Cloud Phone

FAQs

Issue 07

Date 2021-09-30

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.

Contents

1 Consulting

1.1 What Are the Advantages of HUAWEI CLOUD Cloud Phone Compared with Other Similar Solutions?

Common mobile phone simulation solutions in the market include the x86 emulator solution and mobile phone solution. **Table 1-1** lists the advantages and disadvantages of the three solutions.

Table 1-1 Comparison between Cloud Phone and other mobile phone simulation solutions

Dimension	x86 Emulator	Physical Phone	Cloud Phone of HUAWEI CLOUD
Performance	Poor Conversion between x86 and ARM instruction sets is required, resulting in low efficiency and at least 50% performance loss.	Medium Cannot exceed the performance of a mobile phone.	High Cloud Phone is based on ARM servers and offers various performance and storage specifications. It is far more powerful than physical mobile phones.

Dimension	x86 Emulator	Physical Phone	Cloud Phone of HUAWEI CLOUD
Compatibility	Poor Complex x86 instructions are not converted into simplified ARM instructions in one-to-one mode, causing severe application compatibility issues. These issues persist for a long time and are difficult to resolve.	High Same as mobile phones, ensuring application compatibility.	High High compatibility of ARM-based native applications
Stability	Medium The stability is hard to ensure because it is implemented based on various external open-source or non-commercial simulator software.	Extremely poor A large number of second-hand mobile phones are non-server products. In addition, manual soldering points and complex cable connections cannot ensure product quality and stability.	High Huawei-developed high-performance ARM chips and ARM servers have been widely used in the market, providing high stability and reliability.
Availability	High x86 servers and emulator software are used to build the system, which has low requirements and high resource availability.	Extremely poor It is very difficult to obtain sufficient and stable sources of mobile phones. The second-hand mobile phone market is changing rapidly, and the availability of the target mobile phones in the market is extremely poor.	High The product is provided as a cloud service, which features large volume, flexible usage, and high elasticity of resources. The resources can be charged by month.

Dimension	x86 Emulator	Physical Phone	Cloud Phone of HUAWEI CLOUD
Simulation	Poor Based on the software upper-layer technology, although many mobile phone parameters can be modified, the features are obvious, and the x86 emulator is easily detected by the upper-layer application as a simulator.	High Exactly mobile phone used.	High Fully simulate Huawei mobile phones. If the cost-effective AOSP mode is used, underlying hardware data can be simulated for applications.
Specifications Flexibility	High Specifications can be set flexibly.	Poor Devices are purchased based on the set specifications, which are not flexible.	High The specifications can be flexibly set and adjusted, and high-specification overcommitment instances can be easily implemented.

1.2 Does Cloud Phone Support iOS?

- If you are asking whether the iOS system can be installed on your cloud phone, the answer is no. Currently, only the open-source Google AOSP version is supported. Other mobile phone systems are not supported due to commercial authorization.
- If you are asking whether you can access your cloud phone through the iOS system, the answer is yes. You can access your cloud phone using any system.

1.3 Is There Cloud Phone Root Permission?

Yes, there is Cloud Phone root permission by default. That is, you can obtain the highest permission of your cloud phones.

1.4 Does Each Cloud Phone Has an Independent Public IP Address?

No.

A public IP address is bound to the server, and all cloud phones virtualized from the server share the same public IP address.

Each cloud phone has an independent private IP address.

1.5 Can I Change the IP Address of My Cloud Phone?

Sorry, no.

The EIP and private IP address of the cloud phone are randomly allocated during the cloud phone purchase and cannot be changed.

1.6 How Is Cloud Phone Charged?

Billing Items

Figure 1-1 shows the Cloud Phone billing items.

