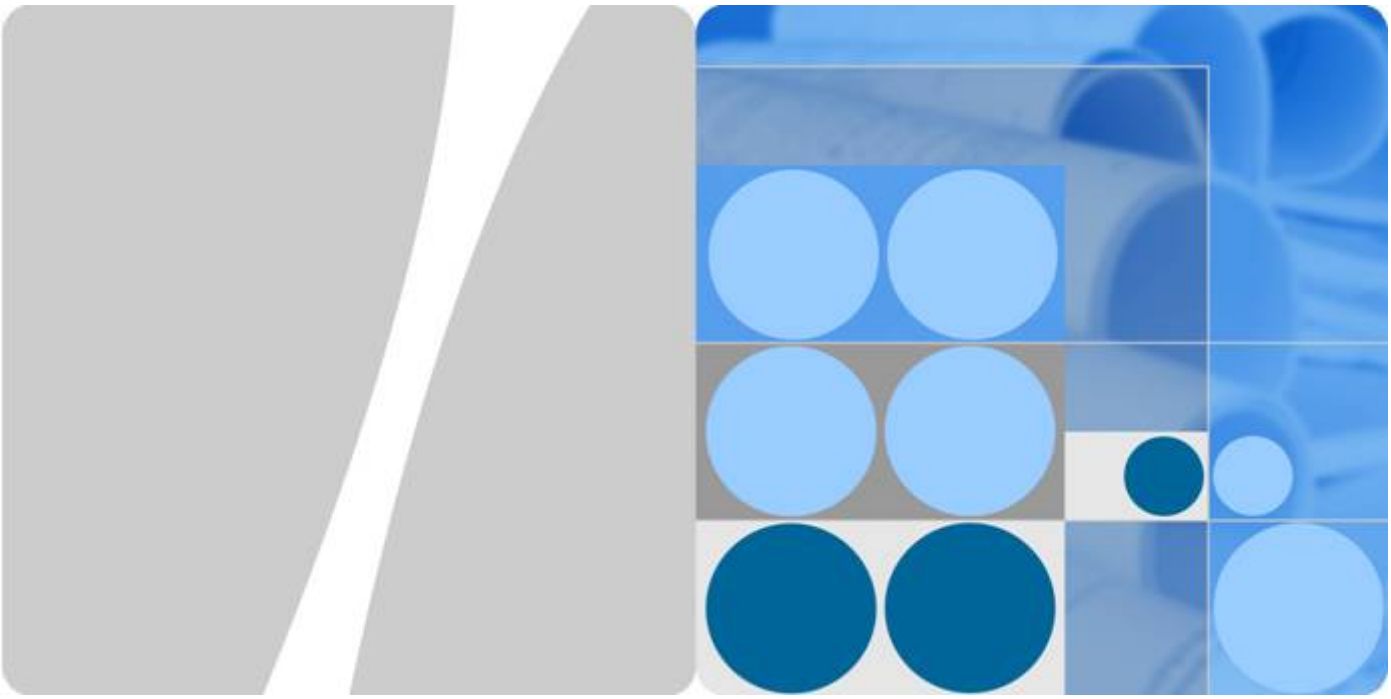


HUAWEI DP300 Desktop Presence

V500R002C00

# Security Maintenance


Issue 01

Date 2015-09-15



HUAWEI TECHNOLOGIES CO., LTD.

### Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

### Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

## Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://e.huawei.com

# About This Document

## Overview

This document introduces security maintenance operations of HUAWEI DP300 desktop presence (DP300 or endpoint for short).

Before you use the product, refer to the product vendor for version mapping information and to confirm compatibility with other videoconferencing equipment.

## Intended Audience

This document is intended for:

- Technical support engineers
- Maintenance engineers

## Symbol Conventions

The symbols that may be found in this document are defined as follows:

| Symbol | Description |
| --- | --- |
|   | Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury. |
|   | Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury. |
|   | Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury. |
|   | Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results.<br>NOTICE is used to address practices not related to personal injury. |

| Symbol | Description |
| --- | --- |
| NOTE | Calls attention to important information, best practices and tips.<br>NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration. |

# Related Documents

| Document Title | Description | Document Location |
| --- | --- | --- |
| HUAWEI DP300 Desktop Presence V500R002C00 Quick Installation Guide | Describes the packaged items and provides guidance for quick installation, and common configuration. | Access **http://e.huawei.com** and choose **Support > Product Support > UC&C > Telepresence and Videoconferencing > Telepresence Endpoints > Desktop Device**. |
| HUAWEI DP300 Desktop Presence V500R002C00 Quick Start Guide | Describes the touchscreen and the remote controlled UI, and provides quick instructions in commonly-used endpoint functions. | |
| HUAWEI DP300 Desktop Presence V500R002C00 User Guide | Describes the methods for operating the endpoint. | |
| HUAWEI DP300 Desktop Presence V500R002C00 Administrator Guide | Describes how to configure, manage, and troubleshooting the endpoint. | |
| HUAWEI DP300 Desktop Presence V500R002C00 Command Reference | Describes the functions, parameters, formats, usage guidelines, and examples of all endpoint commands. | |
| HUAWEI DP300 Desktop Presence V500R002C00 Communication Matrix | Describes the ports, protocols, IP addresses, and authentication modes for the communication of the endpoint. | |

# Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in earlier issues.

## Issue 01 (2015-09-15)

This issue is used for first office application (FOA).

# Contents

# 1 Overview

## 1.1 Purpose of Security Maintenance

Now application systems face severe security threats. Once problems occur, business might be disturbed, profits reduced, or even systems break down. Users must build up and maintain the application system security from different layers, and discover and solve potential threats in advance.

Besides, considering the endless emergence of safety threats, a mere dependence on technology can hardly ensure the application system security. Users must build up a safety management system based on security maintenance suggestions and problems they found during the use of the endpoint to ensure a smooth and safe operation of the endpoint.

## 1.2 What Is Layered Security Maintenance

According to the target and purpose of security maintenance, maintenance personnel must safeguard the service system from different layers.

### Application Layer

Security maintenance of the application layer is to protect the and its web management system so that they can provide services to users with a smooth operation.

### System Layer

Security maintenance of the system layer is to ensure a smooth operation of the operating system, which can support the operation of application software.

### Network Layer

Security maintenance of the network layer is to ensure that network devices, such as the switch, router, and firewall, function properly and that security strategies are implemented at the network layer.

## Management Layer

Security maintenance of the management layer is to strengthen people's management and avoid threats. Maintenance from the management layer involves the maintenance operations at all preceding layers.

# 2 Application Layer Security

## 2.1 Setting the Interaction Mode

On the DP300 display, tap  in the lower right corner to switch between the PC mode and videoconferencing mode.

In PC mode, the DP300 display can be used as the PC monitor, on which you can answer calls to join conferences.

In videoconferencing mode, the DP300 display functions as a platform for users to interact with the videoconferencing system using the touchscreen or remote control.

- Touchscreen (default): Perform operations on the screen by touches, such as tap and slide. In this case, the DP300 display is called touchscreen.
- Remote control: Perform operations on the screen using the remote control. In this case, the DP300 display is called remote control screen.

To set the interaction mode, perform the following steps:

- On the touchscreen, tap  , choose **Advanced** > **Settings** > **General**, and set **Control mode**.
- On the remote control screen, choose **Advanced** > **Settings** > **General**, and set **Control mode**.
- On the web interface, choose **System Settings** > **General**, and set **Control mode**.

## 2.2 Application Layer Account List

### 2.2.1 Administrator Password for the Display

The default administrator password for logging in to the display is **12345678**. To improve device security, set a password at your first login and regularly change the password afterwards. To enhance user experience, the administrator password can be digit-only or empty.

**NOTE**

It is recommended that you set a complex password. A simple or empty password brings security risks.

To set the administrator password for logging in to the display, perform the following steps:

- On the touchscreen, tap  and choose **Advanced** > **Settings** > **Security** > **Password**.
- On the remote control screen, choose **Advanced** > **Settings** > **Security** > **Password**, and set the password.
- On the web interface, choose **System Settings** > **Security** > **GUI**, and set the password.

When using the administrator password for logging in to the display, note that:

- On the touchscreen, the administrator password is required for accessing the **Settings** screen. On the remote control screen, the administrator password is required for customizing the option bar.
- Standard users: By default, they can directly access **Advanced** but must enter the administrator password to access the **Settings** screen under **Advanced** and customize the option bar. (The administrator password can be obtained from the administrator.)
- If the administrator select **Encryption advanced settings**, standard users can directly access **Settings** but must enter the administrator password to access the **Advanced** menu and customize the option bar. If the administrator password is set to null, no password is required for accessing any menu.

## 2.2.2 Web Management Account

The DP300 supports a maximum of 10 concurrent logins to the web interface, and controls user permissions by setting permission levels. **Table 2-1** describes the web management account.

