DSS Express

Quick Deployment Manual

Foreword

General

This user's manual introduces the functions and operations of DSS Express (hereinafter referred to as "the system" or "the platform").

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
⚠ DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
⚠ CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
⊙━ TIPS	Provides methods to help you solve a problem or save time.
📖 NOTE	Provides additional information as a supplement to the text.

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF

format) cannot be opened.

- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.
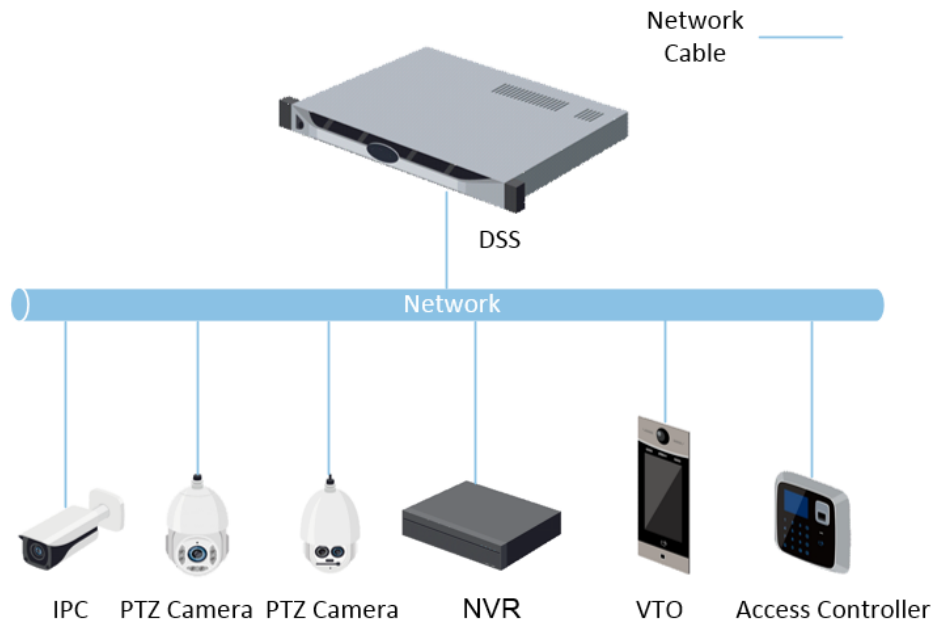
Table of Contents

1 Introduction

DSS platform supports standalone deployment, and LAN to WAN mapping.

Standalone Deployment

For projects with a small number of devices, only one DSS server is required.

Figure 1-1 Standalone deployment

2 Standalone Deployment

2.1 Server Requirements

Table 2-1 DSS Express hardware requirement

Parameter	Hardware Requirement	Operating System
Recommended configuration	- CPU: Intel® Core(TM) I7-9700K CPU@3.60GHZ - RAM: 8 GB - Network card: 1 × Ethernet port @ 1000 Mbps - Hard drive type: 7200 RPM Enterprise Class HDD 1 TB - DSS installation directory space: 500 GB	Windows 7 and above
Minimum configuration	- CPU: Intel® Core(TM) I5-9400 CPU@2.90GHZ - RAM: 8 GB - Network card: 1 × Ethernet port @ 1000 Mbps - Hard drive type: 7200 RPM Enterprise Class HDD 1 TB - DSS installation directory space: 200 GB	Windows 7 and above

□□

- Face recognition images, videos, and files cannot be stored on the system disk and DSS installation disk. Make sure that your server has at least 3 HDD partitions to ensure that these files can be stored.
- For best performance, we recommend adding additional hard drives to store pictures.

