

DSS Express

Quick Deployment Manual



Foreword

General

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

Safety Instructions

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, lower performance, or unpredictable result.
 TIPS	Provides methods to help you solve a problem or save you time.
 NOTE	Provides additional information as the emphasis and supplement to the text.

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate number, email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please see our 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 the company names in the manual are the properties

of their respective owners.

- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please see our final explanation.

Table of Contents

Foreword	I
1 Installation and Deployment	1
1.1 Standalone Deployment	1
1.1.1 Server Requirements	1
1.1.2 Installing DSS	2
1.1.3 Configuring Server IP Address	3
1.1.4 Managing System Services	3
1.1.5 Installing and Logging into DSS Client	5
1.1.5.1 Installing DSS Client	5
1.1.5.1.1 DSS Client Installation Requirements	5
1.1.5.1.2 Downloading and Installing DSS Client	5
1.1.5.2 Logging in to DSS Client	6
1.1.5.3 Homepage of DSS Client	8
1.1.6 Licensing	9
1.1.6.1 Applying for a License	9
1.1.6.2 Activating License	10
1.1.6.2.1 Online Activation	10
1.1.6.2.2 Offline Activation	10
Appendix 1 Service Module Introduction	12
Appendix 2 Cybersecurity Recommendations	14

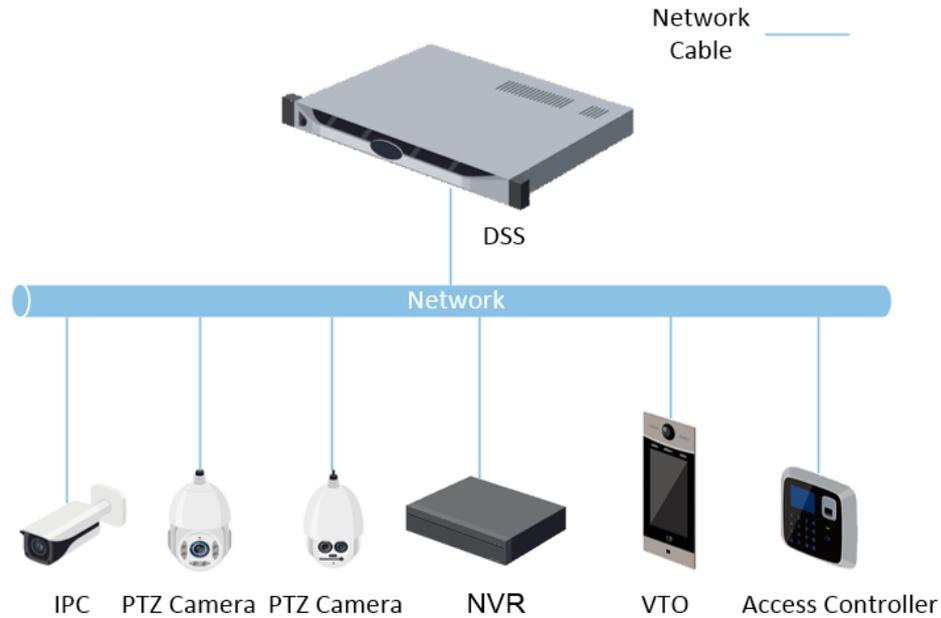
1 Installation and Deployment

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



1.1 Standalone Deployment

1.1.1 Server Requirements

Table 1-1 DSS Express hardware requirement

Parameter	Hardware Requirement	Operating System
Recommended configuration	<ul style="list-style-type: none"> • 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

Parameter	Hardware Requirement	Operating System
Minimum configuration	<ul style="list-style-type: none"> • 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 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 the face images have a storage location.
- For best performance, we recommend adding additional hard drives to store pictures.

1.1.2 Installing DSS

Prerequisites

- You have received the DSS installer from our sales or technical support.
- You have prepared a server that meets the hardware requirements mentioned in "1.1.1 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, please confirm before installation.

Step 2 Click **agreement**, read through the agreement, and then accept it.

Step 3 Select the agreement checkbox, and then click **Next**.

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

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



We recommend you do not install the platform into 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.

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

Step 7 Select the network card you need and click **OK**.

Step 8 Enable or disable TLS1.0 as needed.



TLS1.0 is risky. We recommend you disable it.

Step 9 Click **OK**.



If 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.

1.1.3 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.

1.1.4 Managing System Services

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

Log in to the server, and then double-click .