**Table 2-1** Web management account

| Account Name | Default Password | Description | Remarks |
| --- | --- | --- | --- |
| admin | Change_Me | This account is the default account with the highest permission and cannot be deleted.<br>For details about account levels, see section **Web Management Users**. | To ensure account security, you are advised to change the password at the first login and regularly change the password afterward.<br>To change the password:<br>● On the touchscreen, tap  and choose **Advanced** > **Settings** > **Security** > **Web Login**.<br>● On the remote controlled UI, choose **Advanced** > **Settings** > **Security** > **Web Login**.<br>● On the web interface, choose **System Settings** > **General** > **Personal**.<br>To change the **Administrator name**, you can tap  and choose **Advanced** > **Settings** > **Security** > **Web Login** from the touchscreen.<br>To change the **Administrator name**, you can choose **Advanced** > **Settings** > **Security** > **Web Login** from the remote controlled UI. |

**NOTE**

The web management account has the permission of exporting the address book, exporting logs or exporting settings. Keep the account safe to prevent disclosure of personal information.

If the number of user attempts to log in to the web interface reaches a predefined number, the user account will be locked and cannot be used for login until the locking duration ends. To set the maximum number of user login attempts and locking duration, perform the following operations:

On the web interface, choose **System Settings** > **Security** > **Web Login**. On the displayed screen, set **Maximum login attempts** and **Lock time**.

## 2.2.3 API Account

The API account is required for a third party (for example, a touch panel) to log in to the DP300, or for the SMC2.0 to to add a manageable site. **Table 2-2** describes the API account.

**Table 2-2** describes the touch panel account.

**Table 2-2** API account

| Account Name | Default Password | Description | Remarks |
|---|---|---|---|
| api | Change_Me | The account is required for a third party (for example, a touch panel) to log in to the DP300, or for the SMC2.0 to to add a manageable site.<br>This account is the default account. To change the name: On the web interface, choose **System Settings** > **General** > **Personal** > **Password of API user**. | To ensure account security, you are advised to change the password at the first login and regularly change the password afterward.<br>For details about how to change the password, see section **2.6.2 Changing the Password**. |

## 2.2.4 SSH and Telnet Login

The DP300 supports the Telnet login and Security Shell (SSH) login. Telnet is an insecure protocol. SSH is a cybersecurity protocol for remote access using the encryption and authentication mechanism in an insecure cyber environment. During SSH login, all user data are encrypted. To ensure the security, you are advised to use the SSH login.

- You can log in to the DP300 through port 23 using Telnet. **Telnet login** is set to **Do not allow** by default. Telnet is an insecure communication protocol. You are advised to disable it. If you want to log in using Telnet, see section **2.8.1 Enabling SSH or Telnet**.
- You can log in to the DP300 through port 22 using SSH. **SSH** is set to **Do not allow** by default. If you want to log in using SSH, see section **2.8.1 Enabling SSH or Telnet**.

### SSH and Telnet Login Under the Normal System

The normal system supports SSH and Telnet logins. **Table 2-3** describes the account names and passwords used for SSH and Telnet logins.

**Table 2-3** SSH and Telnet login accounts

| Account Name | Default Password | Description | Remarks |
|---|---|---|---|
| debug | Change_Me | Administrator account with the highest permission for system debugging. | This is a special account and not for common users. |
| admin | Change_Me | Common user account with lower permission than the **debug** account. | - |

| Account Name | Default Password | Description | Remarks |
|---|---|---|---|
| user | Change_Me | Common user account with lower permission than the **admin** account. | - |
| apiuser | Change_Me | Special account with lower permission than the **user** account. | This is a special account and not for common users. |
| test | Change_Me | Dedicated account for testing with lower permission than the **user** account. | - |

NOTE

- To secure your account, it is recommended that you change the password upon the first login and regularly change the password afterwards.
- After you log in using the debug account, you can run the command **mnt debug setpwd [name]** to change other accounts' passwords.

### Telnet Login Under the Mini System

The mini system supports Telnet logins only. The login account and default password are described in **Table 2-4**.

**Table 2-4** Telnet login account

| Account Name | Default Password | Description | Remarks |
|---|---|---|---|
| debug | Change_Me | Administrator account for system debugging | To ensure account security, change the password at the first login and regularly change the password afterward. |

For details about how to change the password and use the debug commands, see the *HUAWEI DP300 Desktop Presence V500R002C00 Command Reference*.

## 2.2.5 Serial Port Account

The DP300 allows for logins using serial ports to commission applications and locate faults. The serial port account and default password are described in **Table 2-5**.

**Table 2-5** Serial port account

| Account Name | Default Password | Description | Remarks |
|---|---|---|---|
| root | Change_Me | This account is used for a computer to log in to the DP300 through serial ports. | To secure your account, it is recommended that you change the password upon the first login and regularly change the password afterwards. To change the password, run the **passwd** command. |

## 2.2.6 Upgrade Password

To upgrade the DP300 under the normal system with the upgrade tool, you must enter the upgrade password.

By default, the upgrade password is **Change_Me**.

You are advised to change the password at the first login and regularly change the password afterward:

- Touchscreen: Tap  and choose **Advanced** > **Settings** > **Security** > **Upgrade password**.
- On the remote controlled UI, choose **Advanced** > **Settings** > **Security** > **Upgrade password**.
- On the web interface, choose **System Settings** > **Security** > **Upgrade password**.

## 2.2.7 Air Content Sharing Password

The air content sharing password is used by an air content sharing client to connect to the DP300. Users can download the air content sharing client from the DP300 web interface. After the air content sharing client successfully connects to the DP300, users can connect the DP300 to presentation sources and share presentations without the use of any physical ports.

The default air content sharing password is **Change_Me**.

You are advised to change the password at the first login and regularly change the password afterward:

- Touchscreen: Tap  and choose **Advanced** > **Settings** > **Security** > **Air Content Sharing**.
- On the remote controlled UI, choose **Advanced** > **Settings** > **Security** > **Air Content Sharing**.
- On the web interface, choose **System Settings** > **Security** > **Air Content Sharing**.

## 2.2.8 Network Diagnostics Tool Account

After the network diagnostics function is enabled, the network diagnostics tool can use the H.323 call port, RAS source port, RAS destination port, or SIP call port to diagnose the DP300. Table 2-6 describes the network diagnostics tool account.

**Table 2-6** Network diagnostics tool account description

| Account Name | Default Password | Description | Remarks |
|---|---|---|---|
| admin | Change_Me | Specify the account name and password that the network diagnostics tool uses for authentication when attempting to communicate with the DP300. | To ensure account security, you are advised to change the password at the first login and regularly change the password afterward.<br>On the web interface, choose **System Settings** > **Network** > **Network diagnostics**, enable **Network diagnostics**, and change the values of **Diagnostics tool user name** and **Diagnostics tool password**. |

## 2.2.9 Information Required for Connecting to the Videoconferencing Network Management System

The DP300 communicates with and is remotely managed by the videoconferencing network management system using SNMP. The videoconferencing network management system implements the following:

- Configures DP300 settings, including the H.323 and SIP.
- Queries DP300 status.
- Checks DP300 alarms.
- Backs up and restores DP300 settings.
- Upgrades the DP300 online.

To remotely manage the DP300 from the videoconferencing network management system, log in to the web interface of the DP300, choose **System Settings** > **Network** > **SNMP Settings**, and set SNMP parameters, as shown in Table 2-7.

When the videoconferencing network management system connects to the DP300 through SNMP V2, configure required SNMP V2 information. When the videoconferencing network management system connects to the DP300 through SNMP V3, configure the SNMP V3 account, password, and protocol.

**Table 2-7** Information required for connecting to the videoconferencing network management system

| Parameter | | Default Setting | Description | Remarks |
|---|---|---|---|---|
| SNMP V2 | Get community name | Change_Public | Specifies the credential that the videoconferencing network management server uses to obtain DP300 settings. | The parameter settings must be the same as those in the videoconferencing network management system.<br>Set these parameters when **Enable SNMP** is set to **Enable** and **SNMPv2** to **Enable**. |
| | Set community name | Change_Private | Specifies the credential that the videoconferencing network management server uses to specify DP300 settings. | |
| | Trap community name | Change_Me | Specifies the credential that the DP300 uses to report alarms to the videoconferencing network management server. | |
| SNMP V3 | User name | v3user | Specifies the user name for connecting your DP300 to the videoconferencing network management system through SNMPv3. | The parameter setting must be the same as that in the videoconferencing network management system. |
| | Authentication protocol | SHA | Specify the authentication mode and password for connecting the videoconferencing network | The parameter settings must be the same as those in the videoconferencing network management system.<br>When the videoconferencing network management system |

| Parameter | | Default Setting | Description | Remarks |
|---|---|---|---|---|
| | Authentication password | Change_Me | management system to your DP300. | attempts to connect to your DP300, Authentication protocol and New password set on your DP300 are required. |
| | Encryption protocol | AES | Specify the encryption protocol and password for connecting the videoconferenc-ing network management system to your DP300. | The parameter settings must be the same as those in the videoconferencing network management system. |
| | Encryption password | Change_Me | | |

**NOTE**

- To secure your account, it is recommended that you change the password upon the first login and regularly change the password afterwards. The password you set on the DP300 must be the same as that set in the videoconferencing network management system.
- For details about how to set SNMP parameters, see the *HUAWEI DP300 Desktop Presence V500R002C00 Administrator Guide*.

