

DSS Professional

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

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

Foreword	I
1 Installation and Deployment.....	1
1.1 Standalone Deployment.....	4
1.1.1 Server Requirements	4
1.1.2 Installing DSS.....	4
1.1.3 Configuring Server IP Address	7
1.1.4 Managing System Services	7
1.1.5 Installing and Logging into DSS Client.....	9
1.1.5.1 Installing DSS Client	9
1.1.5.1.1 DSS Client Installation Requirements.....	9
1.1.5.1.2 Downloading and Installing DSS Client.....	10
1.1.5.2 Logging in to DSS Client.....	10
1.1.5.3 Homepage of DSS Client	12
1.1.6 Licensing	13
1.1.6.1 Applying for a License	13
1.1.6.2 Activating License	14
1.1.6.2.1 Online Activation	14
1.1.6.2.2 Offline Activation.....	15
1.2 Distributed Deployment.....	17
1.2.1 Installing Main Server.....	17
1.2.2 Installing Sub Server	17
1.3 Hot Standby.....	19
1.4 Cascade.....	19
1.5 N+M	20
1.6 Configuring LAN or WAN	20
1.6.1 Configuring Router.....	20
1.6.2 Mapping IP	21
1.7 Mapping Domain	21
Appendix 1 Service Module Introduction	23
Appendix 2 Cybersecurity Recommendations.....	25

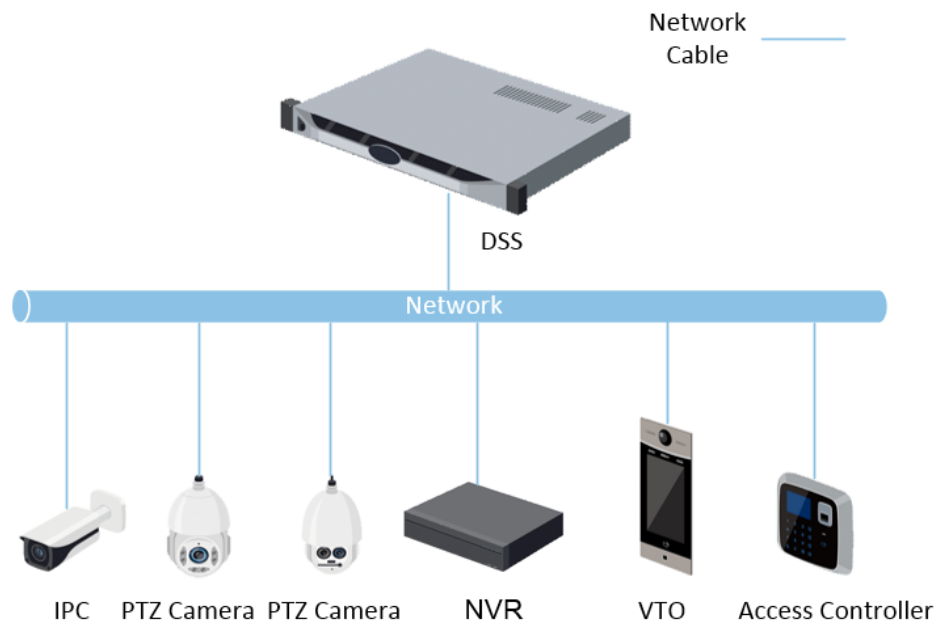
1 Installation and Deployment

DSS platform supports standalone deployment, distributed deployment, hot standby, cascading and N+M deployment, and LAN to WAN mapping.

Standalone Deployment

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

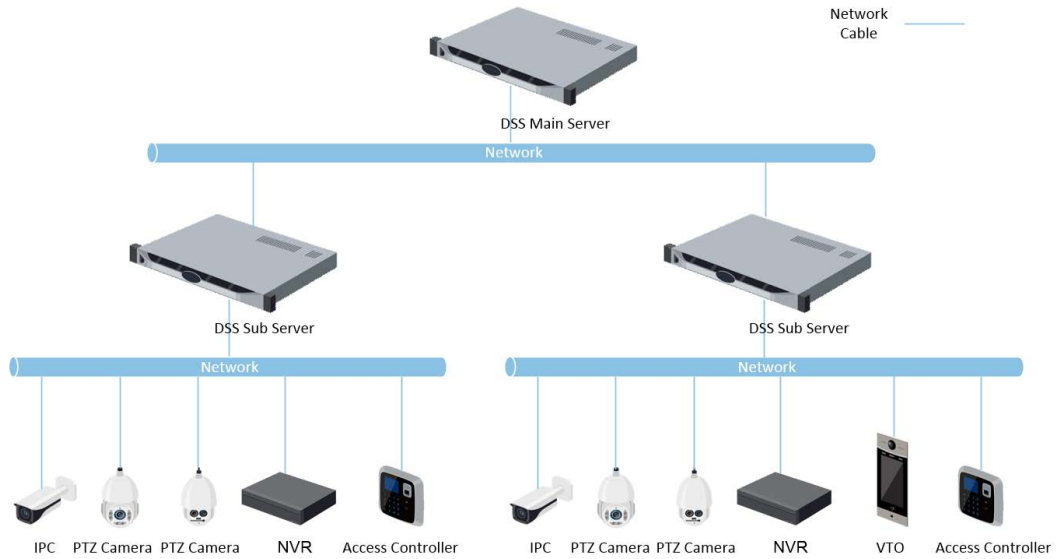
Figure 1-1 Standalone deployment



Distributed Deployment

Suitable for medium to larger projects. Sub servers are used to share system load, so that more devices can be accessed. The sub servers register to the main server, and the main server centrally manages the sub servers.

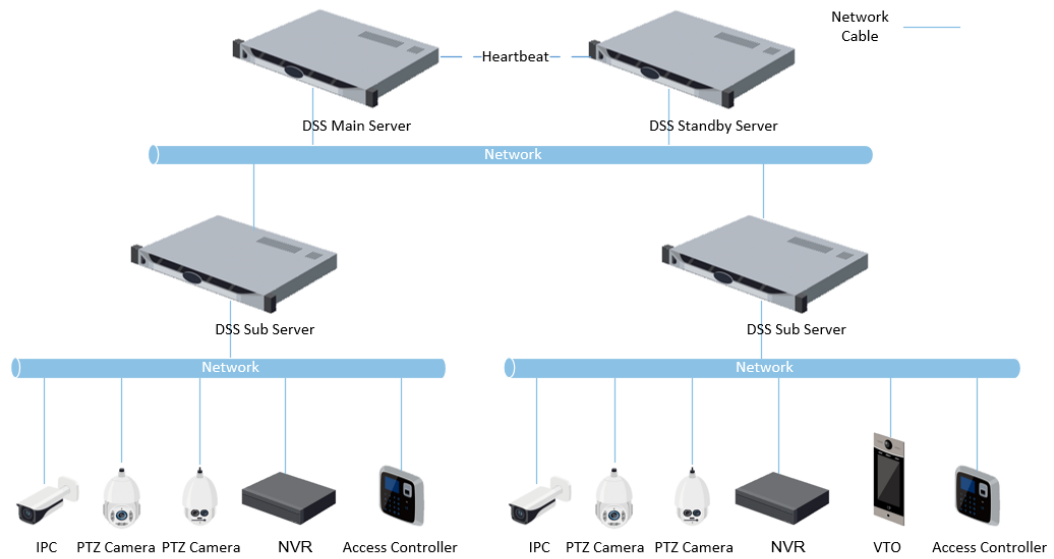
Figure 1-2 Distributed deployment



Hot Standby

Used with systems that require high stability. The standby server takes over the system when the active server malfunctions (such as with power-off and network disconnection). You can switch back to the original active server after it recovers.