2.2 Installing DSS

Prerequisites

- You have downloaded the DSS installer from the official website or received it from our sales or technical support.
- You have prepared a server that meets the hardware requirements mentioned in "2.1 Server Requirements", and the server IP address is configured.
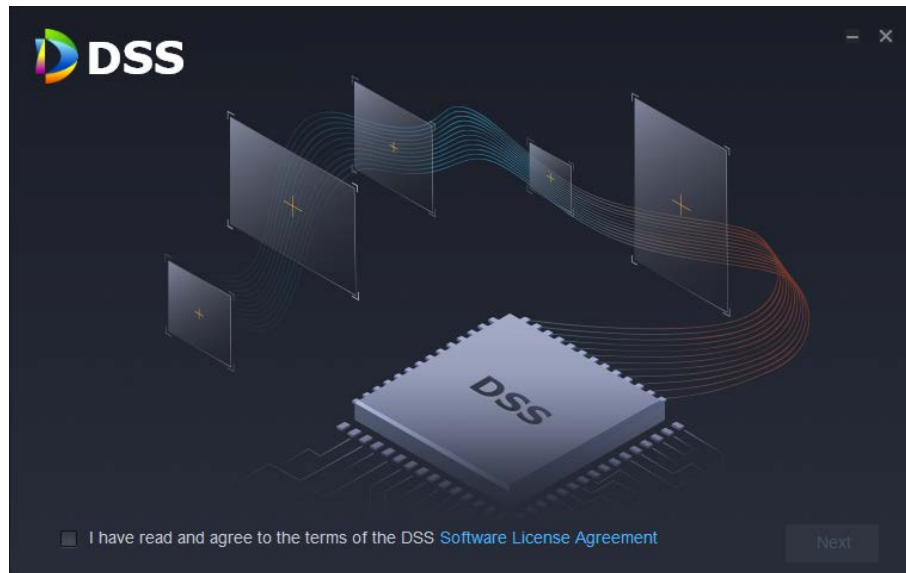
Procedure

Step 1 Double-click the DSS installer 🦫.

📖

The name of the installer includes version number and date, confirm before installation.

Figure 2-1 Install DSS server

Step 2 Click **Software License Agreement**, and then read the agreement,

Step 3 Select the check box to accept the agreement, and then click **Next**.

Figure 2-2 Select the installation path

Step 4 Click **Browse**, and then select the installation path.

If the **Install** button is gray, check whether your installation path and space required meet the requirements. The total space required is displayed on the page.

📖

We do not recommend you install the DSS server on Disk C, because features such as face recognition require higher disk performance.

Step 5 Click **Install**.

⚠️

The installation process takes about 4 to 8 minutes. Do not cut off the power or close the program.

Figure 2-3 Run the DSS server

Step 6   Click **Run** when the installation finishes.

Figure 2-4 Select the network mode and network card
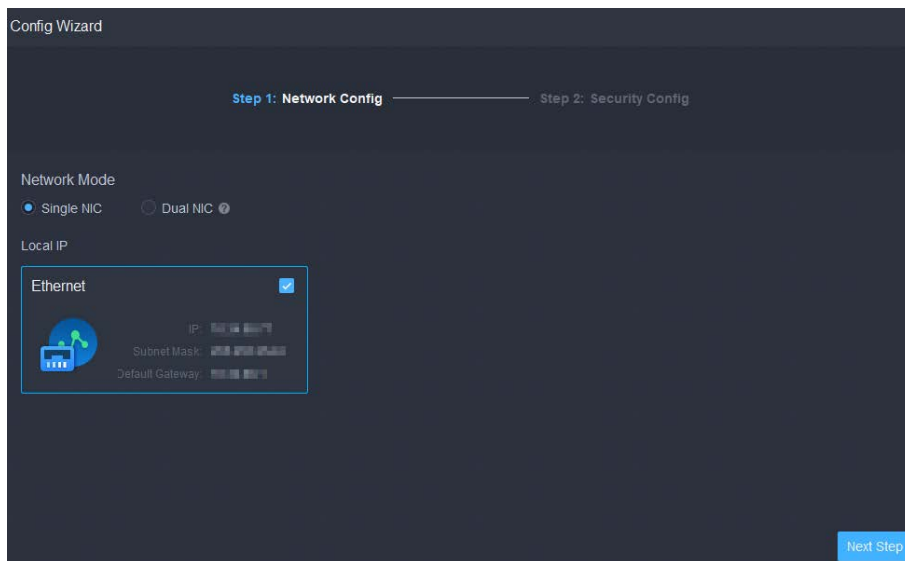
Step 7   Select a network mode and the network card, and then click **Next Step**.

Step 8   Enable or disable TLS1.0 as needed.

📖

TLS 1.0 has known security vulnerabilities. We strongly recommend you disable it to avoid security risks. If it is disabled, the web page of DSS platform cannot be accessed through the browser. You need to enable TLS 1.1 and TLS 1.2 in the browser settings to gain access to the web page.

Step 9   Click **Finish**.

🕮

If the available RAM of the server is less than 2 GB, you can only use basic functions related to video. If it is less than 1.5 GB, you cannot use any function.

Related Operations

- To uninstall the platform, log in to the server, go to "..\DSS\DSS Server\Uninstall", double-click uninst.exe, and then follow the on-screen instructions to uninstall the program.
- To update the system, directly install the new program. The system supports in-place update. Follow the steps above to install the program.