Figure 1-1 Billing items

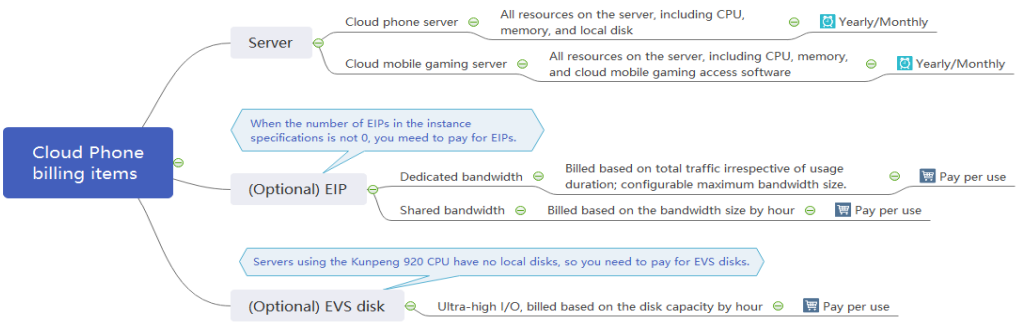


Table 1-2 Billing items

Billing Item	Description	Example	Billing Mode
Server	You obtain cloud phones only after purchasing a server. You pay for all resources on the server. • Server for general-purpose cloud phones: CPU, memory, and local disk • Server for gaming cloud phones: CPU, memory, local disk, and cloud mobile gaming access software	Server for general-purpose cloud phones • physical.rx1.xlarge: ¥5950 CNY/month • physical.kg1.4xlarge.cp: ¥10,700 CNY/month Server for gaming cloud phones • physical.rx1.xlarge.cg: ¥6600 CNY/month • physical.kg1.4xlarge.cg: ¥11,500 CNY/month	Yearly/Monthly
(Optional) EIP	If the number of EIPs is not 0 in the instance specifications, pay for the EIP traffic or bandwidth. The billing standard varies depending on the bandwidth type. • Dedicated bandwidth: billed based on total traffic irrespective of usage duration; configurable maximum bandwidth size • Shared bandwidth: billed based on the bandwidth size by hour For details, see **Price Calculator**.	Take CN East-Shanghai1 as an example. The billing standard of the shared bandwidth is ¥0.167/hour/Mbit/s. If you purchase a 50 Mbit/s bandwidth, you need to pay the following fees: 0.167 x 50 = 8.35 (CNY/hour)	Pay per use

Billing Item	Description	Example	Billing Mode
(Optional) EVS disk	**physical.kg1.4xlarge.cp** and **physical.kg1.4xlarge.cg** servers do not have local disks. By default, the system purchases one or more ultra-high I/O EVS disks that will be billed based on the disk capacity by hour. For details, see **Price Calculator**.	Take CN East-Shanghai1 as an example. The billing standard of ultra-high I/O EVS disks is ¥0.0014/hour/GB. Therefore, if you purchase a physical.kg1.4xlarge.cp server, you need to pay the following fees: 0.0014 x 400 x 3 = 1.68 (CNY/hour) 400 indicates the EVS disk capacity. 3 indicates the number of EVS disks.	Pay per use

Billing Mode

The Cloud Phone servers are billed in yearly/monthly mode and do not support the pay-per-use mode. If you want to use Cloud Phone for a long time, purchase them by year to save more.

1.7 What Are the Specifications of Cloud Phones That Support VNC Login?

Only rx1.cp.c60.d32.e1v1.qemu supports VNC login.

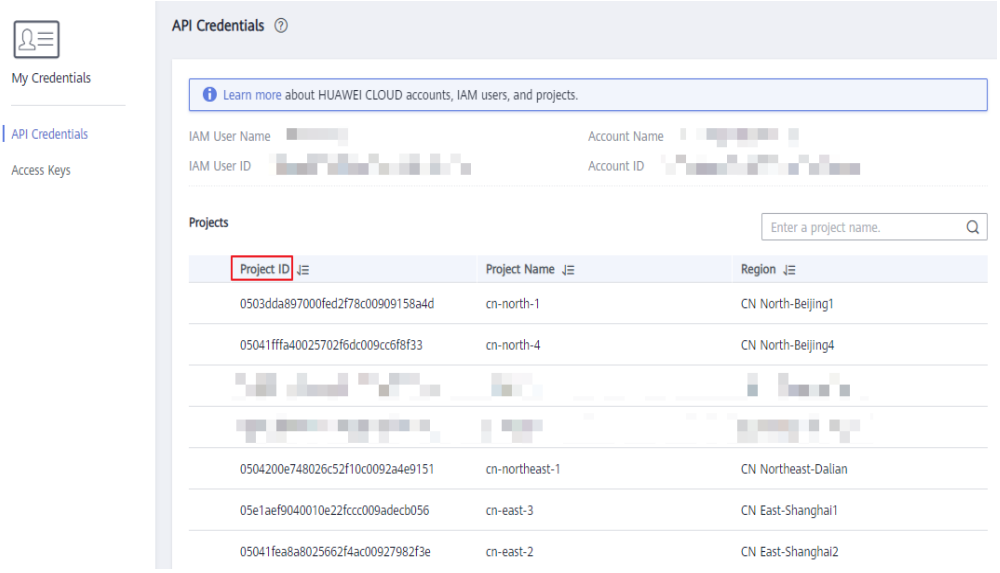
The current cloud phone supports VNC login if

- In the cloud phone list, the **Remote Login** button in the **Operation** column is not dimmed.
- On the cloud phone details page, the VNC port is displayed in the **Application Port** area except the ADB port.

1.8 How Do I Obtain the Project ID?

1. Log in to the management console.
2. Locate the username in the upper right corner, hover the mouse over it, and select **My Credentials** from the drop-down list.
3. In the **Projects** area, obtain the project ID of each region.