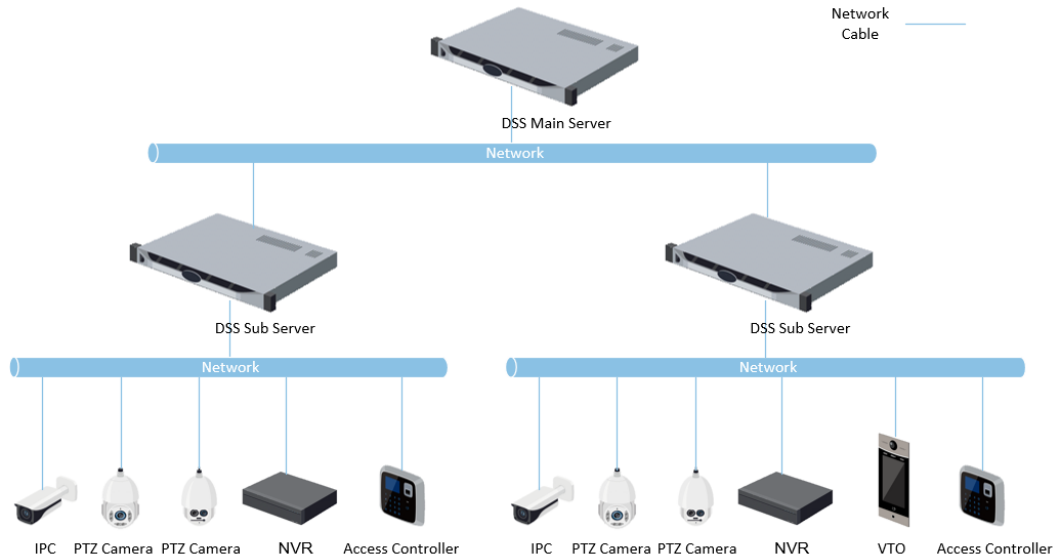
Figure 1-3 Hot standby



N+M

Each sub server has a standby server to maintain stability. When a sub server malfunctions, the system replaces it with an idle standby server. When the malfunctioning server normalizes, you can manually switch back to it. If you do not manually switch them, the system will automatically make the switch if the standby server malfunctions.

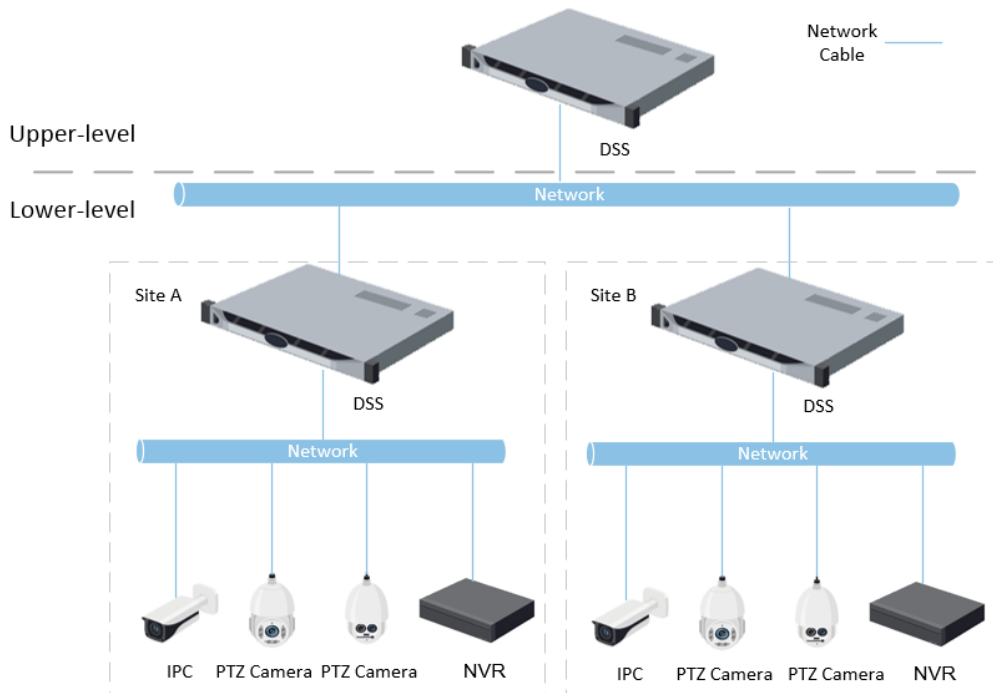
Figure 1-4 N+M



Cascade

In some cases, devices, storage servers and other system resources might not be deployed to a domain, industry system or an administrative area. Cascading is a good solution for that. The system supports up to three cascading levels. DSS Pro can be either the parent node or child node, while Express can only be a child node.

Figure 1-5 Cascade



LAN to WAN Mapping

Perform port mapping when:

- The platform and devices are in LAN, and the DSS Clients are in WAN. To make sure that DSS Clients can access the platform server, you need to map the platform IP to WAN.
- The platform is in LAN, and the devices are in WAN. For devices added to the platform through auto register, to make sure that the devices can access the platform, you need to map the

platform IP and ports to WAN. For devices added to the platform through IP, the platform can visit device WAN IP and ports.



DSS Server configuration system does not differentiate service LAN ports and WAN ports. Make sure that the WAN ports and LAN ports are the same.

1.1 Standalone Deployment

1.1.1 Server Requirements

Table 1-1 DSS Pro hardware requirements

Parameter	Hardware Requirement	Operating System
Recommended configuration	<ul style="list-style-type: none"> • CPU: Intel Xeon Silver 4214 2.2GHz • RAM: 16 GB • Network card: 4 × Ethernet port @ 1000 Mbps • Hard drive type: 7200 RPM Enterprise Class HDD 1 TB • DSS installation directory space: 500 GB 	<ul style="list-style-type: none"> • Win10-64 bit • Windows server 2008 • Windows server 2012 • Windows server 2016 • Windows server 2019
Minimum configuration	<ul style="list-style-type: none"> • CPU: Intel Xeon E-2224 3.4GHz/4core • RAM: 8 GB • Network card: 2 × Ethernet port @ 1000 Mbps • Hard drive type: 7200 RPM Enterprise Class HDD 1 TB • DSS installation directory space: 500 GB 	Win10-64 bit



- 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 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 "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, confirm before installation.

Figure 1-6 Install DSS server



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

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

Figure 1-7 Select a server type



Step 4 Select server type to **Main**, and then click **Next**.

Step 5 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 interface.

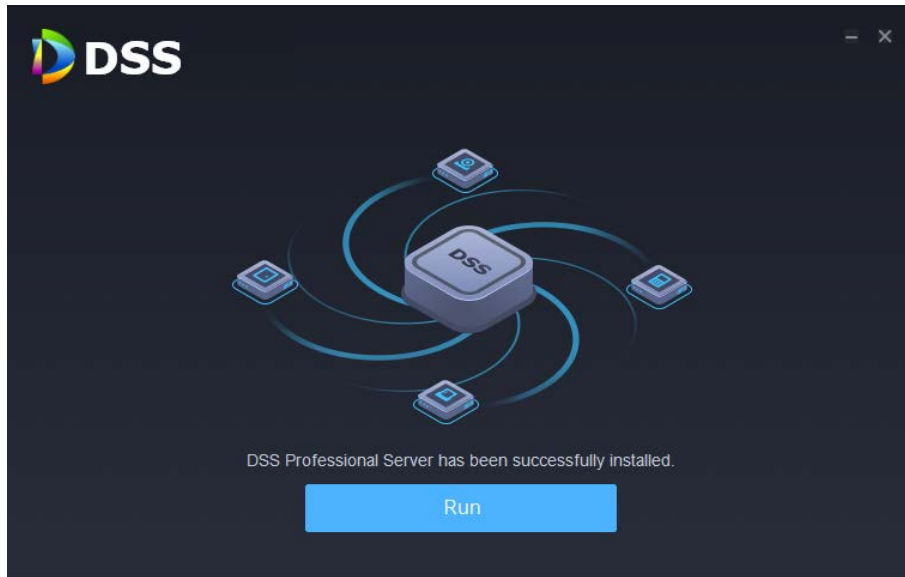


We do not recommend you install the DSS server on Disk C, because features such as face recognition require higher disk performance.