Figure 1-2 Service management interface

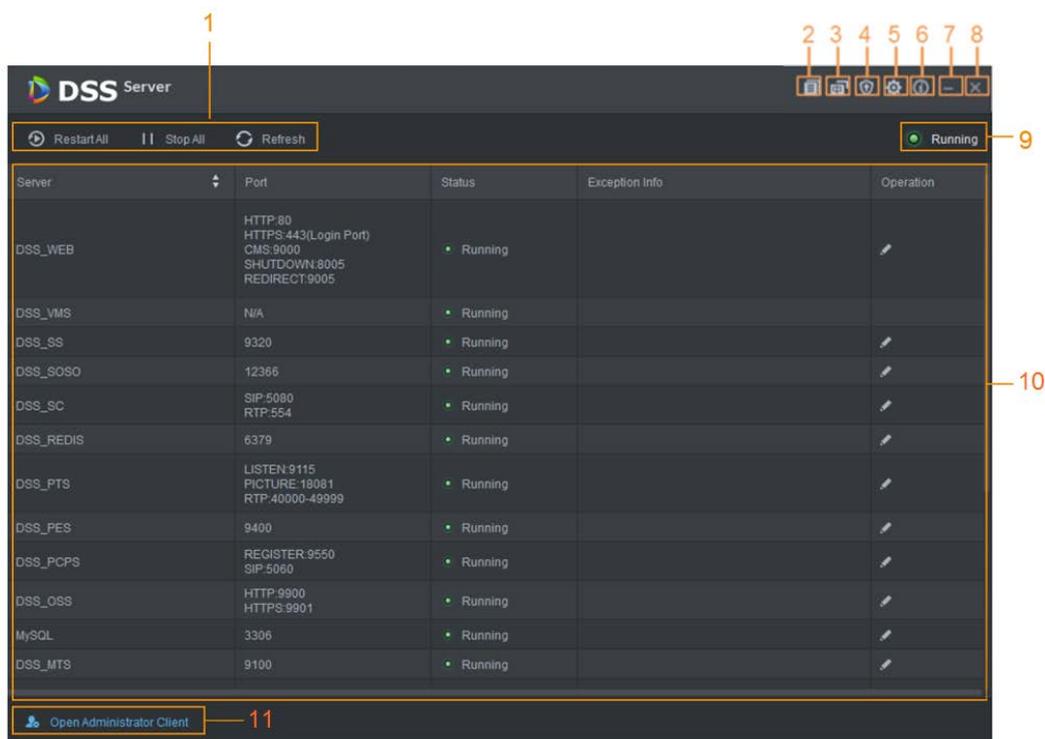


Table 1-2 Parameters

No.	Function	Description
1	Service Management	<p>Supports 3 types of operations:</p> <ul style="list-style-type: none"> Click  Restart All to restart all services. <p> 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.</p> <ul style="list-style-type: none"> Click  Stop All to stop all services. Click  Refresh to refresh services.
2	User's manual	User's manual.
3	Language	Switch language.
4	Security Setting	Enable or disable the TSL 1.0 protocol. TSL 1.0 protocol is a non-security protocol and is recommended to be disabled. If TLS 1.0 protocol is disabled, ensure that the browser has proper access to the platform. To enable TLS1.1 and TLS 1.2, open your browser, select  > Internet Options > Advanced .
5	Setting	Set the server IP as the platform CMS IP. If the network has to go across LAN and WAN, you need to enter WAN IP in the Mapping IP box.
6	About	Software version information.
7	Minimize	Minimize the interface.
8	Close	—

No.	Function	Description
9	Service Status	<ul style="list-style-type: none"> ●  Starting ●  Unavailable: Service is running abnormally ●  Stopping ●  Running: Service is running normally ●  Stopped
10	Services	Display each service and service status. Click  to modify service port number, and then the services will restart automatically after modification.
11	Download Client	Go to client download interface.

1.1.5 Installing and Logging into DSS Client

Install the DSS client before licensing it.

1.1.5.1 Installing DSS Client

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

1.1.5.1.1 DSS Client Installation Requirements

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

Table 1-3 Hardware requirements

Parameters	Description
Recommended system requirements	<ul style="list-style-type: none"> ● 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 DSS client.
Minimum system requirements	<ul style="list-style-type: none"> ● CPU: I3-2120@3.20GHz ● Memory: 4 GB ● Graphics: Intel® HD Sandbridge Desktop Gra ● Network Card: 1000 Mbps ● DSS client installation space: Make sure that at least 50 GB is reserved for DSS client.