# 2.3 Restoring Systems to Default Settings

If you forget the passwords of the normal or mini system, restore the system (including the passwords) to its default settings.

- Normal system

Restores the DP300 to its default settings, if you press and hold the **RESET** button for 10 seconds or more when the DP300 is operating properly.

**NOTE**

Place the DP300 face down on the desktop, and open its rear cover. Then you can view the interfaces on the rear panel. The **RESET** button is located at the second position on the left of the rear panel.

- Mini System

1. Press and hold the **RESET** button for 10 seconds or more when the DP300 is starting.

   The DP300 enters the mini system.
2. In mini system, press and hold the **RESET** button for 10 seconds or more to restore the **Telnet** login password to its default settings.

# 2.4 SiteCall Security

The DP300 uses Hypertext Transfer Protocol Secure (HTTPS) mode to upload the multipoint conference information and supports Transmission Control Protocol (TCP) mode when a multipoint conference is initiated. If **HTTPS mode** is disabled, the DP300 uses the insecure TCP mode. You are advised to use HTTPS mode for better communication security.

If **HTTPS mode** is enabled, you are advised to enable **Multipoint conference authentication**.

Enable **HTTPS mode** and **Multipoint conference authentication**.

- On the touchscreen, tap  and choose **Advanced** > **Settings** > **Network** > **IP** > **H.323**, and then select **HTTPS mode** and **Multipoint conference authentication**.
- On the remote controlled UI, choose **Advanced** > **Settings** > **Network** > **IP** > **H.323**, and select **HTTPS mode** and **Multipoint conference authentication**.
- On the web interface, choose **System Settings** > **Network** > **H.323/SIP Settings**, and set **HTTPS** mode and **Multipoint conference authentication** to **Enable**.

# 2.5 Configuring Encryption

You can enable encryption to improve video communication security.

## Background

On an IP network that is neither quality-guaranteed nor secure, encryption can be used to increase the video communication security, though it may affect the call rate. Both parties in communication must support encryption, including H.235 encryption and Secure Real-time Transport Protocol (SRTP) encryption.

To improve communication security, you are advised to enable encryption.

Before initiating a Session Initiation Protocol (SIP) encrypted conference, you are advised to enable encryption and Transport Layer Security (TLS) registration to improve communication security.

## Procedure

To configure encryption on the touchscreen:

1. Tap  and choose **Advanced** > **Settings** > **Security** > **Encryption**, and then select one of the following options:
   - **Disable**: No stream is encrypted.
   - **Enable**: Streams are forced to be encrypted. If you select this option, your DP300 can attend encrypted conferences only. To improve communication security, select this option.
   - **Maximum interconnectivity**: Streams are encrypted only when a call is set up. If you select this option for the local site and encryption is disabled at a remote site, the conference between the local and remote sites is not encrypted.
2. Select **Save**.

To configure encryption on the remote controlled UI:

1. Choose **Advanced** > **Settings** > **Security** > **Encryption** and select one of the following options:
   - **Disable**: No stream is encrypted.
   - **Enable**: Streams are forced to be encrypted. If you select this option, your DP300 can attend encrypted conferences only. To improve communication security, select this option.
   - **Maximum interconnectivity**: Streams are encrypted only when a call is set up. If you select this option for the local site and encryption is disabled at a remote site, the conference between the local and remote sites is not encrypted.
2. Select **Save**.

To configure encryption on the web interface:

1. Log in to the web interface, choose **System Settings** > **Security** > **Encryption** and configure the encryption mechanism.
2. Select **Save**.

# 2.6 Web Management Users

The web interface of the DP300 supports two types of users: administrators and common users.

- Administrators: Administrators have all permissions to the web interface.

NOTE

Administrators can modify accounts and passwords of common users, as well as system configuration operations.

- Common users: They have some permissions on the web interface and can configure only personal settings but not system settings.

## 2.6.1 Logging In to the Web Interface

The DP300 supports logins in HTTP and HTTPS modes. HTTPS mode, which is more secure, is used by default. If you use HTTP to log in to the web interface of the DP300, the system automatically switches to the HTTPS mode.

**Step 1** Open a browser on the computer. In the address box, enter the IP address, such as **https://192.168.1.1**.

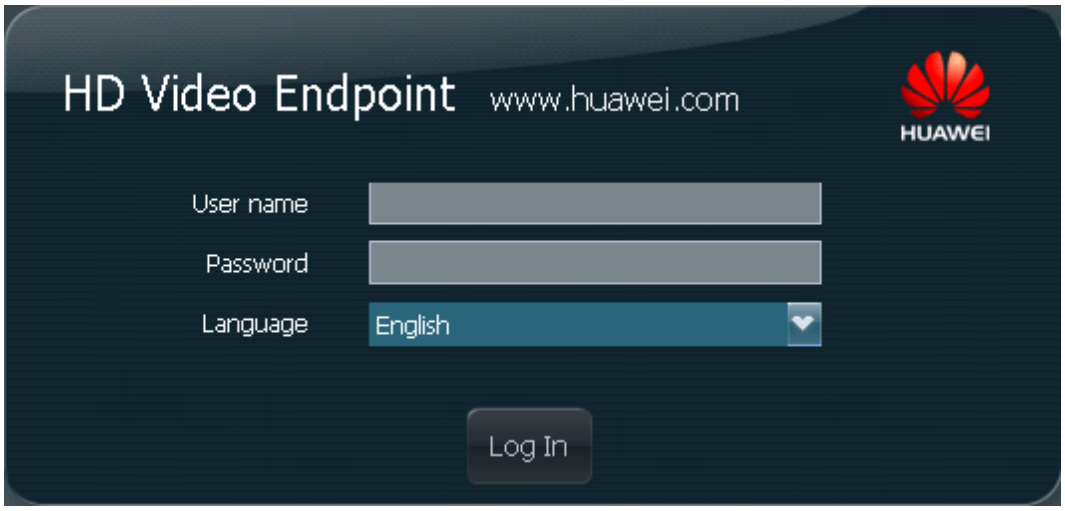
**Step 2** Press **Enter**.

The login page is displayed, as shown in **Figure 2-1**.

NOTE

If the security certificate is invalid, click **Continue to this website** to resume the login.

**Figure 2-1** Web login page




**Step 3** Enter the user name and password. Select a **language**.

**Step 4** Click **Log In**, or press **Enter**.

NOTE

To ensure data security, after accessing the web interface, close the browser and delete browser caches.

**----End**

## 2.6.2 Changing the Password

On the web interface, you can change the passwords for the web management account, common user accountand API account as follows:

**Step 1** Choose **System Settings** > **General** > **Personal**.

**Step 2** Change the account password.

The password can contain 8 to 32 characters and must include at least two of the following: uppercase letter, lowercase letter, digit, or special character.

**Step 3** Click **Save**.

**----End**

# 2.7 Web Access Control

The DP300 adopts HTTPS mode, which is the secure version of Hypertext Transfer Protocol (HTTP). Following are methods to control the web access:

- Support the user to submit the log out application.

  When you have logged in to the web interface, you can click **Exit** in the upper right. The login interface is displayed.
- You are allowed to use the touchscreen to control web login.

  To disable web login, choose **Advanced** > **Settings** > **Secured** > **Web Login** on the touchscreen and deselect **Web Login**.

- You are allowed to use the remote control to control web login.

  To disable web login, choose **Advanced** > **Settings** > **Secured** > **Web Login** on the remote control and deselect **Web Login**.
- The supports a maximum of 10 concurrent logins to the web interface.

# 2.8 SSH Access Control

During remote access and data transmission, SSH commands can be run to create an encrypted channel between the application layer and client.

## 2.8.1 Enabling SSH or Telnet

Use either of the following ways to enable SSH or Telnet.

- On the touchscreen, tap  and choose **Advanced** > **Settings** > **Security** > **SSH/Telnet**, and then select SSH or Telnet.
- On the remote controlled UI, choose **Advanced** > **Settings** > **Security** > **SSH/Telnet**, and select SSH or Telnet.
- On the web interface, choose **System Settings** > **Security** > **SSH/Telnet**, and set **SSH** or **Telnet** to **Enable**.

  Telnet is an insecure communication protocol. You are advised to disable it.

## 2.8.2 User Login

Following describes SSH access control methods using the PuTTY as an example.