Figure 1-2 Project ID



1.9 How Do I Install Apps on a Cloud Phone?

Description

A cloud phone does not have a built-in browser or app store. If you want to install an app on a cloud phone, find an app APK and run the ADB command to upload the package to the cloud phone.

Handling Method

1. Connect ADB to the cloud phone.

   For details, see **Access Methods**.

2. Save the APK of the app to be installed to the local device directory.
3. Run the following command to install the app APK on the cloud phone SD card:

   adb -s 127.0.0.1:*Local idle port* **install** *APK path*

   Example: **adb -s 127.0.0.1:1234 install C:\Users\Administrator\Downloads\QQliulanqi_9515115.apk**

If **Success** is displayed, the installation is successful.

CAUTION

If an error is reported during the command execution, check whether Airtest is started. Airtest must be stopped during the ADB command execution.

1.10 How Long Does It Take to Activate a Server After I Purchase It?

Generally, it takes about 30 minutes.

If the server is not activated for a long time, contact customer service for technical support.

1.11 What Should I Do If I Can't Find My Server on the Cloud Phone Console?

Symptom

I have purchased a server successfully but could not find it on the Cloud Phone console.

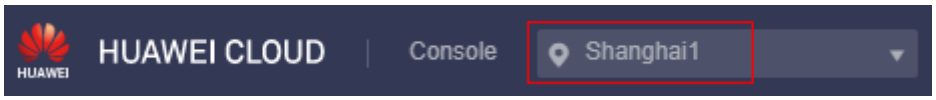
Possible Causes

Your server is not in the selected region or project.

Handling Method

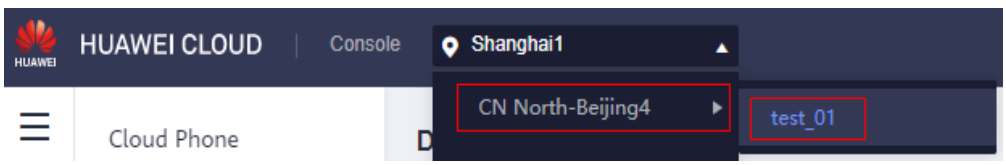
1. Log in to the **Cloud Phone console**.
2. In the upper left corner, select the region where your server locates. Then, your resources are displayed.

Figure 1-3 Switching a region



If your server is purchased under a sub project in a region, switch to the sub project to view your server.

Figure 1-4 Switching a project



1.12 How Long Will Resources Be Released After My Server Expires?

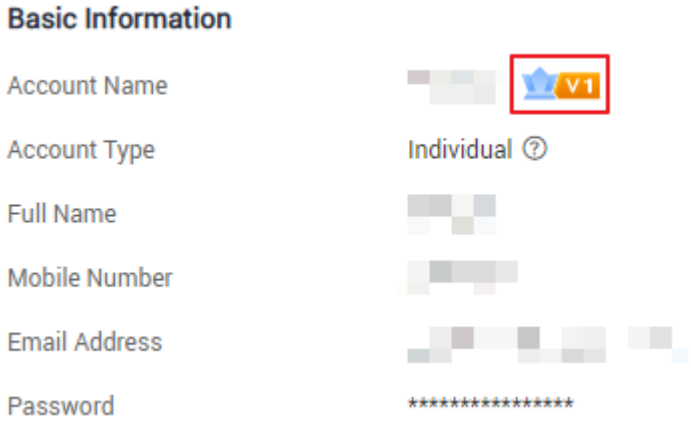
If you do not renew a yearly/monthly server timely after it expires, HUAWEI CLOUD provides a retention period.

The retention period depends on your level. For details, see **Grace Period and Retention Period**.

NOTE

To view your level, log in to the management console, click the username in the upper right corner, click **Basic Information**, and view the level next to the account name.

Figure 1-5 Basic Information



1.13 What Can I Do If the Private Key File Is Lost?

Description

If the private key file is lost, you need to replace the key pair with a new one and use the new private key file to access the cloud phone.

Handling Method

The following describes how to replace the key pair. Ensure that you have created a key pair on the ECS console and downloaded the private key file of the key pair to your local PC.

1. Log in to the management console.
2. On the **Service List** page, choose **Computing** > **Cloud Phone**.

   The Cloud Phone console is displayed.
3. In the navigation pane on the left, choose **Servers**.
4. Locate the target server and choose **More** > **Change Key Pair** in the **Operation** column.
5. On the displayed **Change Key Pair** dialog box, select a new key pair and click **OK**.

   Wait a few minutes for the new key pair to take effect.

