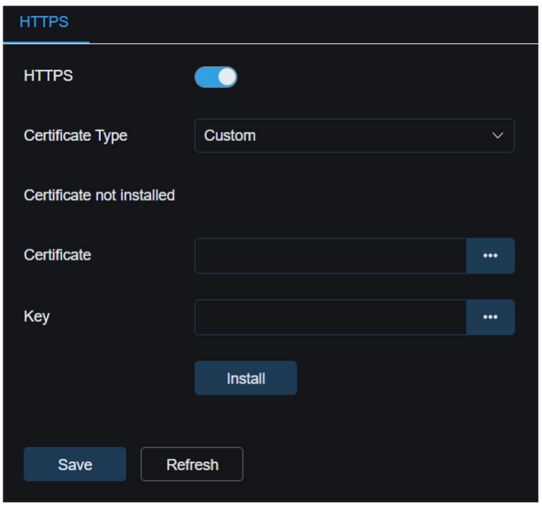
The following services should be disabled by default unless they are really required by the business scenario:

Service Name	describe	Recommendation Status
Telnet	Plain text remote login protocol	⚠ If you need to limit the access time, close it in time
SSH	Secure Terminal Remote Login Protocol	⚠ If you need to limit the access time, close it in time
UPnP	Automatic port mapping, easy to be hijacked	✖ Disable

5.2 Enable HTTPS and Manage Certificates

It is recommended to enable HTTPS service and configure a trusted certificate. We will enable https and http by default, but it is still recommended that you use https to access the device.
The device is configured with a self-signed root certificate and server certificate by default, and the certificate will be automatically updated after it expires. However, the browser will prompt a security risk. **It is recommended that you export the root certificate after logging into the device for the first time (there is no way to export it now),** and then install the root certificate to a trusted root certificate authority through the browser. When you log in to the device again, the browser will not prompt a security risk.

If you do not trust the self-signed certificate, it is recommended to import a certificate issued by a CA to improve the trust level. The device is not configured with a domain name. When you create a CSR certificate application file, it is recommended that you configure the IP of the current device in the SAN.
Recommended operation path:
Network > HTTPS > HTTPS



5.3 Set the Authentication Method

For services such as HTTP, HTTPS, RTSP, and ONVIF, a secure authentication method needs to be set.

Common authentication methods include Basic, Digest, Digest-md5, Digest-sha256, etc., and onvif services also have WSSE authentication. Basic authentication is the most basic authentication method, which uses plain text to transmit user names and passwords. In our system, it is strictly prohibited to use Basic authentication. When there is a Digest-sha256 option, it is strongly recommended to select Digest-sha256.

Except for the separate ONVIF service configuration page, other services share a set of authentication services, which are currently not enabled on the page and the default is Digest-md5 authentication method.

5.4 Open Ports

The default ports opened by the device are as follows:

port	Service Name	describe	Port Features
80	HTTP	HTTP service port	User can change the port
443	HTTPS	HTTPS service port	User can change the port
554	RTSP	RTSP service port	User can change the port
3702	Onvif	Onvif device detection WS-Discovery	Unchangeable
9555	Multicast	Multicast port for device detection service	Unchangeable