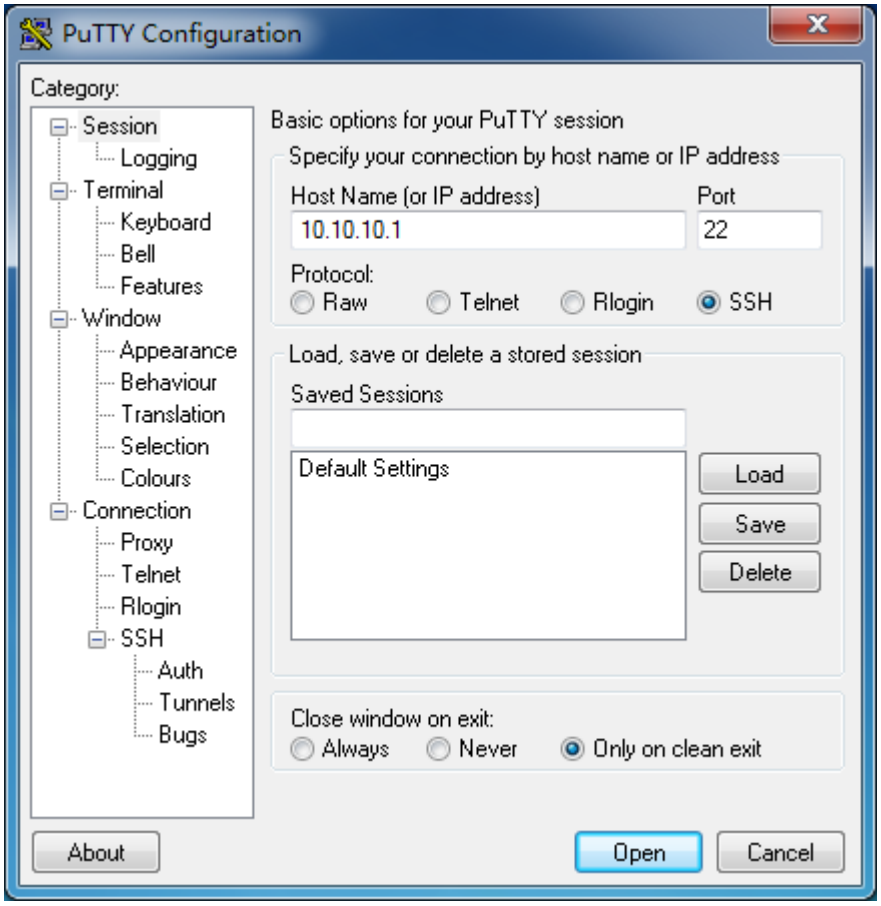
**NOTE**

PuTTY is a login application for remote login across different platforms. It can be obtained from Huawei Unified Communications and Collaboration (UC&C) Security Center by Huawei technical support or downloaded from the Internet. Use PuTTY 0.63 or a later version.

**Step 1** Run PuTTY on your computer.

The PuTTY Configuration dialog box is displayed, as shown in **Figure 2-2**.

**Figure 2-2** PuTTY Configuration dialog box




**Step 2** In **Host Name (or IP address)**, enter the IP address, such as **10.10.10.1**.

**Step 3** Select **SSH** for **Protocol**. Use the default value for **Port**.

**Step 4** Click **Open**.

The login interface is displayed.

**Step 5** Enter the user name and password and run the commands. For details, see the *HUAWEI DP300 Desktop Presence V500R002C00 Command Reference*.

**NOTE**

The default administrator account of Telnet and SSH is **debug** and the password is **Change_Me** by default.

**----End**

## 2.8.3 Logging In Using the SSH Public Key

To secure and simplify SSH login, use the SSH public key to log in to the DP300.

**NOTE**

Before logging in to the DP300 using the SSH public key, ensure that SSH has been enabled. For details, see **2.8.1 Enabling SSH or Telnet**.

## Creating An SSH Private-Public Key Pair

Create a SSH private-public key pair and associate the private-public key pair with the local computer or server.

**Step 1** Log in to the Linux operating system, run the **ssh-keygen** command in any CLI, and press **Enter**.

**Step 2** Enter the name (for example, DP300) of the SSH private-public key pair as prompted and press **Enter**.

The SSH public key **DP300.pub** and SSH private key **DP300** are created.

**Step 3** Go to the directory where **DP300.pub** and **DP300** are created and copy them to the local computer or server.

**----End**

## Importing the SSH Public Key

Import the SSH public key using the DP300 web interface.

**Step 1** Choose **System Settings** > **Installation**. The **Installation** page is displayed.

**Step 2** Click **Import SSH Public Key**. The **Import SSH Public Key** dialog box is displayed.

**Step 3** Click **Select File** and select the SSH public key **DP300.pub** from the local computer or server.

**Step 4** Click **Import**.

**Step 5** Click **Return** when **OK** is displayed.

**----End**

## Logging In Using the SSH Public Key

The following takes the SSH client SecureCRT as an example to describe how to log in to the DP300 using the SSH public key.

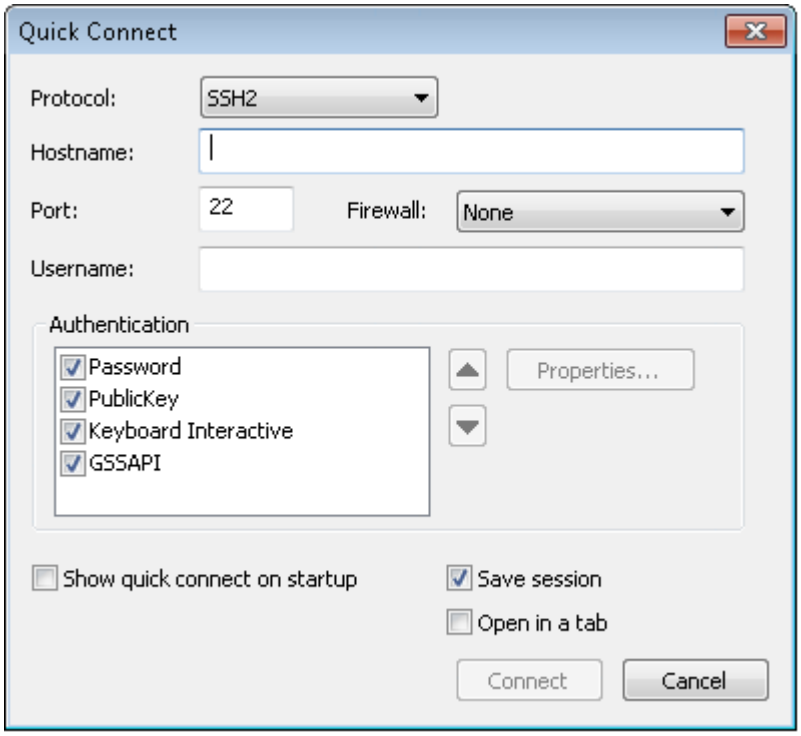
**NOTE**

SecureCRT is a login application for remote login across different platforms. It can be obtained from Huawei Unified Communications and Collaboration (UC&C) Security Center by Huawei technical support or downloaded from the Internet. Use SecureCRT 6.7.1 or a later version.

**Step 1** Run SecureCRT on your computer.

The SecureCRT quick connect dialog box is displayed, as shown in **Figure 2-3**.

**Figure 2-3** Initial Quick Connect dialog box




**Step 2** Select **SSH2** for **Protocol**.

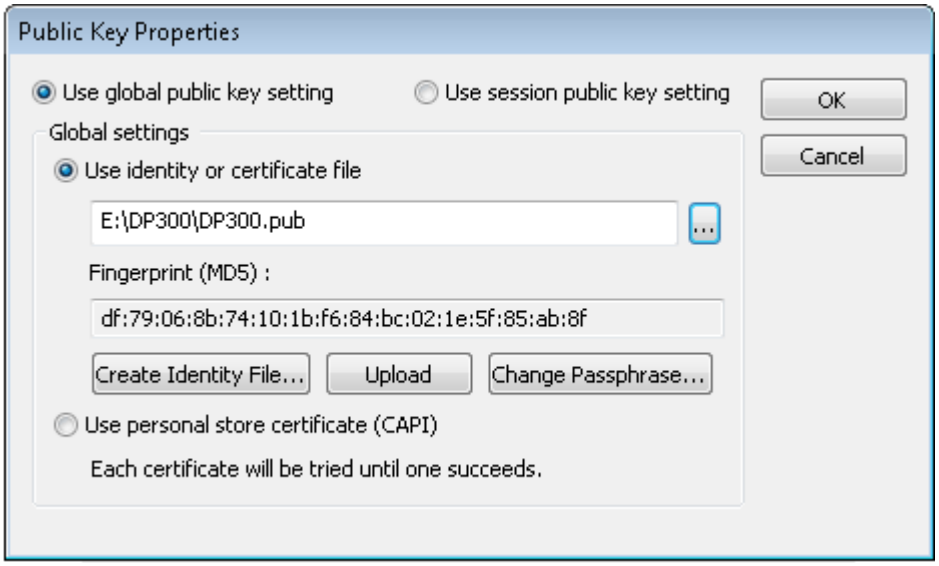
**Step 3** In **Hostname**, enter the IP address, such as **10.10.10.1**. Use the default value for **Port**.