2.3 Configuring Server IP Address

Change the server IP address as you planned. Make sure that the server IP can access the devices in your system. For details, see the manual of the server.

🕮

After changing the IP address of the server, you need to update it in the system services. See the following section.

2.4 Managing System Services

View service status, start or stop services, and change service ports.

On the server, double-click .
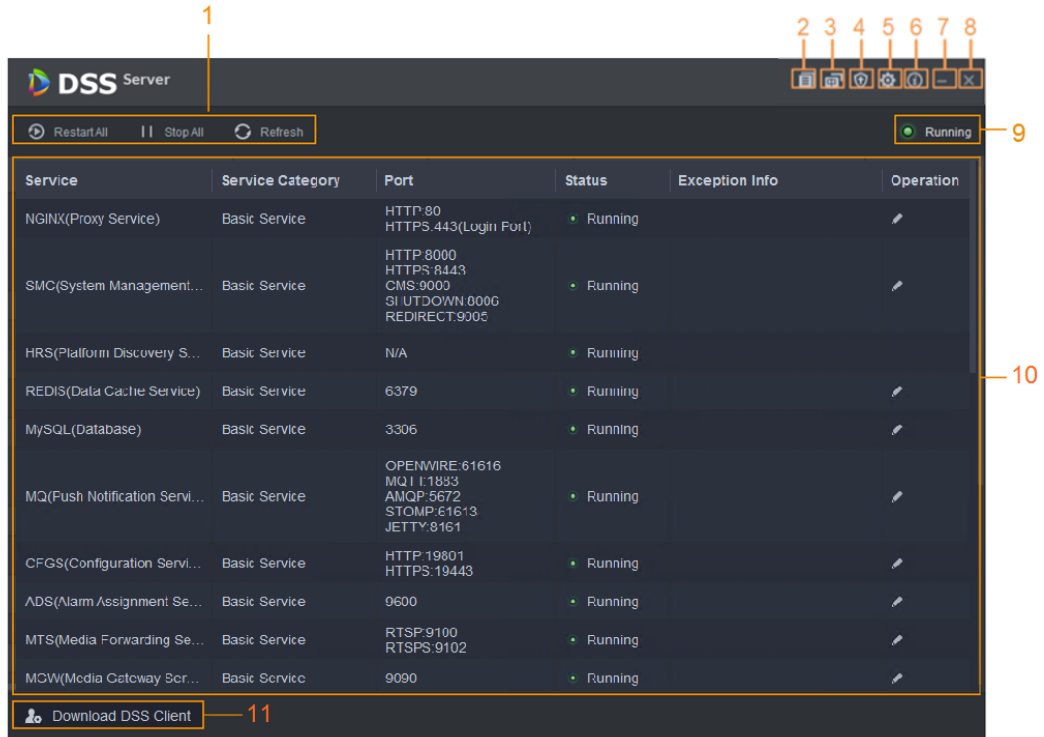
Figure 2-5 Service management page

Table 2-2 Interface description

No.	Function	Description
1	Service Management	• Click ⊕ Restart All to restart all services. 📖 When starting the platform, if the available memory of the server does not reach 2 GB, only the basic video services can be enabled. If the server has less than 1.5 GB of available memory, no services are available. • Click ‖ Stop All to stop all services. • Click ⟳ Refresh to refresh services.
2	User's manual	User manual.
3	Language	Switch language.
4	Security Setting	TLS 1.0 has known security vulnerabilities. We strongly recommend you disable it to avoid security risks. If it is disabled, the web page of DSS platform cannot be accessed through the browser. You need to enable TLS 1.1 and TLS 1.2 in the browser settings to gain access to the web page. 1. Open Internet Explorer. 2. Click the **Tools** button at the upper-right corner, and then select **Internet Options**. 3. Select the **Advanced** tab. 4. Go to the **Settings** > **Security**, and then select **Use TLS 1.1** and **Use TLS 1.2**. 5. Click **OK**.

No.	Function	Description
5	Setting	Configure the IP address of the server and IP mapping. ● Set up an IP address for the server so that the platform can access the network and the devices in it. If the server has two network cards, you can select **Dual NIC** mode, configure two IP addresses, and then the platform will be able to connect to two networks and access the devices on each one. ● If the platform is in a local network and the devices are on the internet, or you need to access the platform that is in a local network from the Internet, you need to map the IP address of the platform to a WAN IP address or a domain name. For details, see "3.2 Mapping IP or Domain Name".
6	About	Software version information.
7	Minimize	Minimize the page.
8	Close	—
9	Service Status	● ⬤ Starting : Services are starting. ● ⬤ Unavailable : Service is running abnormally ● ⬤ Stopping : Services are stopping. ● ⬤ Running : Service is running normally ● ⬤ Stopped : Services have stopped.
10	Services	Displays each service and service status. Click 🖊 to modify service port number, and then the services will restart automatically after modification.
11	Download DSS Client	Go to client download page of the DSS client.