1.1.5.1.2 Downloading and Installing DSS Client

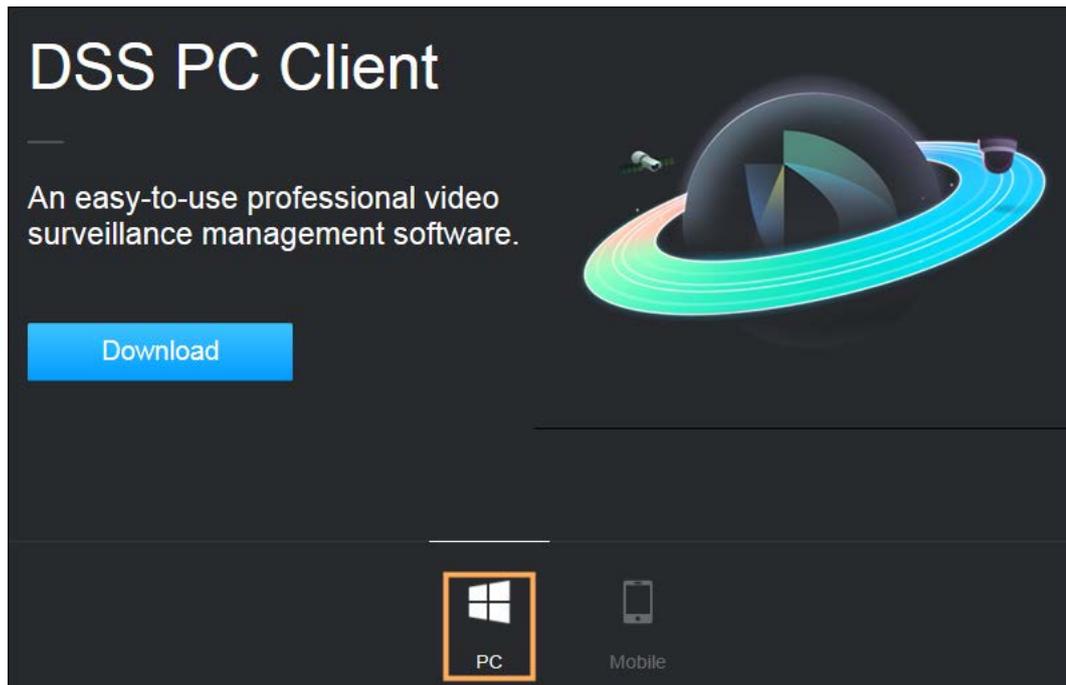
Step 1 Enter the IP address of DSS into the browser and then press Enter.

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

If you save the program, go to **Step 3**.

If you run the program, go to **Step 4**.

Figure 1-3 Download DSS Client

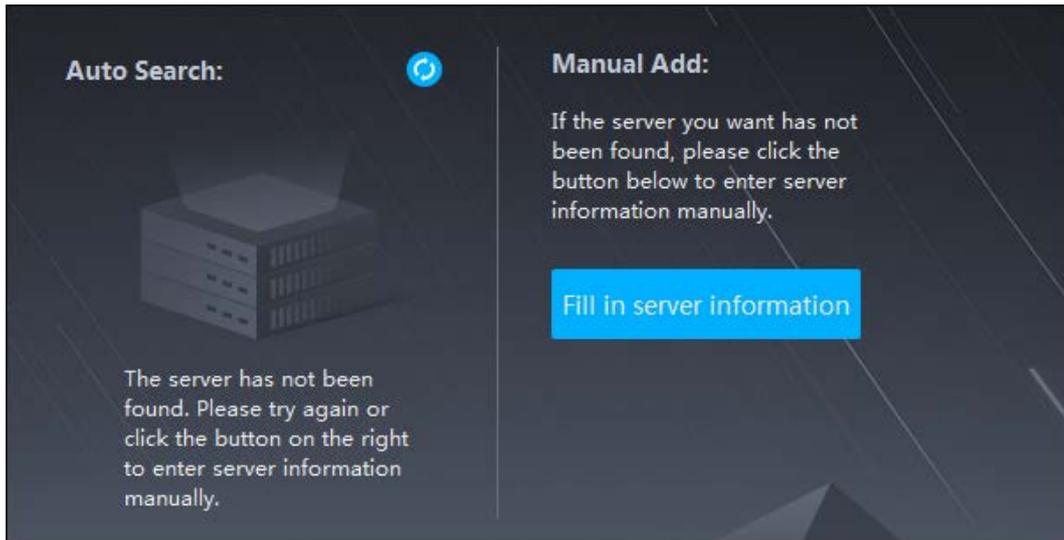


- Step 3** Double-click the DSS Client program.
- Step 4** Select the check box of **I have read and agree to the DSS agreement** and then click **Next**.
- Step 5** Select installation path.
- Step 6** Click **Install**.
System displays the installation process. It takes about 5 minutes to complete. Please be patient.