**Step 4** In the **Authentication** area, select **PublicKey** only.

**Step 5** Click **PublicKey**, then click **Properties...**. The **Public Key Properties** dialog box is displayed.

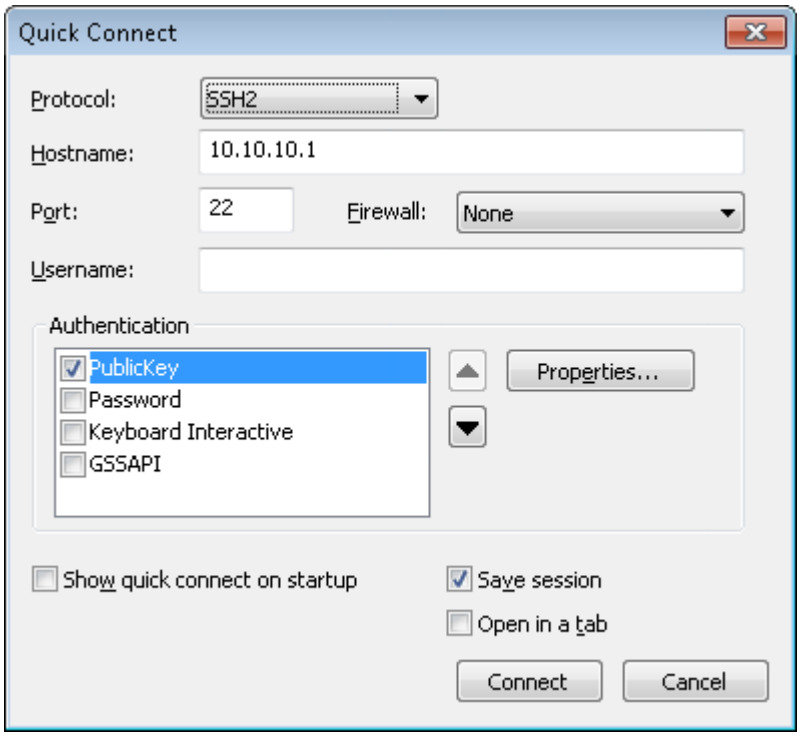
**Step 6** In the **Use identity or certificate file** text box, click **...** and select the SSH public key **DP300.pub**, as shown in **Figure 2-4**. (The **Use global public key setting** and **Use identity or certificate file** options are selected by default.)

**Figure 2-4** Selecting the SSH public key




**Step 7** Click **OK** to return to the **Quick Connect** dialog box, as shown in **Figure 2-5**.

**Figure 2-5** Quick Connect dialog box




**Step 8** In the **Username** text box, enter the SSH login account, for example, SSH administrator account **debug**.

**Step 9** Click **Connect**.

The login interface is displayed.

**Step 10** Run the commands.

For details, see the *HUAWEI DP300 Desktop Presence V500R002C00 Command Reference*.

**----End**

# 2.9 Viewing Logs

Logs record all non-query events during the DP300 running, such as non-query user operations and commands. These events can help you locate and rectify faults, as well as assist you in auditing.

- On the touchscreen, tap  and choose **Advanced** > **Diagnostics** > **Logs**.
- Select **Advanced** > **Diagnostics** > **Logs** on the remote control UI.
- Check logs on the web interface:
  1. Log in to the web interface and choose **Maintenance** > **Logs**.
  2. On the **Logs** page, click **Export**.
  3. Click **Save** in the displayed dialog box.
  4. Choose the folder to save the logs and click **Save**.
  5. Open the exported logs and check them.

# 2.10 Enabling FTPS

The DP300 supports File Transfer Protocol over SSL (FTPS) and File Transfer Protocol (FTP). To improve communication security, enable FTPS. If FTPS is disabled, the DP300 uses insecure FTP.

You can enable FTPS in one of the following ways:

- On the touchscreen, tap  and choose **Advanced** > **Settings** > **Network** > **Network Address Book** > **Network Address Book**, and select **FTPS**.
- On the remote controlled UI, choose **Advanced** > **Settings** > **Network** > **Network Address Book** > **Network Address Book**, and select **FTPS**.
- On the web interface, choose **System Settings** > **Network** > **Network Address Book**, and enable **FTPS**.
- Use commands to enable FTPS. For details, see the *HUAWEI DP300 Desktop Presence V500R002C00 Command Reference*.

# 2.11 Configuring an FTPS Server

FTPS is an extension of the commonly used FTP to support the SSL. The FTPS server ensures the security of the DP300 network address book.

**NOTE**

To configure the network address book after the FTPS client is configured, see the *HUAWEI DP300 Desktop Presence V500R002C00 Administrator Guide*.

Following uses the FileZilla server as an example to describe how to configure an FTPS server.

**Step 1** Set the IP address of the computer on which the FTPS server (for example, FileZilla server) is to be installed. Ensure that the IP addresses of the computer and DP300 are in the same network segment.

**Step 2** Run the FTPS server installer (for example, FileZilla_Server-0_9_41.exe) to install the FTPS server on the computer.

**Step 3** Double-click  to run the FTPS server. Click **OK** in the displayed dialog box, as shown in **Figure 2-6**.

**Figure 2-6** Connect to Server dialog box

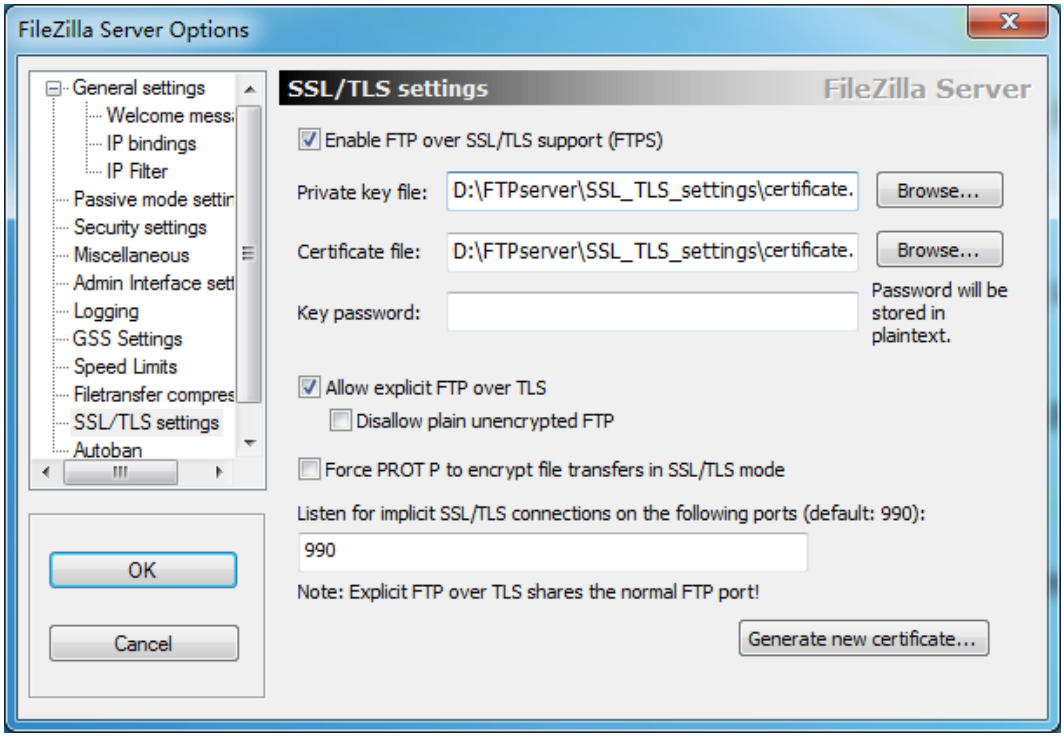

**Step 4** Choose **Edit** > **Settings**.

**Step 5** Click **SSL/TLS settings** in the left column and select **Enable FTP over SSL/TLS support (FTPS)**, click **Browse** to import the certificate, and click **OK**, as shown in **Figure 2-7**.