2.5 Installing and Logging into DSS Client

Install the DSS client before licensing it.

2.5.1 Installing DSS Client

You can visit the system through the DSS Client for remote monitoring.

2.5.1.1 DSS Client Requirements

To install DSS Client, prepare a computer in accordance with the following requirements.

Table 2-3 Hardware requirements

Parameters	Description
Recommended system requirements	• CPU: I5-6500@3.20GHz • Memory: 8 GB and above • Graphics: NVIDIA® GeForce®GT 530 • Network Card: 1000 Mbps • HDD: Make sure that at least 100GB is reserved for the client.
Minimum system requirements	• CPU: I3-2120@3.20GHz • Memory: 4 GB • Graphics: Intel® HD Sandbridge Desktop Graphcs • Network Card: 1000 Mbps • DSS client installation space: Make sure that at least 50 GB is reserved for DSS client.

2.5.1.2 Downloading and Installing DSS Client

Step 1   Go to https://*IP address of the platform* in the browser

Step 2   Click **PC**, and then **Download**.

If you save the program, go to Step3.

If you run the program, go to Step4.

Figure 2-6 Download DSS Client
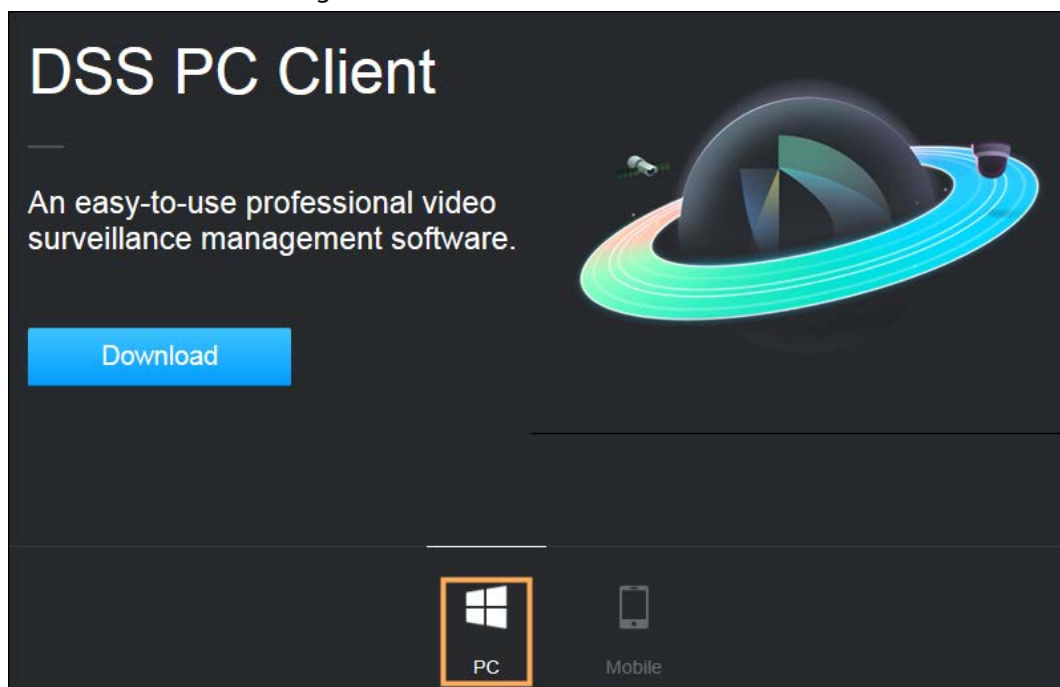
Step 3   Double-click the DSS Client program.

Step 4   Select the check box of **I have read and agree to the DSS agreement** and then click **Next**.

Step 5   Select installation path.

Step 6   Click **Install**.

System displays the installation progress. It takes about 5 minutes to complete.

2.5.2 Logging in to DSS Client

Step 1   Double-click [icon] on the desktop.

Step 2   Select a language.

Step 3   Enter the IP address and port number of the platform.

On the drop-down list, platforms that are in the same network as your computer will be shown.

If you want to log in to the platform using its domain name, you must link its IP address to a domain name first. For details, see the user's manual.