Step 6 Click **Install**.

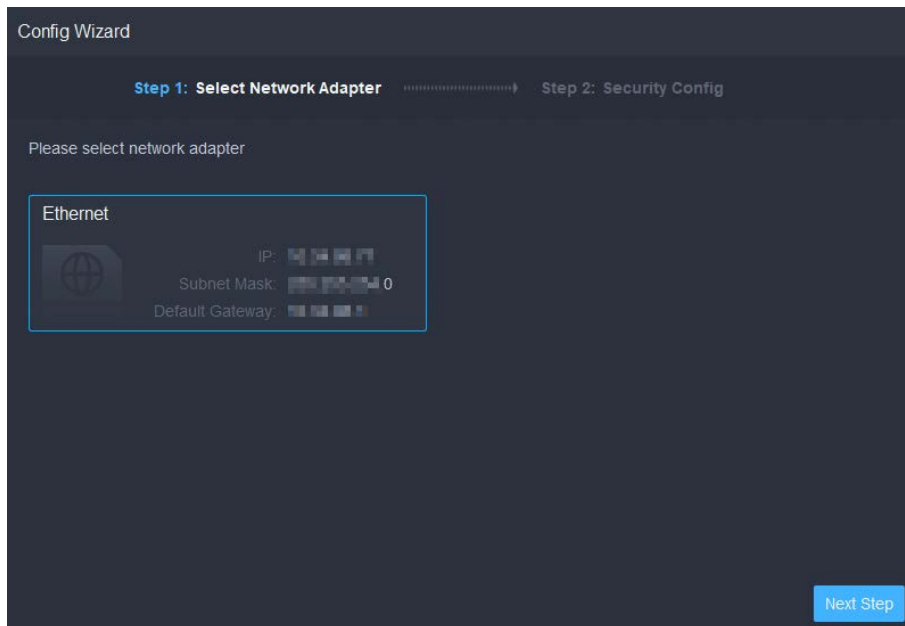
The installation process takes about 4 to 8 minutes.

Figure 1-8 Run the DSS server



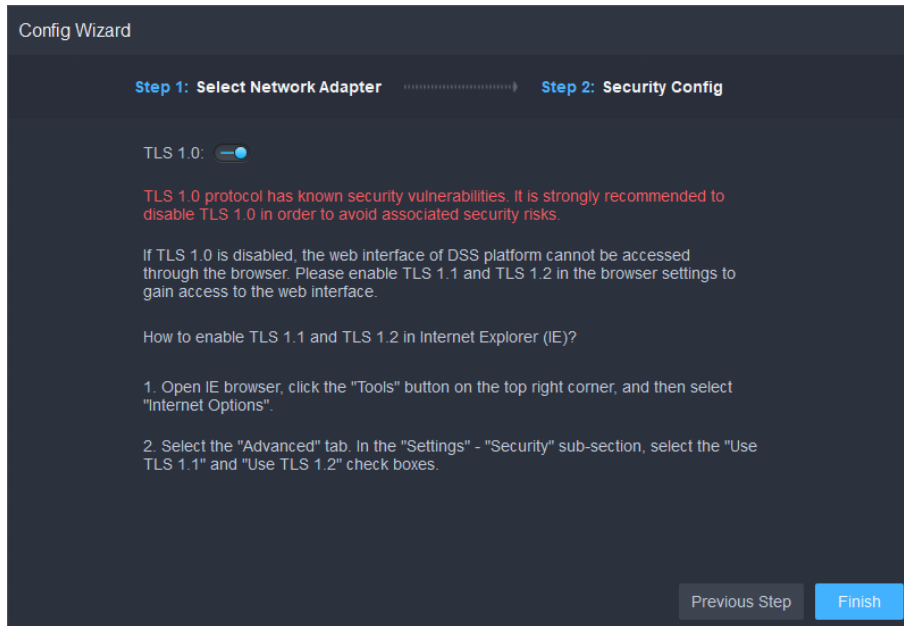
Step 7 Click **Run** when the installation finishes.

Figure 1-9 Select a network card



Step 8 Select the network card you need and click **OK**.

Figure 1-10 Enable or disable TLS1.0



Step 9 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 interface 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 interface.

Step 10 Click **Finish**.



If the available RAM of the server is less than 4 GB, you can only use basic functions related to video. If it is less than 2.5 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. See the following section.

1.1.4 Managing System Services

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


On the server, double-click .

Figure 1-11 Service management interface

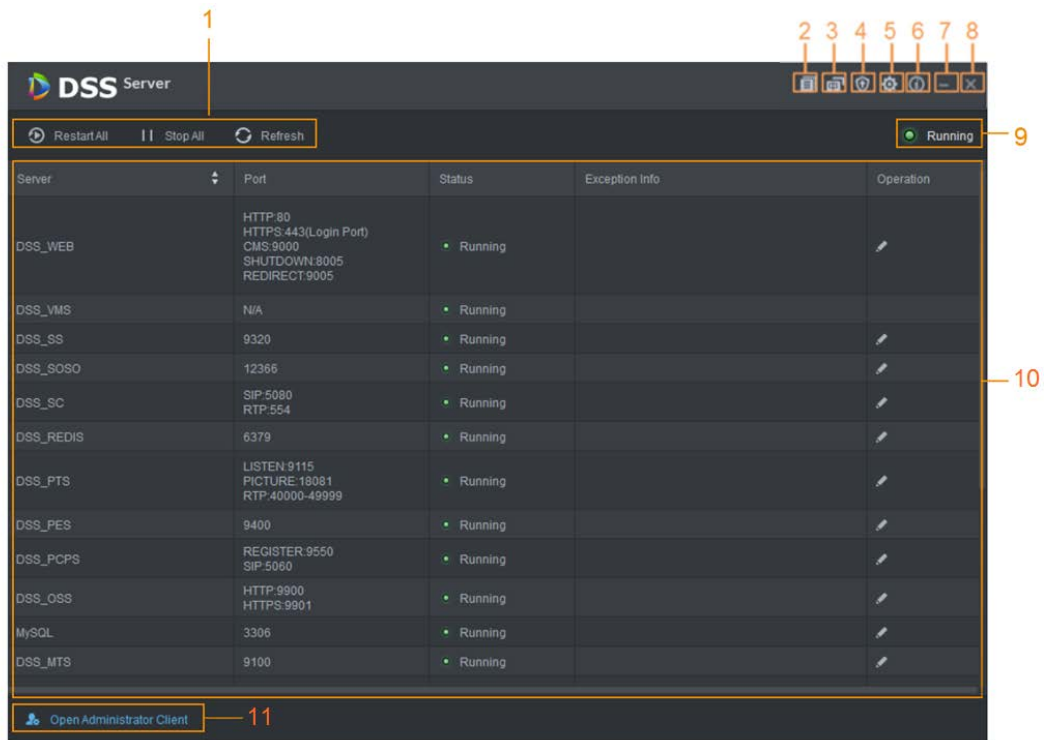












Table 1-2 Interface description

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></p> <p>When starting the platform, if the available memory of the server does not reach 4 GB, only the basic video services can be enabled. If the server has less than 2.5 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 manual.
3	Language	Switch language.