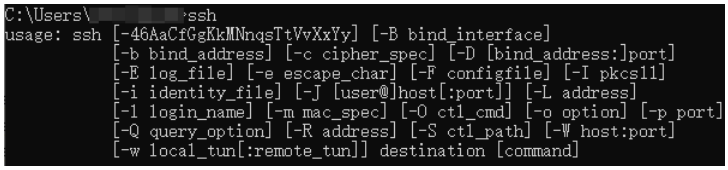
1.14 How Can I Know Whether the SSH Service Has Been Installed on My Local Device?

1. Open the CLI on your local device. The following uses Windows 10 as an example:

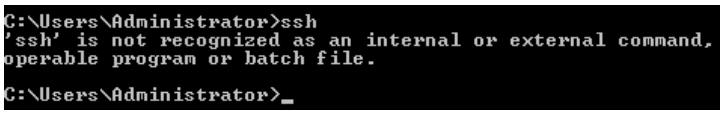
   Press **Win+R**, enter **cmd** in the **Run** dialog box, and press **Enter**.

2. Enter the **ssh** command and press **Enter**.

   - If no error is reported and the following information is displayed, SSH is installed on the system.

   - If the following error message is displayed, download an SSH, such as OpenSSH.

     Download SSH from **https://www.mls-software.com/files/setupssh-8.1p1-1.exe**.

     Install the SSH software. Run the **ssh** command. If the error persists, restart the local device and try again.

1.15 Common ADB Commands

This section describes common ADB commands.

Basic Operations

- Install an app.
  adb install -r *xxx*.**apk** //Reinstall the existing application and retain its data and cached files.
  adb install -s *xxx*.**apk** //Install the APK to the SD card.
  adb install -f *xxx*.**apk** //Install the APK to the internal system memory.
- Obtain the installation position.
  adb shell pm get-install-location
- Uninstall an app.
  adb uninstall *<package>*
  adb uninstall -k <*package***>** //Uninstall the app but retain its data and cached files.
- Start ADB.
  adb start-server
- Stop ADB.
  adb kill-server
- Go to the shell environment.
  adb shell
- Exit from the shell environment.
  exit

Checking Device Information

- Check the connected device and its serial number.
  adb devices
- Check the CPU architecture and number of cores of a cloud phone.
  adb shell cat /proc/cpuinfo
- Check detailed system memory information.
  adb shell cat /proc/meminfo
- Obtain the disk space of a cloud phone.
  adb shell df
- Obtain the OS version of a cloud phone.
  adb shell getprop ro.build.version.release
- Obtain the MAC address of a cloud phone.
  adb shell cat /sys/class/net/wlan0/address

Software Package Manager

- Clear all data associated with an application.
  adb shell pm clear <package>
- View the APK path of a specified application.
  adb shell pm path <package>
- Check the package names of all installed applications.
  adb shell pm list packages
- Check the application package whose name contains the "android" field.
  adb shell pm list packages android
- Check the package name of a third-party application.
  adb shell pm list packages -3

Checking Processes

- Check the memory usage of each process.
  adb shell procrank
- Check the process information about an application.
  adb shell "ps | grep <package>**"**
- Stop a process.
  adb shell kill [pid]

File Operations

- Send a file from a local device to a cloud phone.
  adb push file mobile_directory

  Example:

  Send file **C:/Downloads/test.png /data/media/0/Pictures** on the local device to the cloud phone directory **/data/media/0/Pictures** by running the following command: **adb push C:/Downloads/test.png /data/media/0/Pictures**. To check whether the file is sent successfully, run the following commands:

  ```
  adb shell
  cd /sdcard/Download
  ls
  ```

- Copy a file from a cloud phone to a local device.
  adb pull file local_computer_directory

  Example:

Copy file **/sdcard/Download/test.png** on a cloud phone to the **C:/Downloads** directory on a local device by running the following command: **adb pull /sdcard/Download/test.png C:/Downloads**.

- Move a file or folder.
  adb shell mv path/file newpath/file
- Create a folder.
  adb shell mkdir path
- Create a file.
  adb shell touch filename
- Rename a file or folder.
  adb shell rename path/filename newpath/newfilename
- Check the file content.
  adb shell cat file

1.16 Does the Cloud Phone Support Cameras?

No. Due to the compliance requirements, cloud phones do not support the functions such as SIM card, mobile phone number, SMS, and camera.

1.17 Does the Cloud Phone Support Facial Recognition?

No. The cloud phone does not support the camera function. Therefore, facial recognition cannot be performed.

1.18 What Are the Security Group Authorization Rules for Cloud Phones Using Custom Networks?

If you set **Network** to **Custom** when you create a cloud phone server, a **cph_admin_trust** agency will be created for you. This agency has the **VPC FullAccess** permission.