Figure 2-7 Automatically discovered platform
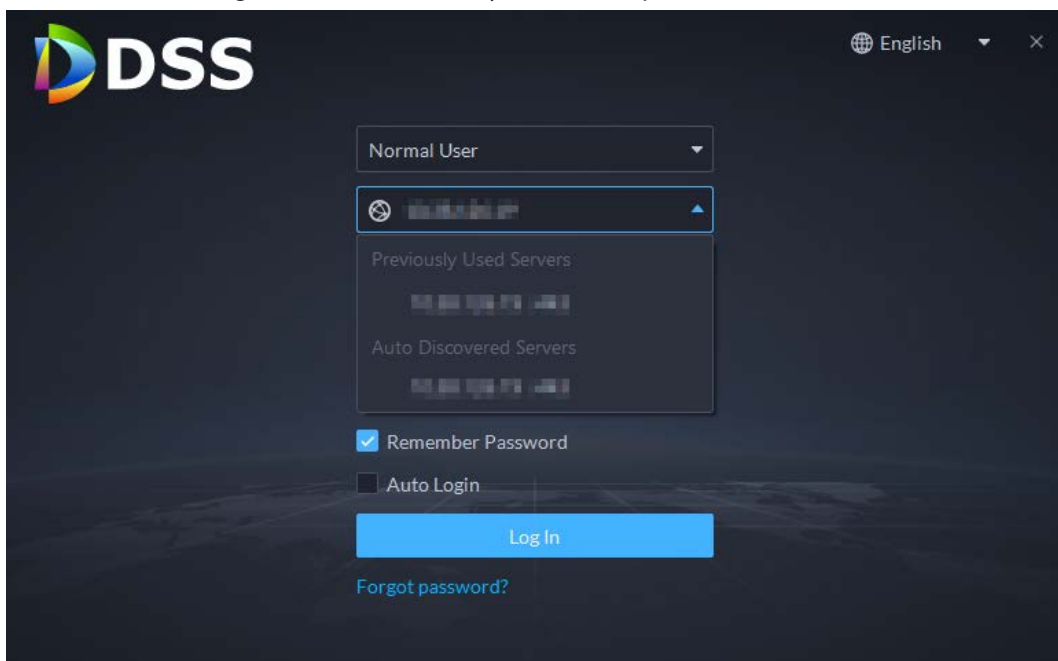
Step 4   Click anywhere else on the page to start initializing the platform.

For first-time login, you will be automatically directed to the initialization process.

If you are not logging in for the first time, enter the IP address, port number of the platform, username, and password, and then click **Login**.

1) The default user is system. Enter and confirm the password, and then click **Next**.

The password must consist of 8 to 32 non-blank characters and contain at least two types of characters: Uppercase, lowercase, number, and special character (excluding ' " ; : &).

2) Select your security questions and enter their answers, and then click **OK**.

The client will automatically log in to the platform by using the password you just set.

2.5.3 Homepage of DSS Client

Figure 2-8 Homepage

Table 2-4 Parameter description

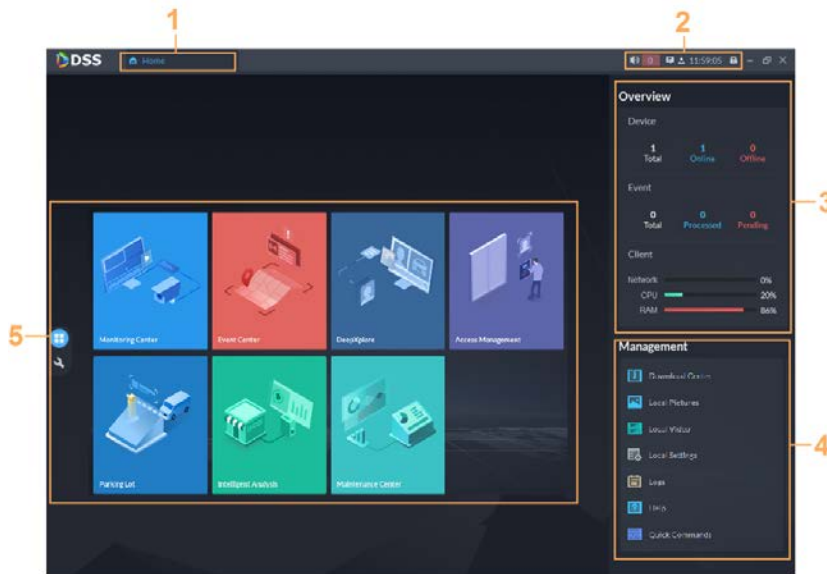| No.	Name	Function
1	Tab	Displays the names of all tabs that are opened.
2	System settings	: Enable or disable alarm audio. 0 : Displays number of alarms. Click the icon to go to **Event Center**. - Click to view system messages, such as the information of a device was edited or deleted. The permissions of a user will determine what messages can be seen. For example, if user A does not have the permission of device A, then user A will not get the message when device A is deleted. : User information: Click the icon, and then you can log in to the web page by clicking system IP address, change password, lock client and log out. ◇ Click platform IP address to go to the Web page. ◇ Click **Change Password** to change user password. ◇ Click **About** to view version information. ◇ Click **Sign Out** to exit client. - Click to lock client.
3	Overview	- The number of devices in total, offline and online. - The number of total, processed and pending events. - The client network, CPU and RAM usage.