NOTE

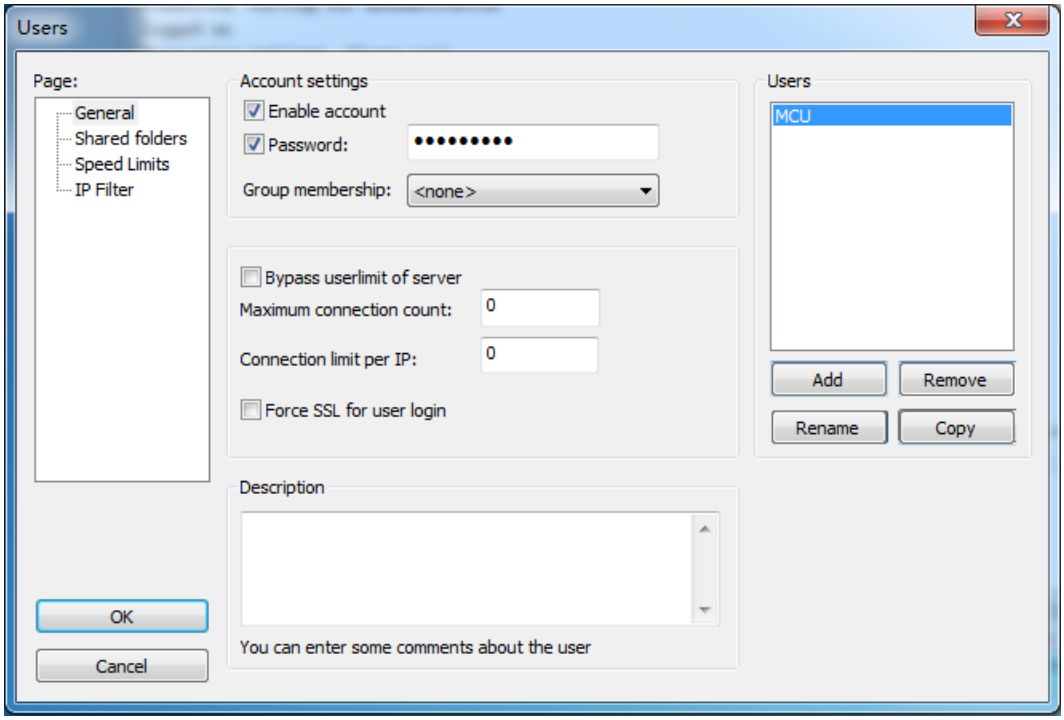
- Before importing a certificate, make sure it is issued by a security authority to prevent security risks.
- If no certificate is available, click **Generate new certificate**.

**Figure 2-7** FTPS Server Options dialog box




**Step 6** Choose **Edit** > **Users**. The Users dialog box is displayed, as shown in **Figure 2-8**.

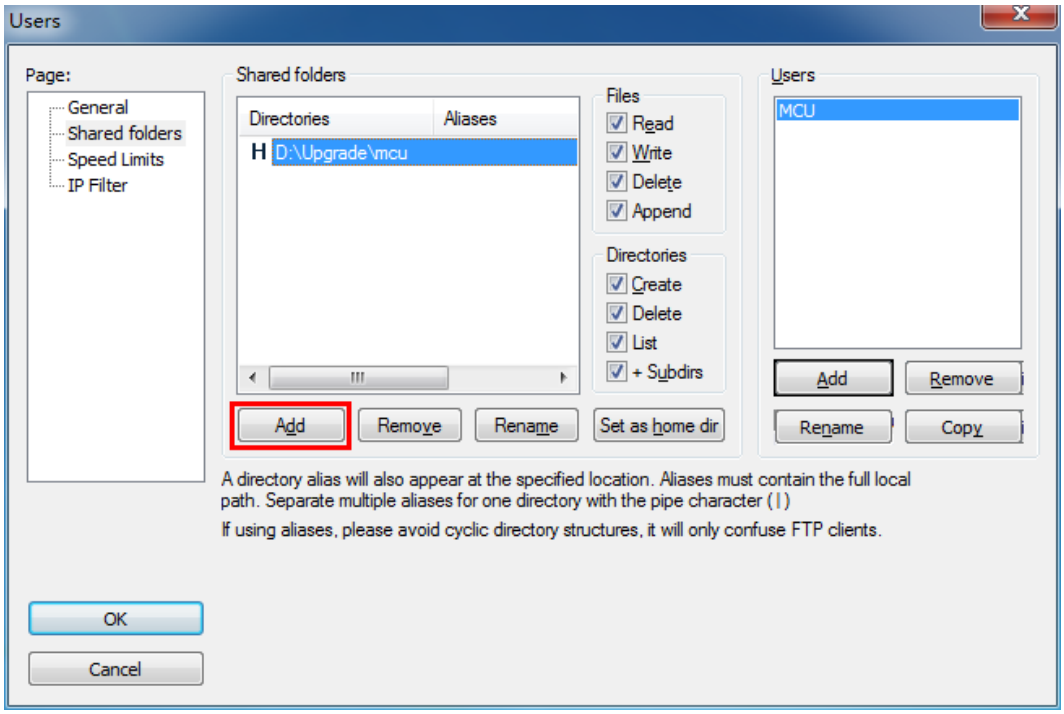
**Figure 2-8** Adding a user



**Step 7** Click **Add** to add a user. Select **Enable account** and **Password** and enter the **Password**.

**Step 8** Click **Shared folders** under **Page**, then click **Add**, and set the path for the user root directory of FTPS server, as shown in **Figure 2-9**.

**Figure 2-9** Specifying the path for the user root directory of FTPS server




**Step 9** Click **OK**.

**----End**

# 2.12 Video Monitoring

This function involves personal privacy. Ensure that its use complies with local laws and regulations.

To ensure conference security and protect conference privacy, this function is disabled by default and can be enabled on the touchscreen and remote controlled interface.

## 2.12.1 Enabling Video Monitoring

To enable video monitoring:

On the touchscreen, tap  and choose **Advanced** > **Settings** > **Security** > **Web Login** and then select **Monitor video**.

On the remote controlled UI, choose **Advanced** > **Settings** > **Security** > **Web Login** and select **Monitor video**.

## 2.12.2 Taking Picture

After the video monitoring and management function is enabled, you can capture and view local and remote videos and presentations on the web interface.

**Step 1** On the web interface, choose **Device Control** > **Device Control** > **Video Control**.

NOTE

After you access the **Video Monitor** page,  appears on the DP300 display screen to indicate that site monitoring is enabled.

**Step 2** Select the source you want capture of and click **Capture**.

**Step 3** In the displayed interface, select the picture and right-click it.

**Step 4** From the displayed shortcut menu, choose **Save Picture As** to save the picture.

**----End**

# 2.13 Upgrading Using the Mini System

If the DP300 cannot start as usual because the local upgrade fails due to power outage or other incidents, you can use the mini system for the upgrade instead.

You can use the mini system for upgrades whenever the DP300 software malfunctions. This method can be repeatedly used, and can ensure successful software upgrades when there are no hardware failures.

## 2.13.1 Preparing for the Upgrade

Before the upgrade, note the following prerequisites:

- Save the software package for upgrading on the computer.
- Connect the computer to the DP300 through a crossover cable or specifies the IP address of the computer and the DP300 in the same segment.
- Obtain the upgrade password. The upgrade password is **Change_Me** by default. For details, see section **2.2.6 Upgrade Password**.
- The default administrator user name and password of Telnet is **debug** and **Change_Me** respectively. If you forget the password, use the mini system to restore the DP300 to its default settings. For details, see section **2.3 Restoring Systems to Default Settings**.

## 2.13.2 Performing an Upgrade

**Step 1** While the DP300 is restarting or powering on, press and hold the **RESET** button for 10 seconds.

The DP300 enters the mini system.

NOTE

At this time, the DP300 has two IP addresses available: the static IP address of the normal system and the default IP address (192.168.1.1). If the connection setup using the normal system IP address fails or the DP300 IP address is dynamic and unknown, you can use the default IP address for the upgrade.

**Step 2** Use Telnet to log in to the DP300 and run **mnt upgswitch on** to enable the mini system upgrade function.

NOTE

By default, the mini system upgrade function is disabled.

**Step 3** Extract the compressed file of the upgrade software on the computer.

**Step 4** Run the upgrade program **UpgMaster.exe**.

The upgrade dialog box is displayed.

**Step 5** (Optional) Click **Browse**. Find and select the file in .dat format.

NOTE

By default, the path of the .dat file is displayed in Upgrade File.

**Step 6** In **Remote Teminal IP Address**, enter your DP300 IP address, for example, **192.168.1.1**. Then click **Upgrade**.

**Step 7** In the displayed dialog box, enter the upgrade password and click **OK**.

**Step 8** Restart the DP300.

**----End**

# 2.14 U-Boot Operations

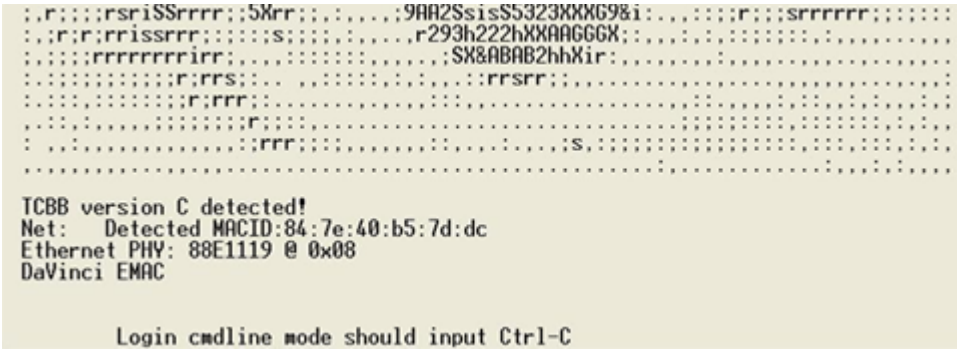
**Step 1** Use a serial cable to connect the serial port on the computer to the COM serial port on the DP300.