1.1.5.2 Logging in to DSS Client

- Step 1** Double-click  on the desktop.
- The first time you log in to the platform, go to **Step 2**.
 - If this is not your first time logging in to the platform, go to **Step 3**.
- Step 2** Initialize the platform.
The first time you log in, you have to initialize the platform. Set the system username and password, and password protection questions. The questions are used when you need to change your password in the future.
- 1) Configure system username and 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 questions and their answers, and then click **OK**.
- Step 3** Select the detected server on the left of the interface, or click **Fill in site information**, and then enter the IP address and port number.
Server IP is the IP address of DSS server or PC. The port is 443 by default.

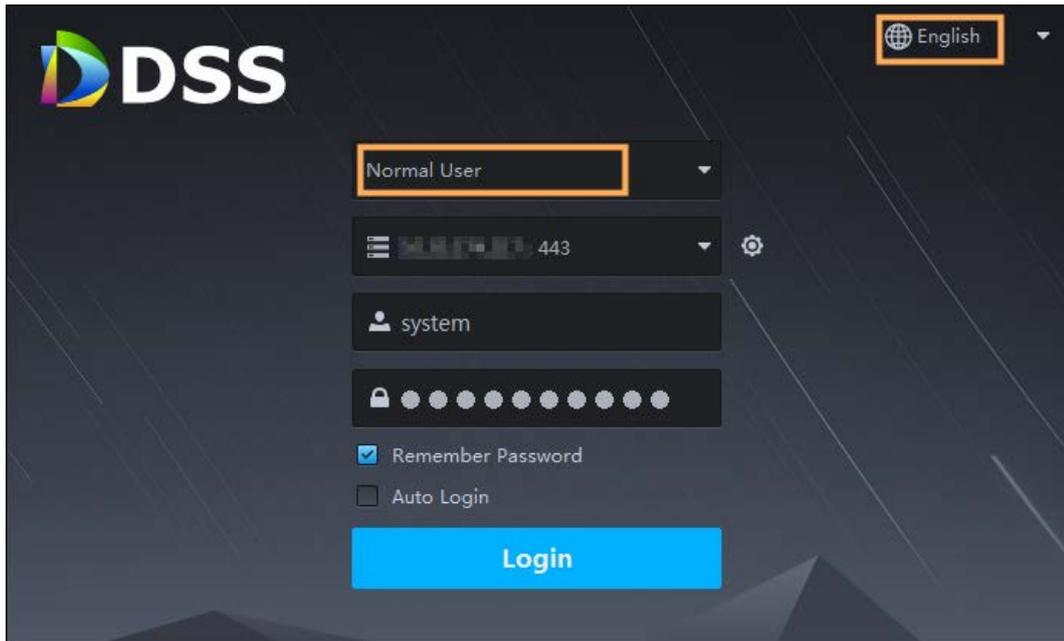
Figure 1-4 Select a site



Step 4 Select a user type, language and platform.

Step 5 Enter username and password, and then click **Login**.

Figure 1-5 Login interface (not first-time login)