No.	Function	Description
4	Security Setting	<p>TLS 1.0 has known security vulnerabilities. We strongly recommend you disable it to avoid security risks. If it is disabled, the web interface 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 interface.</p> <ol style="list-style-type: none"> 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 section, and then select Use TLS 1.1 and Use TLS 1.2. 5. Click OK.
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	—
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: Intel Core i5, 64 bits 4 Core Processor • Memory: 8 GB and above • Graphics: NVIDIA® GeForce®GT 730 • Network Card: 1000 Mbps • HDD: Make sure that at least 200GB is reserved for DSS client.

1.1.5.1.2 Downloading and Installing DSS Client

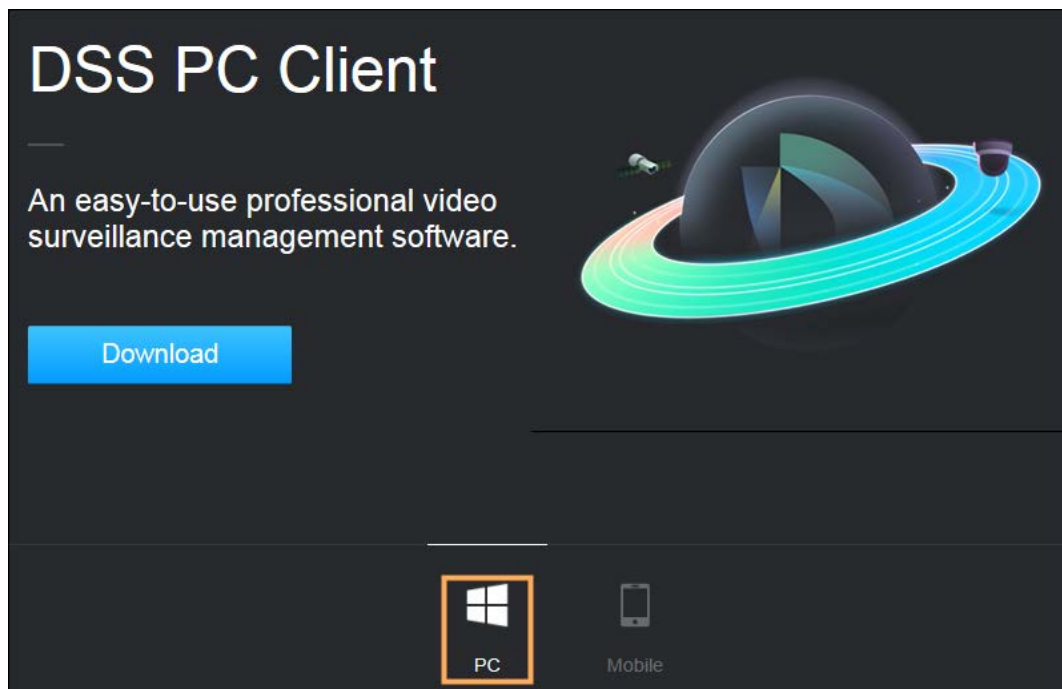
Step 1 Enter the IP address of DSS into the browser and then press Enter.

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

If you save the program, go to Step3.

If you run the program, go to Step4.

Figure 1-12 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.

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 Step2.
- If this is not your first time logging in to the platform, go to Step3.

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**.

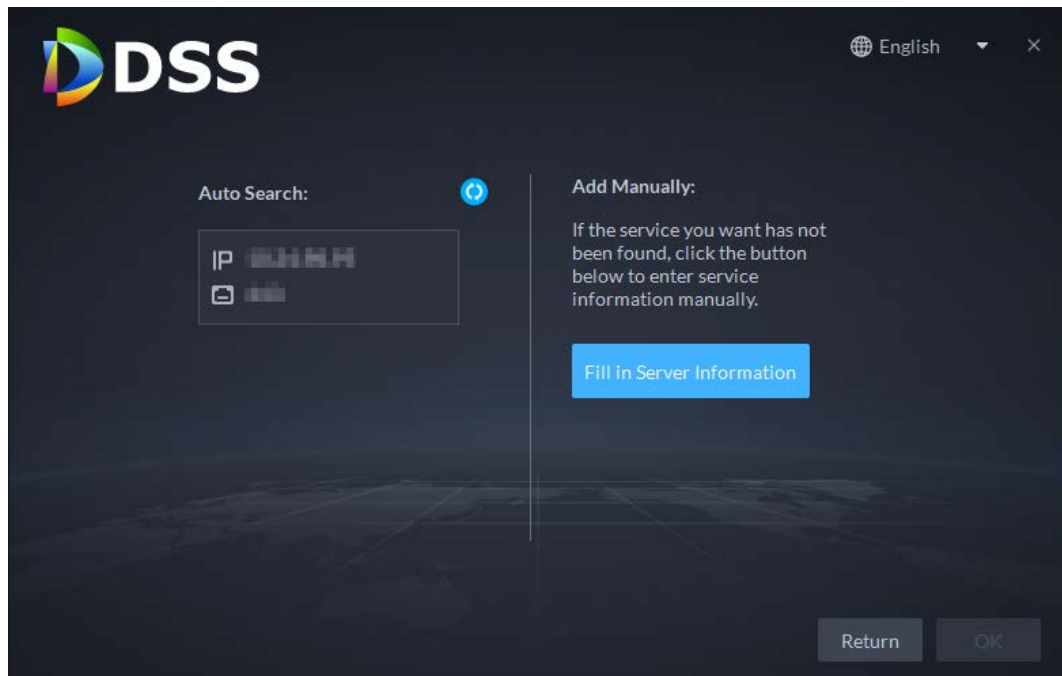
Step 3 Select the detected server on the left of the interface, or click **Fill in site information**, and then enter the IP address or domain name, and the port number.

Server IP is the IP address of DSS server or PC. The port is 443 by default.



If you want to log in to the platform using domain name, you must bind the IP address of the platform to a domain name first. See "1.7 Mapping Domain".

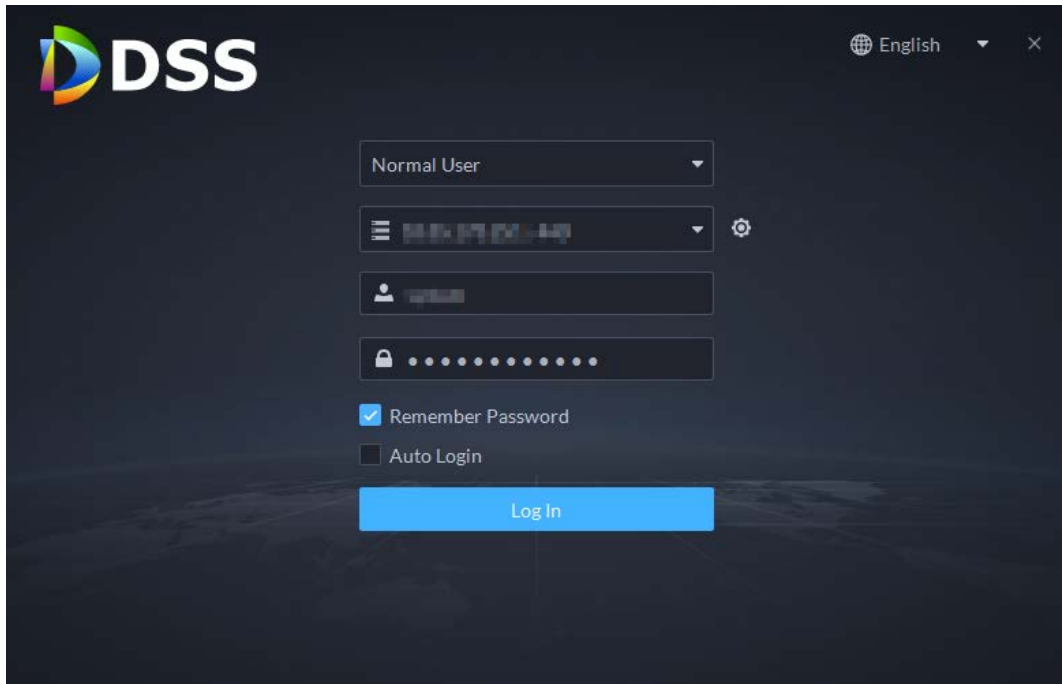
Figure 1-13 Select a site



Step 4 Select a user type, language and platform.