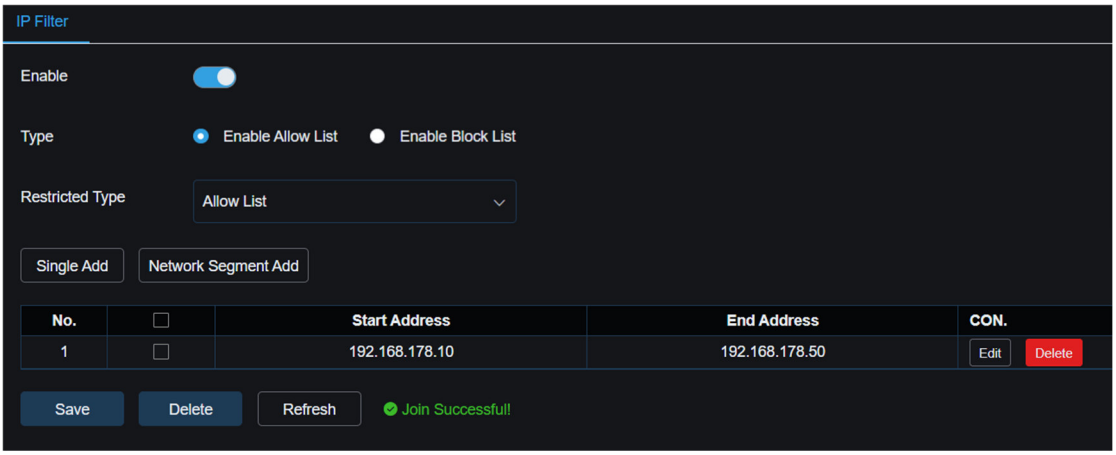
By default, only the required ports are opened. After the service is applied, they should be closed in time to avoid exposing too many ports. At the same time, it is also necessary to change the commonly used ports such as 80 to uncommon ports in time to prevent others from exhaustively listing the ports.

5.5 IP Filtering Function

The whitelist and blacklist in IP filtering function are commonly used access control mechanisms in network security.

type	Admission Logic	Applicable scenarios
Whitelist	Only allow specified IP addresses to access, and deny all others	Used when access sources (such as internal systems, API interfaces) need to be strictly restricted or when defending against unknown threats
Blocklist	Block access from specified IP addresses and allow access to all others	Use this feature when you need to block known malicious IP addresses (such as DDoS attack sources and crawlers) or reduce the risk of misblocking.

When IP filtering is enabled, each IP address or IP range added to the whitelist "allow list" or blacklist "deny list" will be allowed or denied access to the device, respectively.
Recommended operation path:
Network > IP Filter > IP Filter



5.5 Service Security

By default, only basic services are enabled on the device, including: WEB service, RTSP service, ONVIF service, device search service, and P2P service.

In fact, we support many services and provide users with more choices. When using, it is recommended that users prefer secure configuration to prevent information leakage.

5.5.1 FTP Client Service

By starting the FTP client function, you can transfer the device's alarm pictures and videos to an external FTP server. FTP communication is not encrypted and there are risks in using it. If there is an SFTP option, it is recommended to use SFTP. If not, you should close the FTP function in time after use to prevent information theft.

5.5.2 Email Service

Enable the email service to send the device's alarm messages and alarm pictures to emails. Email servers that do not support encryption may cause the risk of information leakage during use. It is recommended that users choose an email server that supports SSL/TLS encryption, and then select SSL or TLS encryption in the Email client configuration.

5.5.3 SNMP Service

By enabling the SNMP service, you can obtain device information and perform unified device management. It is recommended to choose the V3 service instead of the V1/V2 service, because in V1/V2, the data is not encrypted and the data packets may be eavesdropped and tampered. The SNMP V3 service has encryption and anti-tampering functions.

5.5.4 HTTPS Service

By default, http and https services are enabled. It is recommended that users use https to access the device.

5.5.5 RTSP OVER HTTPS Service

RTSP streams are not encrypted, so user information and stream data may be tampered with in RTSP. It is recommended to use RTSP over HTTPS to access RTSP streams when HTTPS service is enabled.
The specific access methods are as follows:
https://ip:port/rtsp/streaming?channel=1&subtype=A
A: 0(main stream), 1(sub stream), 2(mobile stream)

5.5.6 DDNS Service

The DDNS service can apply for a domain name for the device, and then access the device through the domain name, regardless of how the IP changes. The service is being upgraded for security, and users are advised to enable it only when necessary.

5.5.7 RTMP Service

It is a streaming service. When this service is enabled, the audio and video can be pushed to the user's RTMP streaming server. The user can view the RTMP stream in real time. This service is undergoing security upgrades, and users are advised to enable it only when necessary.

5.5.8 Event Push Service

It is an event push service. When this service is enabled, various alarm messages and pictures can be pushed to the user's server. This service is undergoing security upgrades, and users are advised to enable it only when necessary.

6. Logs and Audit Recommendations

Audit logs are an important means of discovering anomalies and obtaining security evidence. Audit logs can improve system security, enhance system stability, and meet the security and compliance requirements of equipment. For security equipment, log storage space is limited, so it is recommended that you export and save them regularly.