1.1.5.3 Homepage of DSS Client

Figure 1-6 Homepage

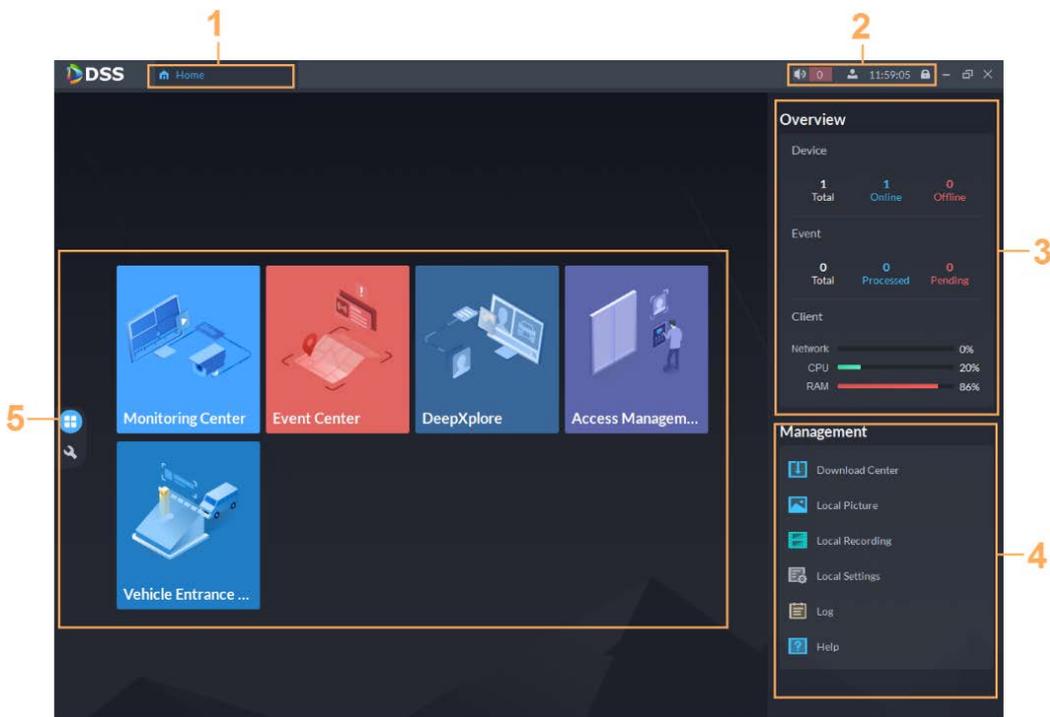


Table 1-4 Description

No.	Name	Function
1	Tab	Tabs.

No.	Name	Function
2	System settings	<ul style="list-style-type: none"> ● : Enable or disable alarm audio. ● : Displays number of alarms. Click the icon to go to Event Center. ● : User information: Click the icon, and then you can log in to the web interface by clicking system IP address, change password, lock client and log out. <ul style="list-style-type: none"> ◇ Click platform IP address to go to the Web interface. ◇ Click Change Password to modify user password. ◇ Click About to view version information. ◇ Click Sign Out to exit client. ● Click  to lock client.
3	Overview	<ul style="list-style-type: none"> ● The number of devices in total, offline and online. ● The number of total, processed and pending events. ● The network, CPU and RAM usage.
4	Management	<ul style="list-style-type: none"> ● Download videos. ● Check local pictures and videos. ● Settings of video, snapshot, alarm, security and shortcut key. ● View and manage logs. ● View help file.
5	Applications	<ul style="list-style-type: none"> ● : Application options including video monitoring, events, intelligent search, access management, and vehicle entrance control. ● : Configuration options.

1.1.6 Licensing

You can upgrade your license for more features and 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.

1.1.6.1 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, go to the official website of Dahua,

find DSS Express, click **Ask for Demo**, and then follow the application instructions.

1.1.6.2 Activating License



The following images of the interface might slightly differ from the actual interfaces.

1.1.6.2.1 Online Activation

Prerequisites

- You have received your license. If not, see "1.1.6.1 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, go to official website of Dahua, find DSS Express, and then follow the application instructions.
- The platform server can access the Internet.

Procedure

- Step 1 On the **Home** interface, click , and then in **System Configuration**, 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** interface, view your license details.