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

Figure 1-14 Login interface (not first-time login)



1.1.5.3 Homepage of DSS Client

Figure 1-15 Homepage

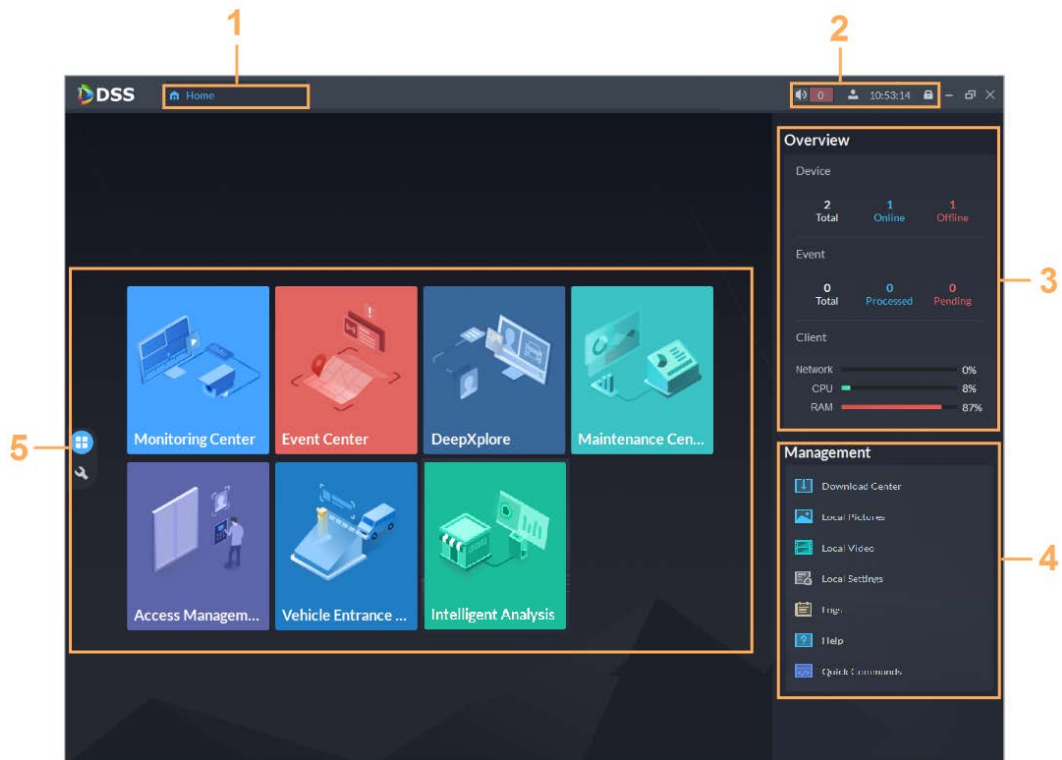








Table 1-4 Description

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 client network, CPU and RAM usage.
4	Management	<ul style="list-style-type: none"> ● 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.
5	Applications	<ul style="list-style-type: none"> ● : Application options including monitoring center, access management, intelligent analysis and vehicle entrance control. ● : Configuration options.

1.1.6 Licensing

Activate the platform with a trial or paid license the first time you log in to it. Otherwise you cannot use it. 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.

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, visit our website and find DSS Pro,

scroll to the bottom, click **Apply**, and then follow the 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, visit our website and find DSS Pro, and then follow the application instructions.
- The platform server can access the Internet.

Procedure


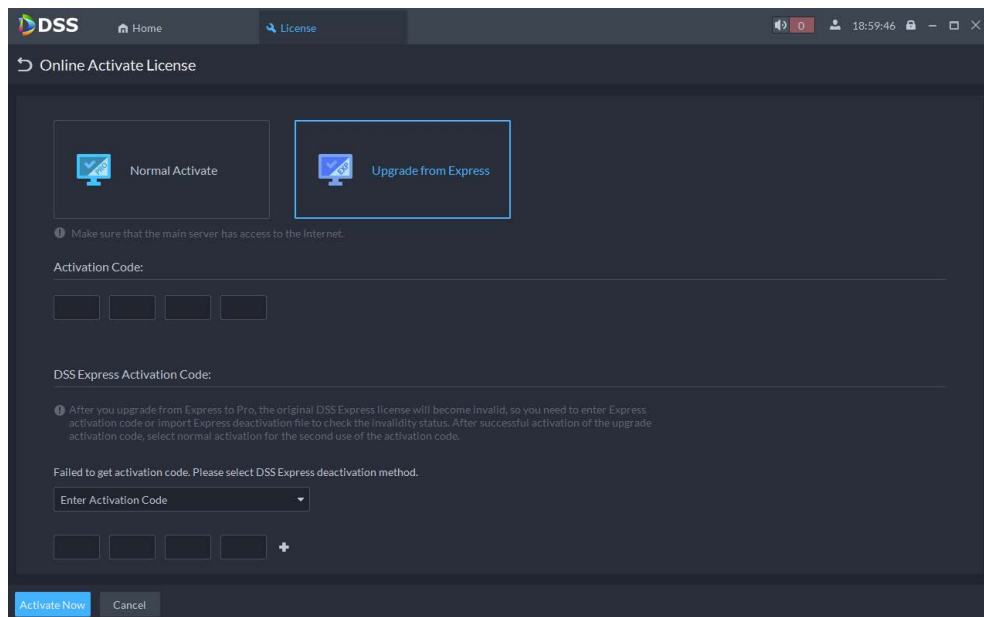

- Step 1 On the **Home** interface, click , and then in **System Configuration**, select **License**.
- Step 2 Click **Online Activate License**.
- Step 3 Select an activation method. Select **Normal Active** to complete the process. If you upgraded the system from Express to DSS Pro, and Express has a paid license, then select **Upgrade from Express** instead.

Figure 1-16 Select a method



- Step 4 Enter your new **Activation Code**.
1. Enter the DSS Pro activation code that you received.
 2. If you select **Upgrade from Express**, enter the original Express activation code or import the deactivation file.
 - Enter the original activation code: Select **Enter Activation Code**, and then enter the original activation code.
 - Import the deactivation file: Select **Import DSS Express Deactivation Code**, click , and then select the deactivation file.

Step 5 Click **Activate Now**.

Step 6 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, visit our website and find DSS Pro, and then follow the application instructions.