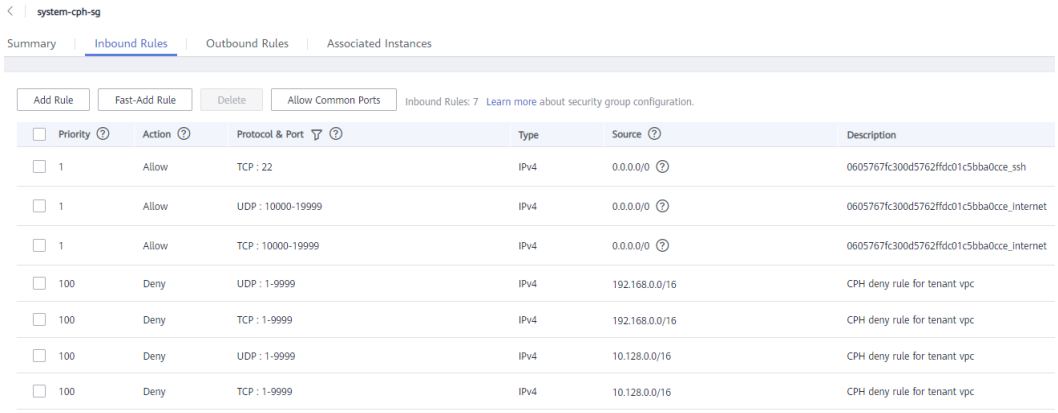
NOTE

To authorize the Cloud Phone service to create an agency for you, ensure that your login user has the **Security Administrator** permission or the fine-grained permission **iam:agencies:createAgency** for creating agencies. For more information, see **Permission Management**.

The Cloud Phone service will use the agency to perform the following operations:

- Create an elastic NIC, EIP, and virtual IP address for a general-purpose or gaming cloud phone.
- Create a security group named **system-cph-sg** for a cloud phone and gaming phone server, and set the port or port range based on **Figure 1-6** and **Figure 1-7**.

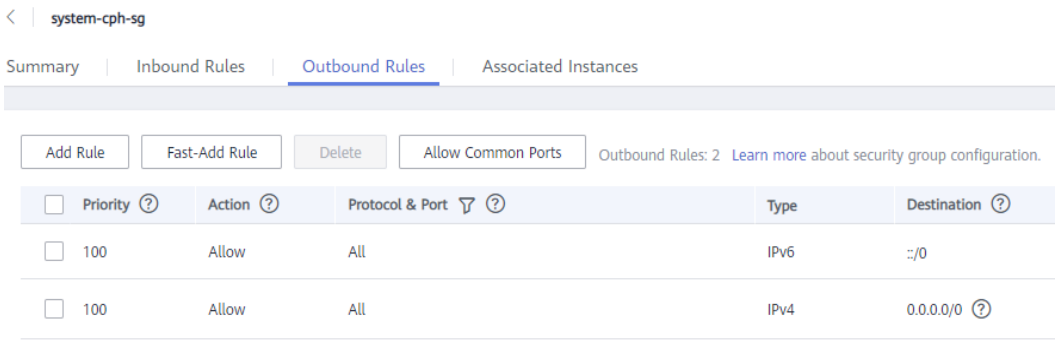
Figure 1-6 Inbound rule



NOTE

- Port 22 is used by the Internet to connect to the cloud phone using ADB and through the SSH encryption tunnel.
- Ports 10000 to 19000 are mapped to the available application ports of each general-purpose or gaming cloud phone. You can view the available application ports on each cloud phone in the cloud phone details.
- The **CPH deny rule for tenant vpc** rule is used to restrict the cloud phones virtualized the servers in the same VPC so that the phones cannot access each other through ports 1 to 9999.

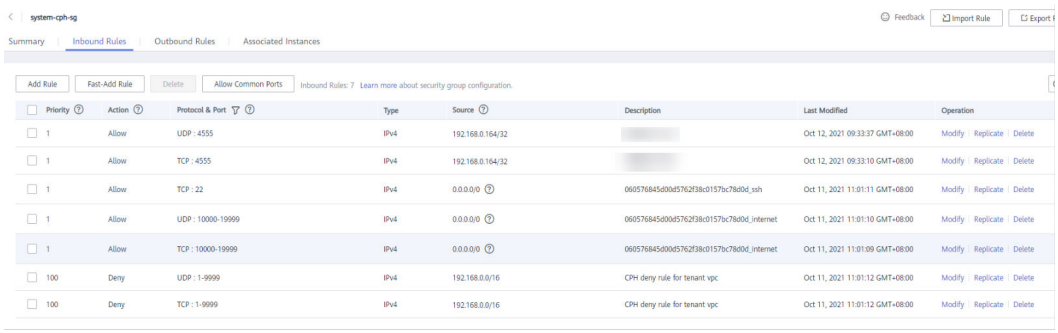
Figure 1-7 Outbound rule



By default, if an ECS and cloud phone are in the same VPC, the ECS cannot access the cloud phone through ports 1 to 9999. If you want to allow such access, add a security group rule with a higher priority. For example, if the IP address of an ECS is 192.168.0.164 and you want to access a cloud phone through port 4555, add the following inbound rule:

- **Priority**: Set it to **1**.
- **Action**: Select **Allow**.
- **Protocol & Port**: Set the port to **4555**.
- **Source**: Enter **192.168.0.164**.