1.1.6.2.2 Offline Activation

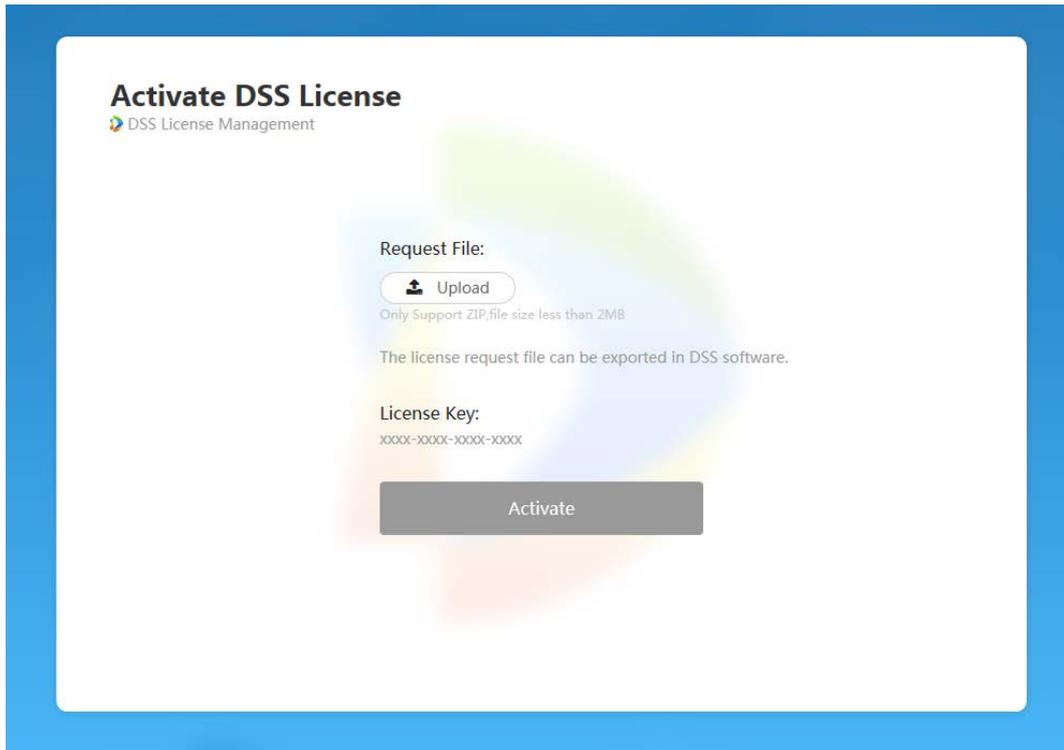
Prerequisites

You have received your license. If not, see "1.1.6.1 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, go to official website of Dahua, find DSS Express, and then follow the application instructions.

Procedure

- Step 1 On the **Home** interface, click , and then in **System Configuration**, 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 interface is displayed, where a download prompt is displayed asking you to save the license activation file.

Figure 1-7 Upload license request file



- 5) On the success interface, 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** interface, click **Import**, and then follow the on-screen instructions to import the license activation file.

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

Appendix 1 Service Module Introduction

Service Name		Function Description
Access Service	DSS_NGINX	Reverses user requests to distributed system management services.
System Management Service	DSS_SMC	Manages services and provides access to various interfaces.
Device Discovery Service	DSS_HRS	Broadcasts platform information to discover devices.
Data Cache Service	DSS_REDIS	Platform temporary business data storage.
Database	MySQL	Stores platform business data.
Message Queue Service	DSS_MQ	Transfers messages between platforms.
Device Management Service	DSS_DMS	Registers encoders, receives alarms, transfers alarms and sends out the sync time command.
Media Transmission Service	DSS_MTS	Gets audio/video bit streams from front-end devices and then transfers the data to DSS, the client and decoders.
Storage Service	DSS_SS	Store, search and play back recordings.
Device Search Service	DSS_SOSO	Search for device information.
Auto Register Service	DSS_ARS	Listens, logs in, or gets bit streams to send to MTS.
ProxyList control Proxy Service	DSS_PCPS	Logs in to ONVIF device, and then gets the stream and transfers the data to MTS.
Alarm Dispatch Service	DSS_ADS	Sends alarm information to different objects according to defined plans.
External Access Controller Access Service	DSS_MCDDoor	Manages access controller access and other related operations.
External LED Device Access Service	DSS_MCDLed	Manages LED access and other related operations.
External Alarm Controller Access Service	DSS_MCDAlarm	Manages alarm controller access and other related operations.
Power Environment Server	DSS_PES	Manages access of dynamic environment monitoring devices.
Video Intercom Switch Center	DSS_SC	Manages PC client and App client login as SIP client, and also forwards audio-talk streams.
Object Storage Service	DSS_OSS	Manages storage of face snapshots and intelligent alarm pictures.

Service Name		Function Description
Object Storage Service	DSS_SubOSS	Mainly manages storage evidence recordings and pictures.
Picture Transfer Service	DSS_PTS	Manages picture transmission.
Speed Measurement Service	DSS_EAS	Measures vehicle average speed and analyzes traffic data.

Appendix 2 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

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. Update Firmware and Client Software in Time

- According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. Physical Protection

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. Change Passwords Regularly

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

3. Set and Update Passwords Reset Information Timely

The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. **Construct a Safe Network Environment**

In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.