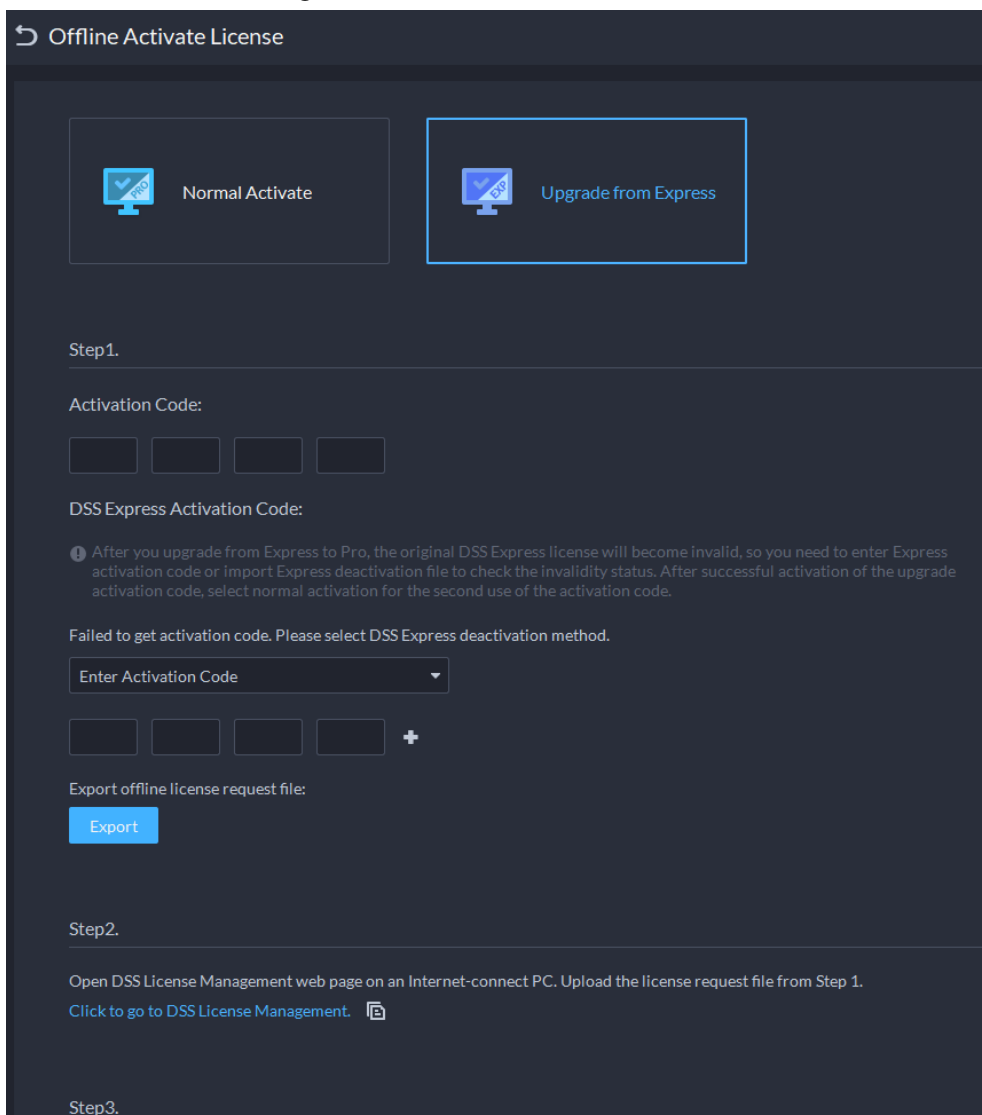
Procedure

Step 1 On the **Home** interface, click , and then in **System Configuration**, select **License**.

Step 2 Click **Offline Activate License**.

Step 3 Select an activation method. Select **Normal Active** to complete the process. If you upgraded the system from Express to DSS Pro, and Express has a paid license, then select **Upgrade from Express** instead.

Figure 1-17 Select a method



Offline Activate License

Normal Activate Upgrade from Express

Step1.

Activation Code:

DSS Express Activation Code:

After you upgrade from Express to Pro, the original DSS Express license will become invalid, so you need to enter Express activation code or import Express deactivation file to check the invalidity status. After successful activation of the upgrade activation code, select normal activation for the second use of the activation code.

Failed to get activation code. Please select DSS Express deactivation method.

Enter Activation Code

Export offline license request file:


Export

Step2.

Open DSS License Management web page on an Internet-connect PC. Upload the license request file from Step 1. [Click to go to DSS License Management.](#)

Step3.

Step 4 Enter your new **Activation Code**.

1. Enter the DSS Pro activation code that you received.
2. If you select **Upgrade from Express**, enter the original Express activation code or import the deactivation file.
 - Enter the original activation code: Select **Enter Activation Code**, and then enter the original activation code.
 - Import the deactivation file: Select **Import DSS Express Deactivation Code**, click , and then select the deactivation file.

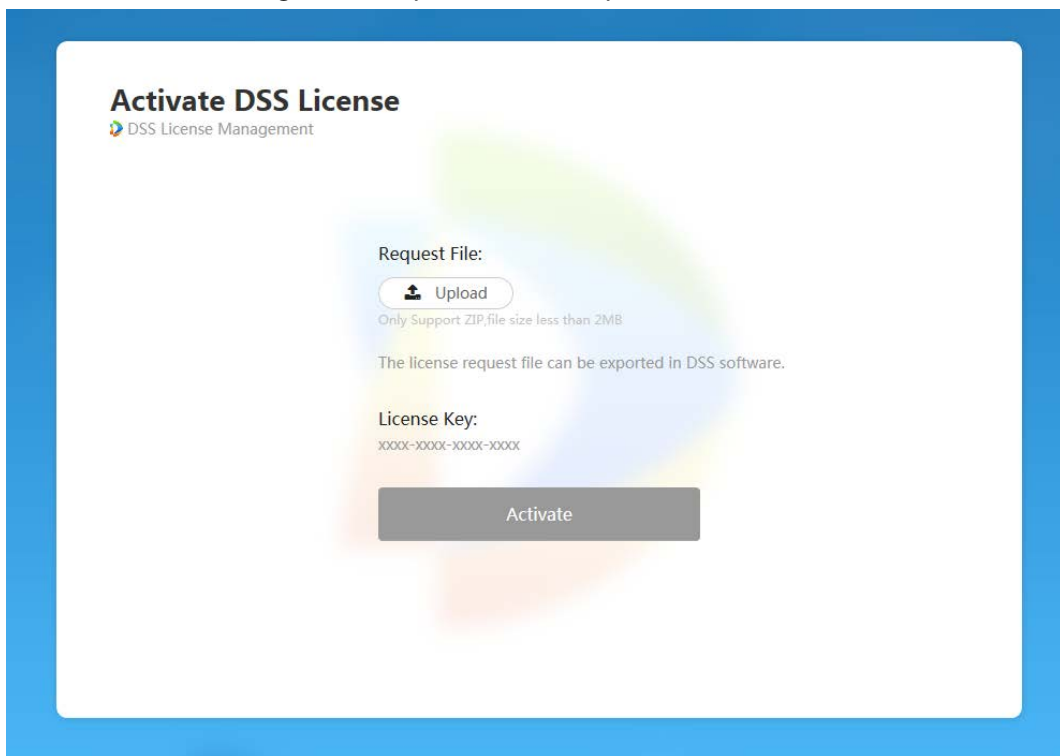
Step 5 Click **Export** to export the license request file.

Step 6 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 1-18 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 7 On the **License** interface, view your license details.

1.2 Distributed Deployment

1.2.1 Installing Main Server

For details about how to install the main server, see "1.1 Standalone Deployment".

After the main server is deployed, log in to it, and then you can view the status of sub servers.

1.2.2 Installing Sub Server

This section introduces how to install sub servers and register them to the main server.

Prerequisites

- You have received the DSS installer from our sales or technical support.
- You have prepared a server that meets the requirements mentioned in "1.1.1 Server Requirements", and the server IP address is set.

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 Select **Sub** for server type, and then click **Next**.

Step 5 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.