**Step 2** Start the serial port tool and set information such as the serial port number and baud rate.

Set the baud rate to **115200**.

**Step 3** Start the DP300. When the interface shown in **Figure 2-10** is displayed on the serial port tool, press **Ctrl+C** repeatedly until **Password:** is displayed.

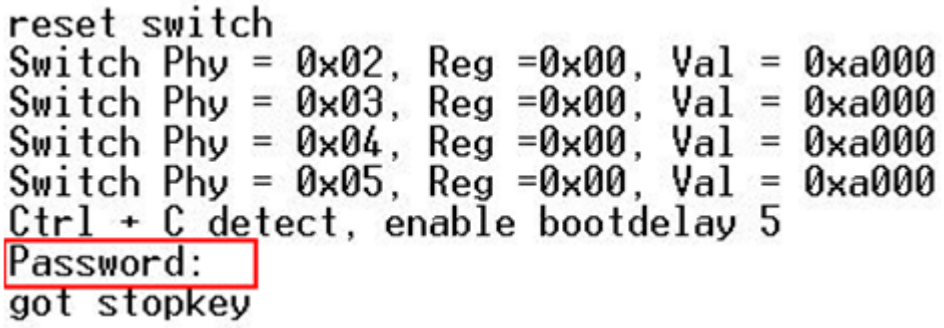
**Figure 2-10** Starting the system



**Step 4** Enter the password to the U-boot system as shown in **Figure 2-11**. The default password is **12345678**.

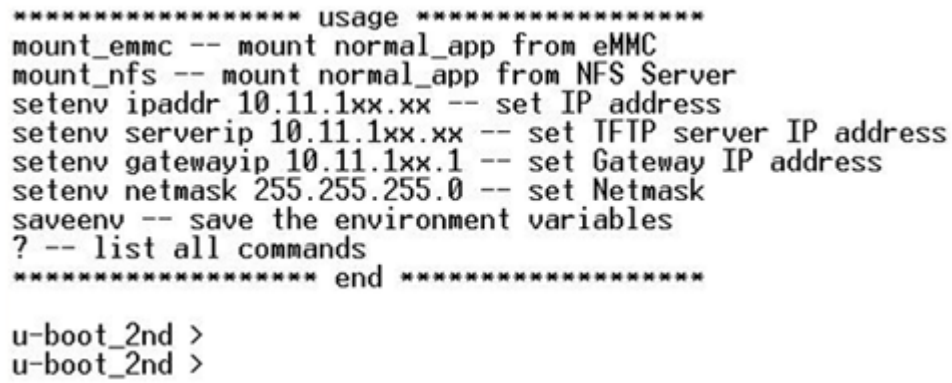
To improve device security, set a password at your first login and regularly change the password afterward. Use the **passwd** command to change the password. The new password must be a string of eight characters, consisting of digits, letters, and special characters.

**Figure 2-11** Enter password




**Step 5** Enter the command as show in **Figure 2-12**. For details, see the *HUAWEI DP300 Desktop Presence V500R002C00 Command Reference*.

**Figure 2-12** Enter command




**----End**

# 2.15 Verifying a Digital Signature

To prevent software packages from being maliciously corrupted or damaged during transmission and to protect the carrier's network security, verify software package integrity after obtaining the packages. Only verified software packages can be deployed.

### Background

Each software package corresponds to one digital signature file. A digital signature file is a **.asc** file named after a software package. For example, the digital signature file for the software package **HUAWEI-DP300.exe** is **HUAWEI-DP300.exe.asc**.

### Procedure

1. Obtain the verification tool package.

   Open **http://support.huawei.com/enterprise/toolsinfo?lang=en** to enter the **Tools and Resources** page.
2. Under **Tools and Resources**, choose **Tools software** > **Enterprises Common** > **Software digital signature (OpenPGP) validation tool** > **V100R001C00**.
3. Refer to the *OpenPGP Signature Validation Guide* to verify software package integrity.

## 2.16 Importing a Certificate

You can import client, server, SiteCall and 802.1x authentication certificates into your DP300 from the DP300 web interface. These certificates can be used to identify users, certificate authorities, and servers to improve communication security. For example, a client certificate is required when your DP300 registers with the SIP server using the Transport Layer Security (TLS) protocol.

**NOTICE**

Before importing a certificate, make sure it is issued by a security authority to prevent security risks.

**Step 1** Choose **System Settings** > **Installation**. The **Installation** page is displayed.

**Step 2** Click **Import Certificate**. The **Import Certificate** dialog box is displayed.

**Step 3** Click **Select File** to select the certificate you want to import.

**Step 4** Select the desired certificate type.

- To import a certificate for authentication calls and when the DP300 functions as the server, select **Server certificate**.
- To import a certificate for authentication registration or calls and when the DP300 functions as a client (for example, TLS-based registration), select **Client certificate**.
- To import a certificate used for SiteCall security, select **Multipoint conference certificate**.
- To import certificates used for 802.1x wired or wireless network authentication, select the desired certificates. When selecting the certificate type, choose the network type, which is **Wireless and wired** by default.

**Step 5** Click **Import**.

**Step 6** Click **Return** when **OK** is displayed.

**----End**

# 2.17 Importing Web Certificates

To help ensure communication security, import web certificates, including the trusted Certificate Authority (CA) file, local certificate file, local private key file, and local private key password file, to the DP300 through the DP300 web interface.

**NOTICE**

Professional guidance is required for importing certificates. Make sure the certificate to be imported matches the certificate type selected; otherwise, the may malfunction.

**Step 1** Choose **System Settings** > **Installation**.

The **Installation** page is displayed.

**Step 2** Click **Import Web Certificate**.

The **Import Web Certificate** dialog box is displayed.

**Step 3** Click and select a certificate type.

**Step 4** Click Select File, select the certificate you want to import, and click **Import**.

**Step 5** Click **Return** when **OK** is displayed.

After importing the web certificate, click **Update Web Certificates** and restart the DP300 as prompted for the web certificate to take effect.

**----End**

# 2.18 Importing and Exporting Settings

## Import and Export Settings on the Web Interface

You can import or export settings on the DP300 web interface to a configuration file. After your DP300 is restored to its default settings, you can import previously exported settings from the configuration file.

**NOTE**

Keep the configuration file safe to prevent disclosure of personal information.

**Step 1** Choose **System Settings** > **Installation**. The **Installation** page is displayed.

**Step 2** Click **Import/Export Settings**. The **Import/Export Settings** page is displayed.

**Step 3** Click **Import Settings** to import or **Export Settings** to export system settings.

The web administrator password is required when you import the configuration file. After the configuration file is imported successfully, the DP300 automatically restarts for the configuration file to take effect.

**----End**

## Import Settings on the USB Device

**NOTICE**

Use the USB device to import the configuration file only in videoconferencing mode.

**Step 1** Use the USB configuration tool to import the configuration file to a USB device.

**Step 2** Insert the USB device into the DP300's USB port.

**Step 3** Using the remote controlor on the touchscreen, enter the administrator password as prompted.

**NOTE**

When compressing the configuration file, set the password to the same as the administrator password; otherwise, the configuration file cannot be imported to your DP300. If the administrator password is empty, set the password to **123455678**, which is the default password for the administrator.

The DP300 restart automatically.