Figure 1-8 Adding a security group rule of a higher priority



2 SSH Tunnel Faults

2.1 What Can I Do If the SSH Tunnel Fails to Be Established When I Access the Cloud Phone over the Public Network?

If the SSH tunnel fails to be established, check whether parameters in the following commands are correct.

ssh -L *Local idle port:Cloud phone listening IP address: Cloud phone listening port SSH tunnel username@Public IP address* **-i** *Private key file path* **-Nf**

- Check whether the local idle port is occupied.
- Ensure that you obtain the cloud phone listening port instead of the server listening port.
- Check whether the SSH tunnel username is the project ID. For details, see **How Do I Obtain the Project ID?**.
- Create a new key pair. On the **Servers** page, change the key pair of the server where the cloud phone is located. Wait for 1 to 2 minutes until the new key pair takes effect, and use the new private key file path to run the command again.

2.2 What Does Message "Authorized users only. All activities may be monitored and reported." Indicate?

It indicates that your SSH tunnel is successfully established.

Figure 2-1 Prompt for successful establishment of the SSH tunnel

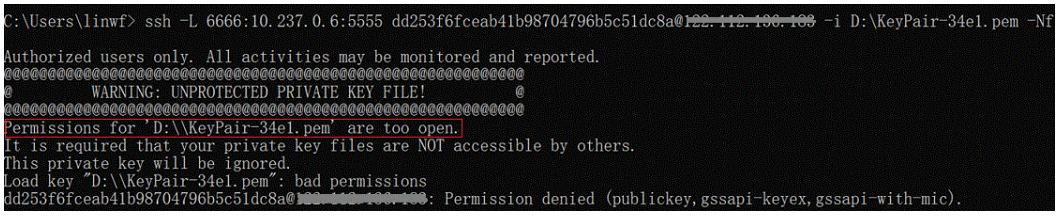
If your SSH tunnel fails to be established, messages like "Permission denied" and "Connection closed" are displayed below this prompt.

2.3 What Can I Do If Message "too open" Is Displayed When I Am Establishing the SSH Tunnel?

Description

Error message "too open" is displayed during the SSH tunnel establishment.

Figure 2-2 too open



Causes

The permission of the user's private key file is excessive. Therefore, the SSH tunnel establishment request is rejected.

Handling Method

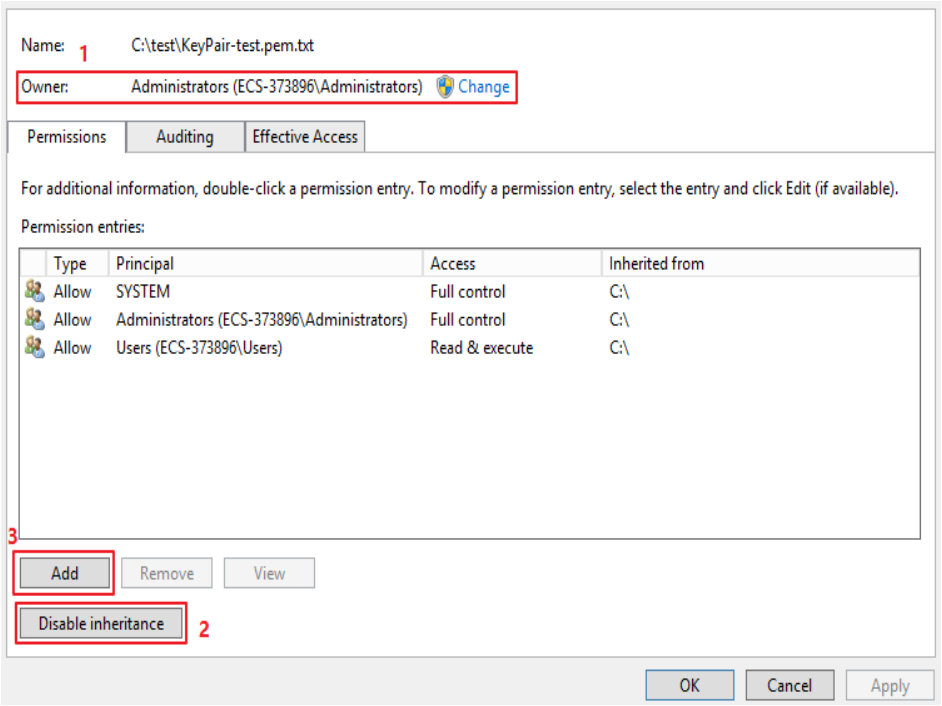
Change the permission on the private key file.