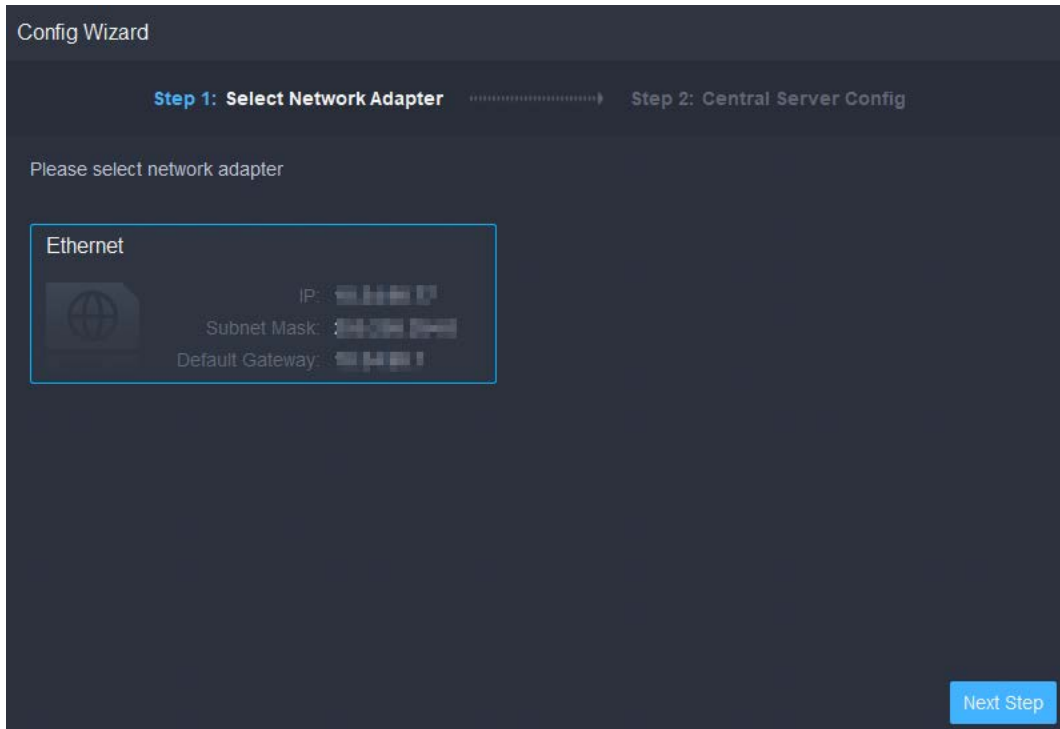
We recommend you do not install the platform into drive C because features such as face recognition require higher disk performance.

Step 6 Click **Install**.

The installation process takes about 5 to 10 minutes.

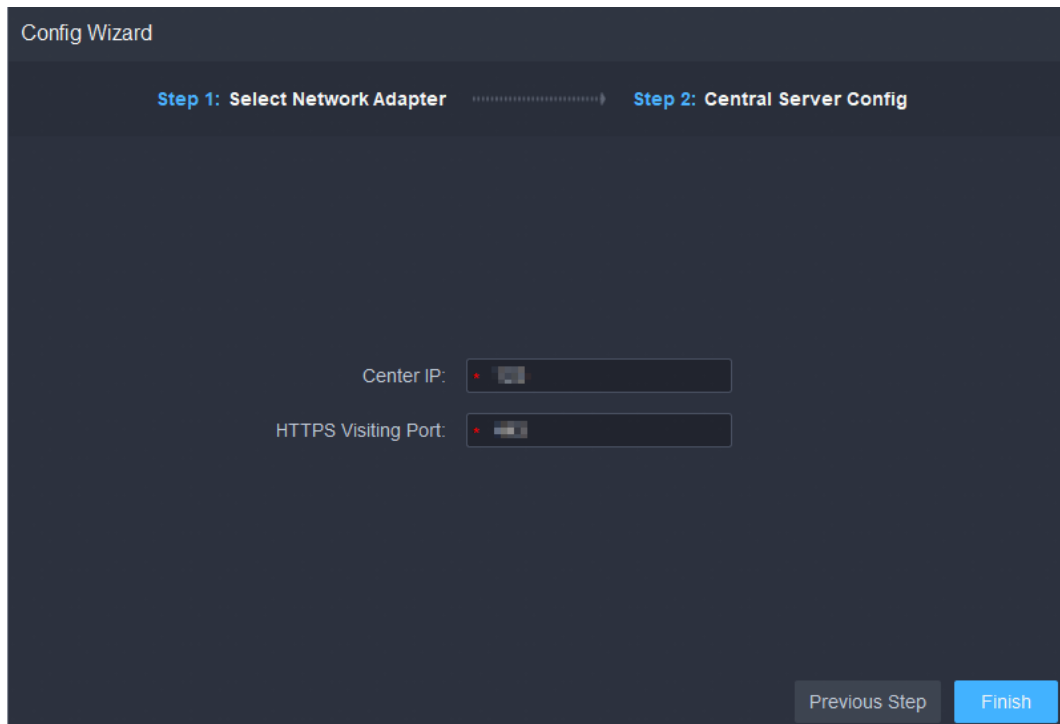
Step 7 Click **Run** when the installation finishes.

Figure 1-19 Select network card



Step 8 Select the network card you need and click **Next Step**.

Figure 1-20 Configure the information of the main server



Step 9 Configure the IP address and port of the main server.

Step 10 Click **Finish**.



After successfully installing a sub server, you need log in to the platform of main server to enable it so that it can work properly.

- To edit service ports, start or stop services, refresh services, view service status or more, see "1.1.4 Managing System Services".

- To uninstall the platform, go to **Control Panel > Programs and Features**, and then locate DSS Server. Double-click it, and then uninstall it according to the on-screen instructions.

1.3 Hot Standby

For details on how to deploy hot standby, contact our technical support.

1.4 Cascade

Attach a DSS platform to another DSS platform, and then you can view videos of the child platform from the parent platform. You can create up to 3 cascade levels.

Prerequisites

Make sure that all the platforms on the system were already installed.

Background Information

- You only need to configure the child DSS information on the parent DSS information.
- Express can only be a child platform.

Procedure

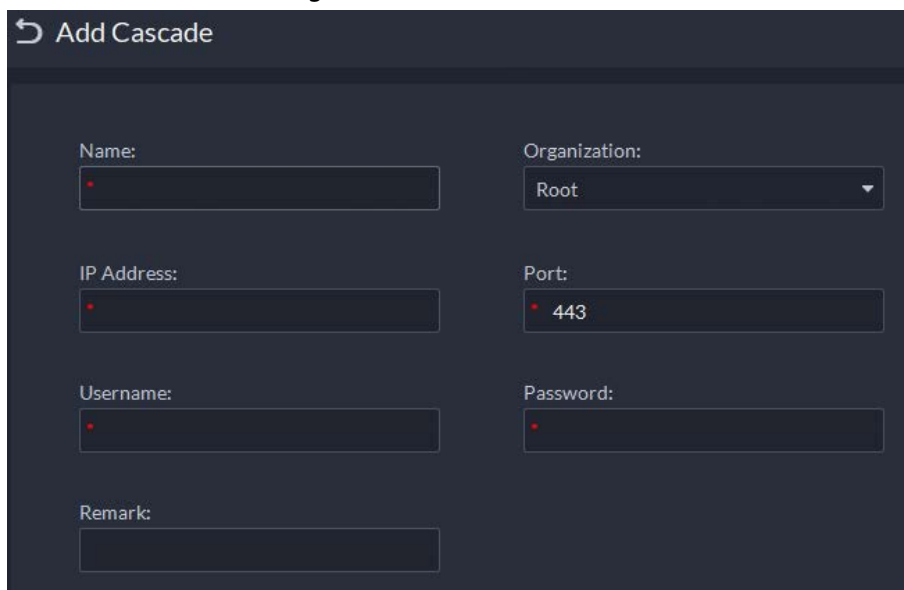
Step 1 Log in to the parent DSS client. On the **Home** interface, click  > **System Deployment**.