**Step 4** After the restart is complete, remove the USB device.

**----End**

# 3 System Layer Security

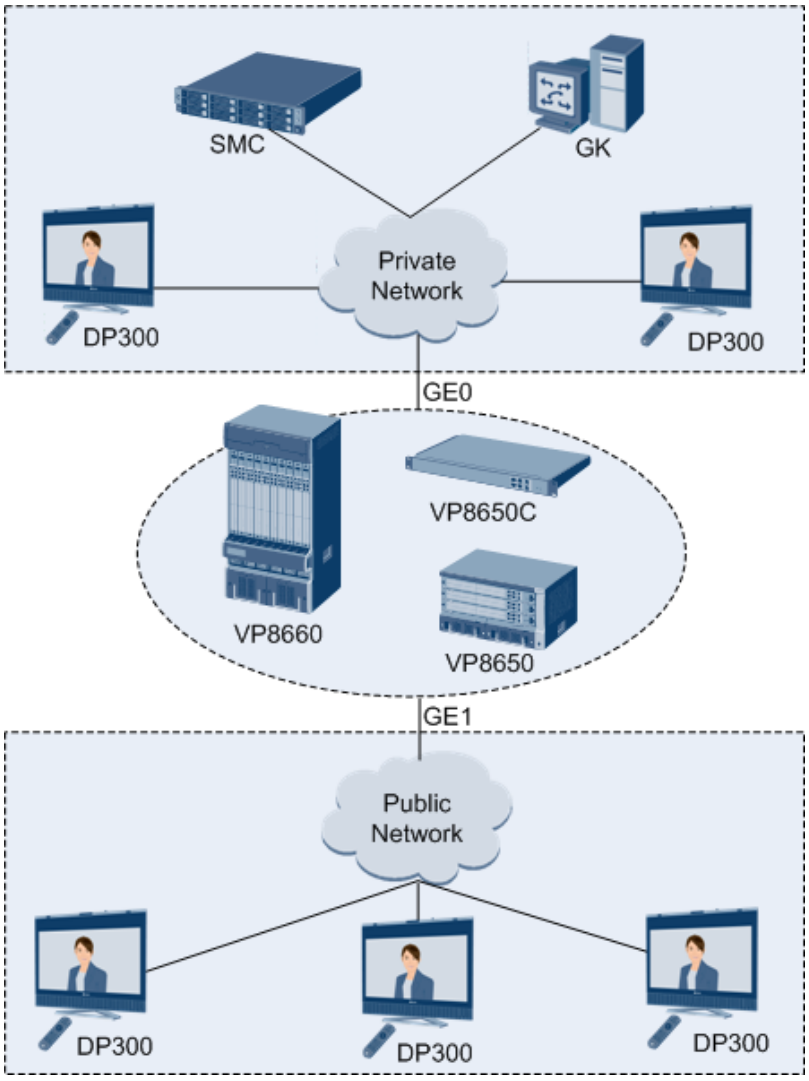
Security maintenance of the system layer is to ensure a smooth operation of the operating system, which can support the operation of application layer. The DP300 uses Linux, which is more secure and immune to viruses than Windows.

Patches are released regularly. To improve system security, it is recommended that users download latest patches at **http://e.huawei.com** regularly and apply them after performing antivirus checks.

# 4 Network Layer Security

Figure 4-1 show the DP300 security networking.

**Figure 4-1** DP300 security networking



Over the network:

The DP300 is connected to the Multipoint Control Unit (MCU) through the private network, which connects to different networks through different ports. The DP300s in the private or public network can join the conference even if you do not change H.323 protocol or the firewall settings (such as opening the port).

# 5 Management Layer Security

This chapter describes some management recommendations on users' daily security maintenance and can be referred to when users set the rules on security management.

# 5.1 Principles of System Security Maintenance

## 5.1.1 Account Management

- Manage the accounts strictly.
- Control the permissions of accounts of different levels. Only users of higher levels can change the passwords for users of lower levels.

## 5.1.2 Permission Management

- Minimize permissions to the system service and permissions of accounts.
- Strictly control the operation authorization on the web interface.

## 5.1.3 Auditing Principles

- Use logs and other feasible methods to monitor operations on the DP300.
- Audit the failed access to the system's important resources.
- Audit the successful access to the system's important resources.
- Audit the failed and successful access control strategy modification.

# 5.2 Guidelines for Password Security Maintenance

User identities must be authenticated before users can log in to application systems. The complexity and validity periods of accounts and passwords can be configured according to system security requirements. Guidelines for password security maintenance are as follows:

- Change the password periodically to prevent risks.
- Designate specialist personnel to manage the administrator account and password.
- Encrypt passwords during data transmission.
- Remind users to change their passwords after system deployment.
- Change passwords periodically. Do not use the default passwords or old passwords used last five times.

# 5.3 Logs Maintenance Recommendations

Use logs to identify suspicious activities. The system must record the operations, such as system parameter settings and conference calls in the logs. Reinforce the system to protect the logs.

## 5.3.1 Checking Logs Regularly

Check the system logs, applications logs, and security logs regularly and report to the department of a higher level once abnormal logs are found. Ask the local representative office for help if the issues cannot be located or resolved.

### 5.3.2 Backing Up Logs Regularly

Back up logs regularly by exporting them manually and store the logs on devices, such as the disc, tape, or compact disc. The system supports a maximum of 100,000 logs. Once the number of logs exceeds 100,000, new logs will replace the old ones. In this case, users must back up timely.

## 5.4 Guidelines on Signaling Diagnostics

You are obligated to take considerable measures, in compliance with the laws of the countries concerned and the user privacy policies of your company, to ensure that the personal data of users is fully protected. The signaling diagnostics on the DP300 may contain personal information. To protect information security, make sure that your account is secure and properly managed. Use the signaling diagnostics only for problem identification and delete them immediately after use.

## 5.5 Security Evaluation Recommendations

You are advised to look for a qualified organization to evaluate the system security and contact Huawei technical support engineers when problems occur during the evaluation.

## 5.6 Backup Recommendations

In the following scenarios, back up the logs to ensure security.

- Before daily security maintenance, and before and after the system troubleshooting.
- Before patch installation and DP300 upgrade. For details about the upgrade, see the *HUAWEI DP300 Desktop Presence V500R002C00 Administrator Guide*.

## 5.7 Defects Feedback Recommendations

You are advised to give feedback to Huawei once a security incident happens when the DP300 is used. Huawei will take the following actions accordingly.

- If a security incident happens, Huawei technical support engineers will support customers remotely or on site to reduce the impact on the system and improve the report on the accident treatment.
- If no security incident happens, Huawei technical support engineers record defects in to the database and send to the R&D team. Once the R&D team prescribes a solution, the technical support engineers will analyze the solution's possible impact on the site operations and provide a final solution.

# 5.8 Common Measures Against Attacks

- Deploy firewall devices on the network where the DP300 is located.
- Disable protocols that may impose attacks, such as Telnet and SSH. By default, Telnet and SSH are disabled. To check the settings of Telnet and SSH, choose **System Settings** > **Security** > **SSH/Telnet** on the DP300 web interface.
- If the DP300 is deployed on a public network, power off the DP300 when it is not in use.

# 5.9 Security Emergency Response Mechanism

Users need to build a security emergency response mechanism to ensure that the system can immediately respond to security issues and return to proper operations to minimize losses.

# 5.10 Security Emergency Response Email Address

Contact the Huawei Product Security Incident Response Team (PSIRT) via **PSIRT@huawei.com** if you wish to:

- Provide feedback on vulnerabilities of Huawei products.
- Obtain emergency response service from Huawei.
- Obtain information about vulnerabilities of Huawei products.

Encrypt the files that contain sensitive information before sending them. Go to **http://www.huawei.com/en/security/psirt/about-huawei-psirt/index.htm** to obtain the encryption key.

# A Appendix

The communication matrix is used for checking the firewall strategy. For details, see the *HUAWEI DP300 Desktop Presence V500R002C00 Communication Matrix*.

# B Default Settings

To better use your DP300, get to know the default values of common user names and passwords.

NOTE

To secure your account, it is recommended that you change the password upon the first login and regularly change the password afterwards.

**Table B-1** lists the default user names and passwords for the DP300.

**Table B-1** Default user names and passwords

| Item | Default Setting |
| --- | --- |
| Administrator Password for the Display | **12345678**. |
| Administrator password for the remote controlled UI | **12345678**. |
| Administrator user name and password for the DP300 web interface | The default user name and password are **admin** and **Change_Me** respectively. |
| User name and password for connecting the third party (for example, a touch panel or SMC2.0) to the DP300 | The default user name and password are **api** and **Change_Me** respectively. |
| Upgrade password | **Change_Me**. |
| Air content sharing password | **Change_Me**. |

| Item | | Default Setting |
| --- | --- | --- |
| User name and password for logging in to the DP300 in SSH/ Telnet mode | | ● Debug user: The default user name and password are **debug** and **Change_Me** respectively.<br>● Common user: The default user name and password are **admin** and **Change_Me** respectively.<br>● Common user: The default user name and password are **user** and **Change_Me** respectively.<br>● Special user: The default user name and password are **apiuser** and **Change_Me** respectively.<br>● Test user: The default user name and password are **test** and **Change_Me** respectively. |
| User name and password for connecting the DP300 to a web-based diagnostics tool | | The default user name and password are **admin** and **Change_Me** respectively. |
| User name and password for logging in to the DP300 in serial port mode | | The default user name and password are **root** and **Change_Me** respectively. |
| U-Boot password | | **12345678**. |
| Default IP address after the DP300 is restored to its default settings | | **192.168.1.1**. |
| Information required for the network management system to connect to the DP300 through SNMP V2 | Get community name | **Change_Public**. |
| | Set community name | **Change_Private**. |
| | Trap community name | **Change_Me**. |
| Account, password, and protocol required for the network management system to connect to the DP300 through SNMP V3 | User name | **v3user**. |
| | Authentication protocol | **SHA**. |
| | Authentication password | **Change_Me**. |
| | Encryption protocol | **AES**. |
| | Encryption password | **Change_Me**. |