No.	Name	Function
4	Management	• Download videos. • Check local pictures and videos. • Settings for video, snapshot, video wall, alarm, security and shortcut keys. • View and manage logs. • View user manual. • Customize quick HTTP commands. For details, see the user's manual.
5	Applications	• ▦: Application options including monitoring center, access management, intelligent analysis and vehicle entrance control. • 🔧: Configuration options.

2.6 Licensing

You can upgrade your license for more features and increased capacity.

This section introduces license capacity, how to apply for a license, how to use the license to activate the platform, and how to renew your license.

2.6.1 Applying for a License

A license is used to confirm the features and number of channels you purchased. To get a formal license, contact our sales personnel. To apply for a trial license, visit our website and find DSS Express, scroll to the bottom, click **Apply**, and then follow the instructions.

2.6.2 Activating License

📖

The following images of the page might slightly differ from the actual pages.

2.6.2.1 Online Activation

Prerequisites

• You have received your license. If not, see "2.6.1 Applying for a License".
A license is used to confirm the features and number of channels you purchased. To get a formal license, contact our sales personnel. To apply for a trial license, visit our website and find DSS Express, and then follow the application instructions.
• The platform server can access the Internet.

Procedure

Step 1   On the **Home** page, click 🔧, and then in **System Config**, select **License**.
Step 2   Click **Online Activate License**.

Step 3   Enter your new **Activation Code**.

Step 4   Click **Activate Now**.

Step 5   On the **License** page, view your license details.

2.6.2.2 Offline Activation

Prerequisites

You have received your license. If not, see "2.6.1 Applying for a License".

A license is used to confirm the features and number of channels you purchased. To get a formal license, contact our sales personnel. To apply for a trial license, visit our website and find DSS Express, and then follow the application instructions.

Procedure

Step 1   On the **Home** page, click , and then in **System Config**, select **License**.

Step 2   Click **Offline Activate License**.

Step 3   Enter your new **Activation Code**.

Step 4   Click **Export** to export the license request file.

Step 5   Generate license file.

1) Move the request file to a computer with Internet access.

2) On that computer, open the system email that contains your license, and then click the attached web page address or **Click to go to DSS License Management** to go to the license management page.

3) Click **Activate License**.

4) Click **Upload**, select the license request file, and then when you are prompted **uploaded successfully**, click **Activate**.

The success page is displayed, where a download prompt is displayed asking you to save the license activation file.