- If your local device runs the Linux OS, run the **chmod 600** *KeyPair-test.pem* command.
- If your local device runs the Windows OS, perform the following operations (Windows 10 is used as an example):
  a. Right-click the private key file saved on the local device and choose **Properties** from the shortcut menu.

     The **KeyPair-test.pem Properties** dialog box is displayed.
  b. Click the **Security** tab and click **Advanced** in the lower right corner.

     The **Advanced Security Settings for KeyPair-test.pem** dialog box is displayed.
  c. Perform the following operations in sequence:

Figure 2-3 Security settings



a. Check whether the owner is your username. If no, click **Change** to change it.

You can run the **whoami** command in the cmd window to view the username.

b. Click **Disable inheritance**. In the displayed dialog box, select **Remove all inherited permissions from this object**.

c. Click **Add**. In the displayed **Permission Entry for KeyPair-test.pem** dialog box, click **Select a principal**, enter your username, and click **OK**.

Ensure that the permission item contains only your own username, and then click **OK**.

d. Go back to the **KeyPair-test.pem Properties** dialog box, and click **OK**.

NOTE

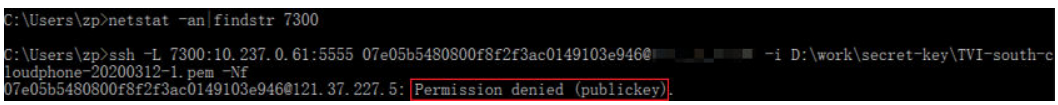
KeyPair-test.pem is the private key file name. Replace it with the actual name.

2.4 What Can I Do If Message "Permission denied" Is Displayed When I Am Establishing the SSH Tunnel?

Description

Message "Permission denied" is displayed during the SSH tunnel establishment.

Figure 2-4 Permission denied



Handling Method

1. Check whether the SSH tunnel username (project ID) in the command for establishing the SSH tunnel matches the region where the cloud phone is located.

   ssh -L *Local idle port:Cloud phone listening IP address SSH tunnel username@Public IP address* **-i** *Private key file path* **-Nf**

   If the fault persists, go to **2**.

2. Check whether the cases of **-L**, **-i**, and **-Nf** in the command to establish the SSH tunnel are correct.

   If the fault persists, go to **3**.

3. Check whether the permissions of the private key file are correctly configured by referring to **What Can I Do If Message "too open" Is Displayed When I Am Establishing the SSH Tunnel?**.

   If the fault persists, go to **4**.

4. Change the local idle port for establishing the SSH tunnel.

   If the problem persists, **create a service ticket**.

2.5 What Can I Do If Message "no match mac found" Is Displayed When I Am Establishing the SSH Tunnel?

Description

When you use the Mac OS to access a cloud phone, "Permission denied" is reported during the SSH tunnel establishment. The details are as follows:

```
no match mac found: client hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh...
```

Causes

OpenSSH programs of multiple versions are downloaded or the downloaded OpenSSH is incompatible. This problem seldom occurs in the scenario where the system itself provides the SSH.

Handling Method

Choose **Control Panel** > **Programs** > **Uninstall a program**, click any OpenSSH program, and press **Option** to view the number of downloaded OpenSSH programs.

- If there are multiple programs, uninstall them and retain the 8.1p1 version.
- If there is only one program, version 8.1p1 is recommended.

NOTE

Download OpenSSH 8.1p1 from **https://www.mls-software.com/files/setupssh-8.1p1-1.exe**.

2.6 How Do I Keep an SSH Session Uninterrupted?

Description

If you do not perform any operation for a long time when accessing a cloud phone, the SSH session may time out and exit. If you have accessed the cloud phone through ADB, you cannot run **adb shell** commands after exiting due to timeout.

Handling Method

Add **-o ServerAliveInterval=30** to the command for setting up an SSH tunnel. The complete command is as follows:

ssh -L *Local idle port:Cloud phone listening IP address: SSH tunnel username@Public IP address* **-i** *Private key file path* **-o ServerAliveInterval=30 -Nf**

ServerAliveInterval=30 indicates that the local SSH client sends the keep-alive packet to the SSHD server every 30 seconds to maintain the session.

2.7 What Can I Do If I Failed to Establish an SSH Tunnel?

If the SSH tunnel fails to be established or the cloud phone status is displayed as **offline** in the **adb devices** command output, the cloud phone fails to be connected. In this case, run the **adb connect** command to re-establish the connection. If the connection still fails to be established, perform the following operations:

- Check whether the private key file of the server is correct.
- Go to the Cloud Phone console to check whether the cloud phone is running.
- Reconfigure mandatory fields in the **config.json** file and re-establish the SSH tunnel.