Step 2 Click .

Step 3 Click **Add**, and then configure parameters.

- **Organization:** Select an organization for the added platform, so that the resources of the platform will be attached to the organization of the current platform.
- **IP Address, Port, Username and Password:** Enter corresponding information of the added platform.

Figure 1-21 Cascade



Step 4 Click **OK**.


1.5 N+M


On the main server, enable the sub server, and then create the sub-standby relationship.

Prerequisites


The relevant servers have been well deployed.

Step 1 Log in to the parent DSS client. On the **Home** interface, click  > **System Deployment**.

Step 2 Click .

Step 3 Click  to enable the sub servers.

Step 4 Configure a standby server.

1) Click  of a sub server.

2) Select **Standby Server** for **Server Type**, and then click **OK**.

Step 5 Configure the sub-standby relationship in either of the following ways.


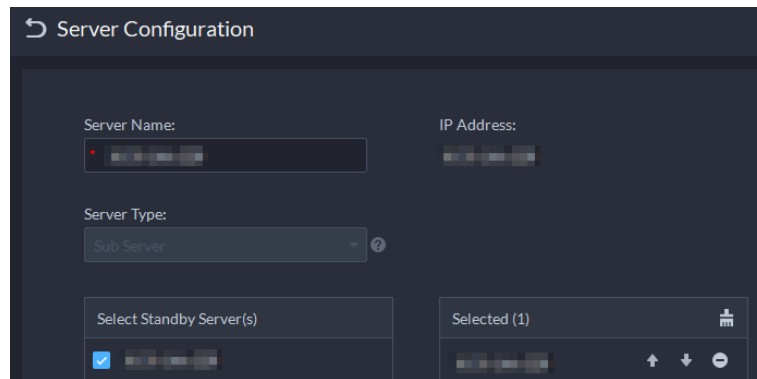


- Go to the **Server Configuration** interface of the sub server to select a standby server.
 1. Click  of a sub server.
 2. On the **Select Standby Server(s)** section, select one or more standby servers.

Figure 1-22 Select a standby server



3. Click **OK**.

- Go to the **Server Configuration** interface of the standby server to select a sub server.
 1. Click  of a standby server.
 2. On the **Select Sub Server(s)** section, select one or more sub servers.
You can click  to adjust the priority.
 3. Click **OK**.

1.6 Configuring LAN or WAN

1.6.1 Configuring Router

If the platform is in a local network, you can visit it from the public network by performing DMZ mapping. For the list of the ports to be mapped, see the port matrix of the platform.



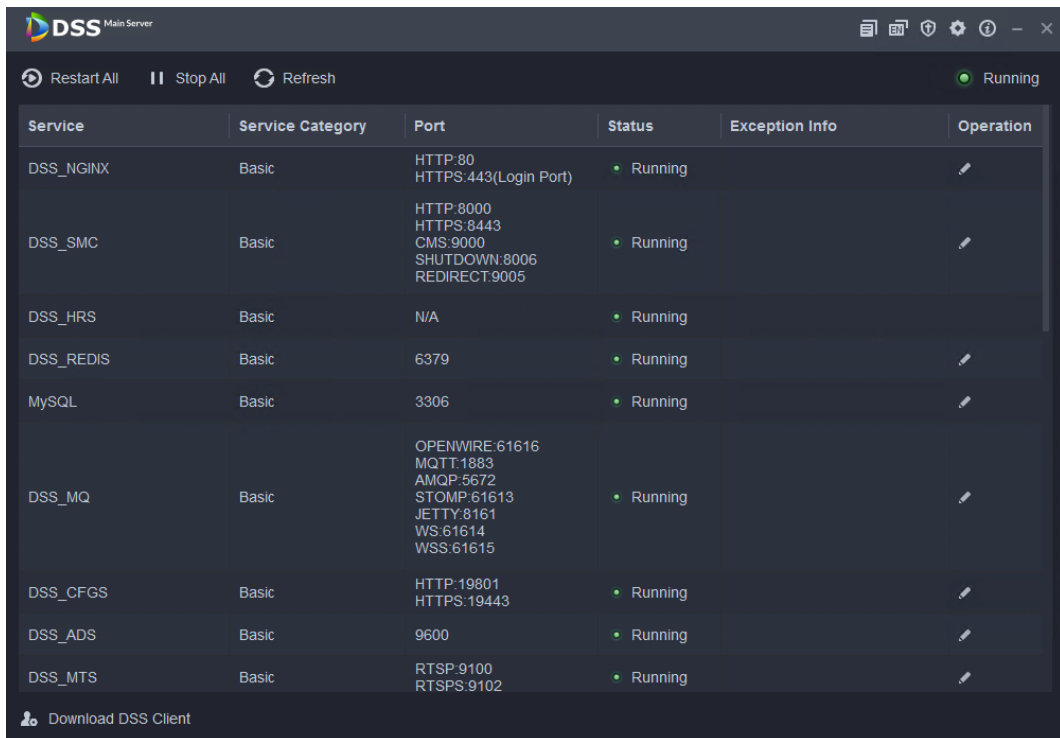
Make sure that the number of the WAN ports is consistent with that of the LAN ports.

1.6.2 Mapping IP

The interface might vary between the main server and the sub server. This section uses the main server interface as an example.

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

Figure 1-23 Status of all services




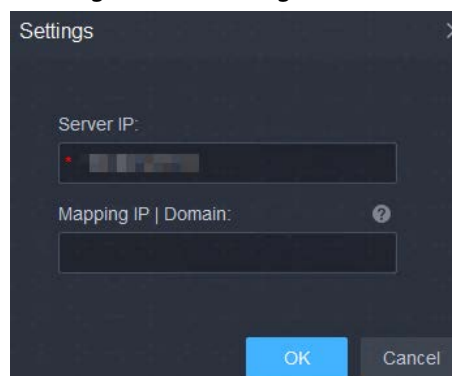
Step 2 Click the  on the upper-right corner.

Figure 1-24 Setting



Step 3 Enter WAN address in the **Mapping IP** box, and then click **OK**.

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

1.7 Mapping Domain

If the server is deployed in a local network, you can map the IP address of the server to a domain

name, and then log in to the server using the domain name.

Prerequisite

Prepare a domain name.

Procedures

See "1.6.2 Mapping IP". In the **mapping IP | Domain** input box, enter the domain name that you prepared, and then click **OK**.

Appendix 1 Service Module Introduction

Appendix Table 1-1 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.
Video Matrix Service	DSS_VMS	Log in to the decoder and send tasks to the decoder to output on the TV wall.
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.
Access Control Service	DSS_ACDG	Manages access control and other related operations.
External LED Device Access Service	DSS_MCDLed	Manages LED access and other related operations.
External Radar Access Service	DSS_MCDRadar	Manages radar 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.

Service Name		Function Description
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.
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.
Media Gateway	DSS_MGW	Sends MTS address to decoders.
Device Update Service	DSS_UPDATE	Updates devices.
File Resource Node Management Service	DSS_FNODE	Manages the file resource node management service.
File Resources Node Service	DSS_FILERESOURCE	Manages files from MPT devices and related operations.
Configuration Service	DSS_CFGS	Manages disks, such as read-and-write operations.
Access Controller Access Service	DSS_MCDDOOR	Manages access controller access and related operations.

Appendix 2 Cybersecurity 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 a whitelist 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.