Figure 2-9 Upload license request file
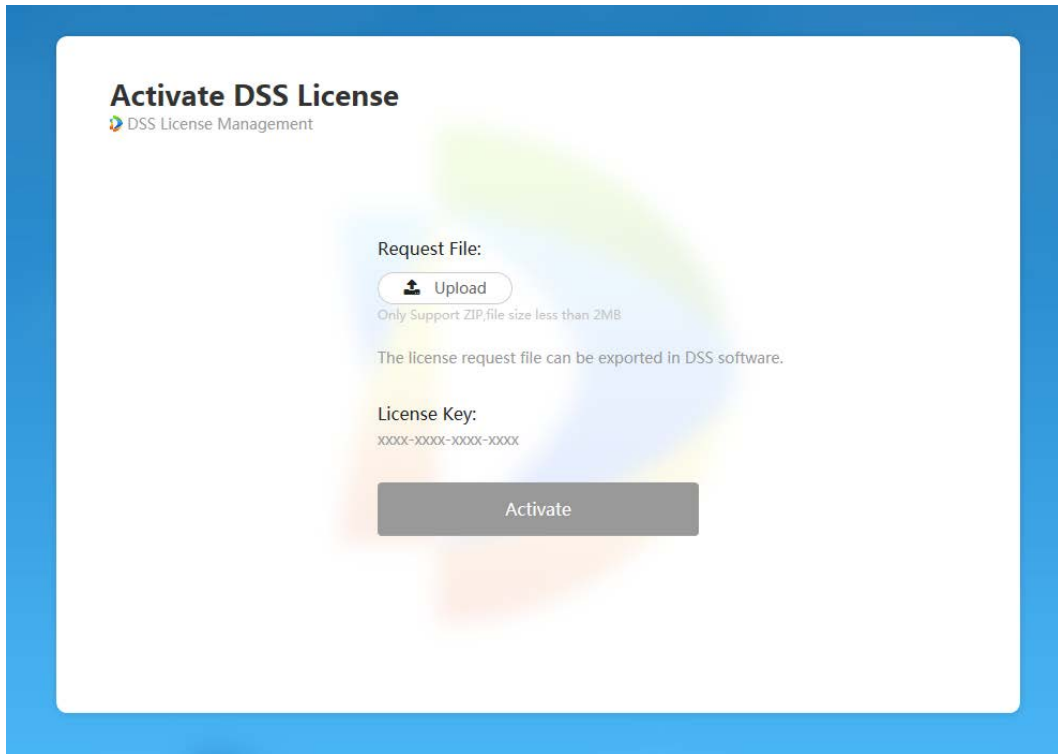
5) On the success page, click **Save** to save the file, and then move the file back to the computer where you exported the license request file.

6) On the **Offline Activate License** page, click **Import**, and then follow the on-screen instructions to import the license activation file.

Step 6   On the **License** page, view your license details.

3 Configuring LAN or WAN

3.1 Configuring Router

For the list of the ports that need to be mapped, see "Appendix 1 Service Module Introduction".

Make sure that the WAN ports is consistent with LAN ports.

3.2 Mapping IP or Domain Name

If the platform is deployed in a local network, you can map the IP address of the server to a fixed WAN IP or a domain name, and then log in to the server using the WAN IP or domain name.
The page might vary between the main server and the sub server. This section uses the main server page as an example.

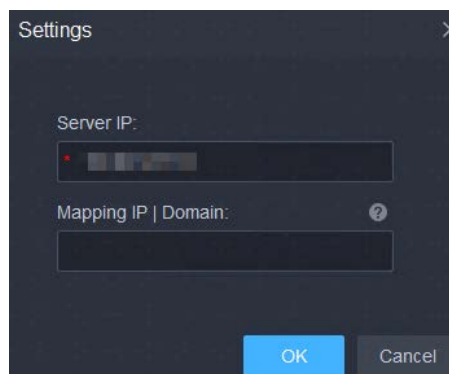Step 1   Log in to DSS server, and then double-click

Step 2   Click the on the upper-right corner.

Figure 3-1 Setting

Step 3   Enter a fixed WAN IP address or a domain name in the **Mapping IP | Domain** box, and then click **OK**.

If you want to use a domain name, you need to make corresponding configurations on the domain name server.

Step 4   Click **OK**, and then the services will restart.

Appendix 1 Service Module Introduction

Appendix Table 1-1 Service module introduction

Service Name		Function Description
Access Service	NGINX	Reverses user requests to distributed system management services.
System Management Service	SMC	Manages services and provides access to various pages.
Device Discovery Service	HRS	Broadcasts platform information to discover devices.
Data Cache Service	REDIS	Stored temporary business data from the platform.
Database	MySQL	Stores platform business data.
Message Queue Service	MQ	Transfers messages between platforms.
Configuration Service	CFGS	Manages disks, such as read-and-write operations.
Alarm Dispatch Service	ADS	Sends alarm information to different objects according to defined plans.
Media Transmission Service	MTS	Gets audio/video bit streams from front-end devices and then transfers the data to DSS, the client and decoders.
Media Gateway	MGW	Sends MTS address to decoders.
Storage Service	SS	Stores, searches for and plays back recordings.
Object Storage Service	OSS	Manages storage of face snapshots and intelligent alarm pictures.
Picture Transfer Service	PTS	Manages picture transmission.
Device Search Service	SOSO	Searches for device information.
Device Management Service	DMS	Registers encoders, receives alarms, transfers alarms, and sends out the sync time command.
Auto Register Service	ARS	Listens, logs in, or gets bit streams to send to MTS.
ProxyList control Proxy Service	PCPS	Logs in to ONVIF device, and then gets the stream and transfers the data to MTS.
Access Control Service	ACDG	Manages access control and other related operations.
Access Controller Access Service	MCDDOOR	Manages access controller access and related operations.