2.8 What Can I Do If an Error Occurs When I Invoke the Cloud Phone Query API?

If the API fails to be invoked, the necessary information for establishing the tunnel cannot be obtained, so the cloud phone cannot be connected. The following is an example of the error message:

```
unable to connect to xxxx:xxxx: An error occurred when calling the Cloud Phone API for querying the ADB access info, check adb.tunnel.log file for more details.
```

Run the **adb connect** command to re-establish the connection. If the error persists, view the **adb.tunnel.log** file in the ADB installation directory to obtain further information. Generally, check whether the following information is correct:

- AK/SK in the configuration file, and server region

- Server EIP and listening port

3 ADB Connection Faults

3.1 What Can I Do If Message "unable to connect to :5555" Is Displayed When I Am Using ADB to Access a Cloud Phone?

Description

After successful establishment of the SSH channel, I ran the ADB command to access a cloud phone, and message "unable to connect to :5555" is displayed.

Figure 3-1 unable to connect to :5555

Causes

The ADB is connected to the cloud phone over USB instead of over Wi-Fi.

Handling Method

Run the **adb tcpip** *Local idle port* command in the CLI, and then run the **adb connect 127.0.0.1:** *Local idle port* command to reconnect to the cloud phone.

3.2 What Can I Do If the ADB Connection Is Interrupted Suddenly?

Description

The ADB connection is interrupted unexpectedly, and no connected device is displayed after the **adb devices** command is executed.

Causes

The network of the local physical device is intermittently disconnected or ADB is faulty.

Handling Method

Restart ADB. The procedure is as follows:

1. Stop ADB.

   adb kill-server
2. Start ADB.

   adb start-server
3. Reconnect to ADB.

   adb connect 127.0.0.1:*Local idle port*

3.3 What Can I Do If an ADB Connection Error Occurs?

Cloud Phone ADB integrates the SSH tunnel service. A normal SSH tunnel is required for successful connections to cloud phones. You can run the **adb kill-server** and **adb start-server** commands to restart ADB and the SSH tunnel. In addition, check whether paths of ADB of other versions exist in the system environment variable *PATH*. If yes, remove ADB of other versions.

Other common configuration errors are as follows:

- **Error: Error file config.json doesn't exist, should in the same path as adb.**

  The **config.json** file and ADB installation package must be under the same directory.
- **Error: Error key pair file C:\Users\Administrator\Desktop\adb\keypair.pem doesn't exist in config.json.**

  The key file does not exist. Check whether the key file path is correct.
- **Error: Error invalid character 'U' in string escape code in config.json.**

  The key file path is invalid. Use \\ for a Windows path, for example, **C:\\Users\\Administrator\\Desktop\\adb\\keypair.pem**.
- **Error: Error access key id is empty in config.json.**

  AK is not provided. Obtain it by referring to **Obtaining an AK/SK**.
- **Error: Error access secret key is empty in config.json.**

  SK is not provided. Obtain it by referring to **Obtaining an AK/SK**.

4 Change History

Released On	Description
2021-09-30	This issue is the ninth official release, which incorporates the following change: Added **What Are the Security Group Authorization Rules for Cloud Phones Using Custom Networks?**.
2020-11-24	This issue is the eighth official release, which incorporates the following change: Added **Can I Change the IP Address of My Cloud Phone?**.
2020-09-30	This issue is the seventh official release, which incorporates the following change: Added **Common ADB Commands**.
2020-07-30	This issue is the sixth official release, which incorporates the following change: Added **Does Each Cloud Phone Has an Independent Public IP Address?**.
2020-06-30	This issue is the fifth official release, which incorporates the following changes: • Added **What Can I Do If Message "unable to connect to :5555" Is Displayed When I Am Using ADB to Access a Cloud Phone?** • Added **What Can I Do If the ADB Connection Is Interrupted Suddenly?**

Released On	Description
2020-05-20	This issue is the fourth official release, which incorporates the following changes: • Added **What Does Message "Authorized users only. All activities may be monitored and reported." Indicate?** • Added **What Can I Do If Message "too open" Is Displayed When I Am Establishing the SSH Tunnel?**
2020-04-30	This issue is the third official release, which incorporates the following changes: • Added **How Do I Install Apps on a Cloud Phone?** • Added **What Should I Do If I Can't Find My Server on the Cloud Phone Console?** • Added **What Can I Do If Message "Permission denied" Is Displayed When I Am Establishing the SSH Tunnel?** • Added **How Do I Keep an SSH Session Uninterrupted?**
2020-02-18	This issue is the second official release, which incorporates the following changes: • Added **Is There Cloud Phone Root Permission?** • Added **How Do I Install Apps on a Cloud Phone?** • Added **How Long Does It Take to Activate a Server After I Purchase It?**
2019-01-31	This issue is the first official release.