6.1 Log Type

The device records the following types of logs:

type	**describe**
System log	System startup, shutdown, upgrade, time calibration and other system logs
Configuring Logging	The operation log of each configuration performed by the user on the configuration page
Alarm log	various deployment events, access anomalies, etc.
User Logs	various logins and logouts, user locks, and user information modifications
Video Log	Search, playback, backup and other operation logs
AI Log	Trigger records of various AI deployment events
Storage logs	Hard disk and SD card related logs

6.2 Log Search and Export

It is recommended to export the log files once a month and keep them properly:

- Support filtering by time/type;
- Support exporting to csv file;
- Supports local viewing or remote downloading.

7. System Recovery and Upgrade Suggestions

To ensure the long-term safe and stable operation of the system, it is recommended to regularly check the firmware version, perform security upgrade operations, and understand the system recovery mechanism.

7.1 Factory Reset and Parameter Clearing

The device provides different factory reset operations as shown in the following table. Select the appropriate reset method.

Way	Operation Effect
Restore Defaults	Keep network/user configuration and only restore other settings
Factory settings	Clear all parameters, including network/IP/user, etc.
Restore to inactive state	Administrator password recovery, need to reset password

7.2 Firmware Upgrade Suggestions

To protect the security of user devices, we encrypt and sign the firmware package. After the device receives the firmware package, it will verify the signature and decrypt it, which can effectively prevent the firmware package from being tampered with.

- **Check official firmware versions regularly** and give priority to security update versions;
- **Only download/OTA firmware from the official website,** and do not use unofficial upgrade packages;
- **Back up important configurations before upgrading;**
- **The upgrade process must not be interrupted by power or network outages.**

8. Cloud Service Security

8.1 2FA Two-Factor Authentication

After turning on 2FA two-factor authentication, when logging into your account remotely, you will need to verify again using the email verification code. This feature is turned on by default and can be turned off manually by the user.
It is recommended that you check the list of trusted devices regularly and delete any devices that are no longer trusted.
It is recommended to enable face/fingerprint verification to protect the app.

9. Recommended Configuration Checklist

The following is a list of recommended network security configurations ✅. It is recommended to check each item during device deployment and annual inspections:

project	Recommendation Status	Current Configuration
Change the default password	✅ Strong passwords are enabled	□ Yes / □ No
Enable automatic logout after timeout (≤ 5 minutes)	✅ Open	□ Yes / □ No
Configure security questions for resetting passwords and exporting certificates	✅ Already set	□ Yes / □ No
Deleting Idle User Accounts	✅ Cleaned	□ Yes / □ No

project	Recommendation Status	Current Configuration
Correctly configure access rights for ordinary users	✅ Configure on demand	□ Yes / □ No
Enable HTTPS and install the certificate	✅ CA certificate or self-signed certificate	□ Yes / □ No
Enable RTSP/HTTP Digest authentication	✅ Enable	□ Yes / □ No
Disable protocols like UPnP/Telnet/Control4 etc.	✅ Disable	□ Yes / □ No
Configuring IP Whitelist	✅ Limit external access	□ Yes / □ No
Disable unnecessary services (HTTP/SNMP/FTP, etc.)	✅ closure	□ Yes / □ No
Enable abnormal login lock mechanism	✅ Enabled	□ Yes / □ No
Logs are saved for ≥ 30 days and can be exported	✅ Can be checked and guided	□ Yes / □ No
The firmware version is the latest security version	✅ Updated	□ Yes / □ No
Enable 2FA two-factor authentication	✅ Opened	□ Yes / □ No

Notes:

- The above configuration items may vary slightly depending on the specific product functions. Please refer to the product manual for actual supported items.
- If the device has been connected to the cloud platform, please check the cloud account binding and alarm mechanism simultaneously.

🟢 **Conclusion of the document:**

This guide is designed to help users improve the level of device network security protection in a standardized and operational way. We will continue to update the version based on new threats, industry compliance requirements and product capabilities. If you need further technical support, please contact the technical representative or service platform in your region.