Service Name		Function Description
External LED Device Access Service	MCDLED	Manages LED access and other related operations.
External Alarm Controller Access Service	MCDALARM	Manages alarm controller access and other related operations.
Power Environment Server	PES	Manages access of dynamic environment monitoring devices.
Video Matrix Service	VMS	Logs in to the decoder and sends tasks to the decoder to output on the TV wall.
Video Intercom Switch Center	SC	Manages PC client and App client login as SIP client, and also forwards audio-talk streams.
DA Management Service	DAMS	Manages DA_BSID and DA_POC.
Link Management Service	DA_BSID	1. Accesses devices that uses the 4G network. 2. Downloads files from devices to the platform. 3. Redirects to the webpage of devices added through automatic registration.

Appendix 2 Cybersecurity Recommendations

Security Statement

- If you connect the product to the Internet, you need to bear the risks, including but not limited to the possibility of network attacks, hacker attacks, virus infections, etc., please strengthen the protection of the network, platform data and personal information, and take the necessary measures to ensure the cyber security of platform, including but not limited to use complex passwords, regularly change passwords, and timely update platform products to the latest version, etc. Dahua does not assume any responsibility for the product abnormality, information leakage and other problems caused by this, but will provide product-related security maintenance.
- Where applicable laws are not expressly prohibited, for any profit, income, sales loss, data loss caused by the use or inability to use this product or service, or the cost, property damage, personal injury, service interruption, business information loss of purchasing alternative goods or services, or any special, direct, indirect, incidental, economic, covering, punitive, special or ancillary damage, regardless of the theory of liability (contract, tort, negligence, or other) , Dahua and its employees, licensors or affiliates are not liable for compensation, even if they have been notified of the possibility of such damage. Some jurisdictions do not allow limitation of liability for personal injury, incidental or consequential damages, etc., so this limitation may not apply to you.
- Dahua's total liability for all your damages (except for the case of personal injury or death due to the company's negligence, subject to applicable laws and regulations) shall not exceed the price you paid for the products.

Security Recommendations

The necessary measures to ensure the basic cyber security of the platform:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters.
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
   - Do not contain the account name or the account name in reverse order.
   - Do not use continuous characters, such as 123, abc, etc.
   - Do not use overlapped characters, such as 111, aaa, etc.

2. **Customize the Answer to the Security Question**

   The security question setting should ensure the difference of answers, choose different questions and customize different answers (all questions are prohibited from being set to the same answer) to reduce the risk of security question being guessed or cracked.

Recommendation measures to enhance platform cyber security:

1. **Enable Account Binding IP/MAC**

It is recommended to enable the account binding IP/MAC mechanism, and configure the IP/MAC of the terminal where the commonly used client is located as an allowlist to further improve access security.

2. **Change Passwords Regularly**

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Turn On Account Lock Mechanism**

The account lock function is enabled by default at the factory, and it is recommended to keep it on to protect the security of your account. After the attacker has failed multiple password attempts, the corresponding account and source IP will be locked.

4. **Reasonable Allocation of Accounts and Permissions**

According to business and management needs, reasonably add new users, and reasonably allocate a minimum set of permissions for them.

5. **Close Non-essential Services and Restrict the Open Form of Essential Services**

If not needed, it is recommended to turn off NetBIOS (port 137, 138, 139), SMB (port 445), remote desktop (port 3389) and other services under Windows, and Telnet (port 23) and SSH (port 22) under Linux. At the same time, close the database port to the outside or only open to a specific IP address, such as MySQL (port 3306), to reduce the risks faced by the platform.

6. **Patch the Operating System/Third Party Components**

It is recommended to regularly detect security vulnerabilities in the operating system and third-party components, and apply official patches in time.

7. **Security Audit**
   - Check online users: It is recommended to check online users irregularly to identify whether there are illegal users logging in.
   - View the platform log: By viewing the log, you can get the IP information of the attempt to log in to the platform and the key operation information of the logged-in user.

8. **The Establishment of a secure Network Environment**

In order to better protect the security of the platform and reduce cyber security risks, it is recommended that:
   - Follow the principle of minimization, restrict the ports that the platform maps externally by firewalls or routers, and only map ports that are necessary for services.
   - Based on actual network requirements, separate networks: if there is no communication requirement between the two subnets, it is recommended to use VLAN, gatekeeper, etc. to divide the network to achieve the effect of network isolation.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING