Alibaba Cloud
Elastic Compute Service

User Guide

Issue: 20180917

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.
5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade

secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).

6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 **Danger:** Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 **Warning:** Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 **Note:** Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 **Note:** You can use **Ctrl** + **A** to select all files.
>	Multi-level menu cascade.	**Settings** > **Network** > **Set network type**
Bold	It is used for buttons, menus, page names, and other UI elements.	Click **OK**.
`Courier font`	It is used for commands.	Run the `cd /d C:/windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *{stand | slave}*

Contents

1 Quick reference

When using ECS, you may encounter various issues, such as connecting to the instance, resizing the disk, upgrading or downgrading the instance configurations, and using snapshots or images. This article provides you with a quick reference to popular features of ECS resources.

Operation instructions and limits

To guarantee proper operation of your ECS instance, You must carefully read all the *ECS operation instructions* and *Limits* before you use it.

Create and manage ECS instances

Basic operations

To use an ECS instances, follow these steps:

1. *Create an ECS instance*.
2. Connect to the ECS instance. Use different methods according to its operating system:
   a. Use the *Management Terminal* regardless of the operating system. Generally, this method is used for troubleshooting and maintenance.
   b. For Linux or Unix-like OS: *Connect to a Linux instance by using a password*, or *Connect to a Linux instance by using an SSH key pair*.
   c. For Windows OS: *Connect to a Windows instance*
3. *Stop the ECS instance*.
4. *Release the instance*.

Change configurations

You can change the instance type, IP addresses, and network bandwidth of your instance if the configurations cannot meet your business needs.

- Subscription instances: *Upgrade configurations of Subscription instances* or *Renew for configuration downgrade*
- *Change configurations of Pay-As-You-Go instances*
- *Change public IP address*
- *Convert public IP address to EIP address*

If the current operating system does not meet your needs, you can *change the operating system*.

Billing

You can *switch from Pay-As-You-Go to subscription*.

You can use different ways to renew Subscription instances:

- *Manual renewal*
- *Auto-renewal*

Elaborate management of and control over ECS instances

You can use the following features to elaborate management of and control over ECS instances:

- *User data*
- *Metadata*, including *instance identity*
- *Instance RAM roles*

Create and manage cloud disks

Basic operations

To use a cloud disk as a data disk, follow these steps:

1. *Create a cloud disk*.
2. *Attach a cloud disk*.
3. *(Linux) Format and mount a data disk* or *(Windows) Format a data disk*.
4. *Create snapshots* to back up data.
5. *Detach a cloud disk*.
6. *Release a cloud disk*.

Change configurations

When the capacity of the system disks or data disks cannot meet your business needs, you can *increase system disk size* or resize the data disks. For more information about resizing a data disk, see *Linux _ Resize a data disk* and *Windows _ Resize a data disk*.

Manage data on a cloud disk

When errors occur to data on a cloud disk, you can use a snapshot to *roll back a cloud disk* of the disk to restore data.

If you want to restore a cloud disk to its initial status after it is created, you can *reinitialize a cloud disk*.

If you want to copy data on an existing cloud disk to a new, empty cloud disk, you can *create a cloud disk from a snapshot*.

Create and manage snapshots

Basic operations

To use a snapshot, follow these steps:

1. Create a snapshot by using either of the following methods:
   - *Create snapshots*.
   - *Create and delete an automatic snapshot policy*, and *apply automatic snapshot policies to disks*, to enable creating snapshots automatically.
2. *View a snapshot chain*.
3. To save space occupied by snapshots, *delete unnecessary snapshots*.

Using snapshots

To copy or back up data: you can use a snapshot to *create a cloud disk from a snapshot*, or *roll back a cloud disk*.

To ease environment deployment, you can use a system disk snapshot to *create a custom image using a snapshot*, and *create an instance from a custom Image*.

Create and manage custom images

Only custom images can be operated in the ECS console. Using custom images can simplify environment deployment.

You can own a custom image by using the following methods:

- *Create a custom image using a snapshot*
- *Create a custom image by using an instance*
- *Use Packer to create a custom image*
- *Copy custom images* across different regions.
- *Share images* across different accounts.
- *Import custom images*
- *Create and import on-premise images by using Packer*

You can *export custom images* to back up the environment and *delete custom images*.

Create and manage security groups

Basic operations

To use a security group, follow these steps:

1. *Create a Security Group*.
2. *Add security group rules*.
3. *Add to or remove from a security group*

4. *Delete a security group rule*.
5. *Delete a security group*.

Manage security groups and their rules

To simplify business deployment, you can *clone a security group* across regions or network types.

When new security group rules impair the online business application, you can *restore security group rules* fully or partially.

Create and manage SSH key pairs

To use an SSH key pair, follow these steps:

1. *Create an SSH key pair*, or *import an SSH key pair*.
2. *Bind a SSH key pair*, or bind the SSH key pair after a Linux instance is created or when you *create an instance*.
3. *Connect to a Linux instance by using an SSH key pair*.
4. *Unbind an SSH key pair*.
5. *Delete a SSH key pair*.

Create and manage ENIs

To use an ENI, follow these steps:

1. *Create an ENI*.
2. *Attach an ENI to an instance*, or *attach an ENI when creating an instance*.
3. Optional. *Configure an ENI*.
4. *Detach an ENI from an instance*.
5. *Delete an ENI*.

Use tags

You can use tags to group resources to improve efficiency. To use tags, follow these steps:

1. *Add a tag to resources*.
2. *Filter resources by tags*.
3. *Delete a tag*.

2 ECS operation instructions

To guarantee proper operation of your ECS instance, you must take the considerations outlined in this section into account before use.

Prohibitions

- Alibaba Cloud prohibits you from using your instance for flow-through services. Any violation results in punishment up to shutdown and lockout of instance, and termination of services.
- Alibaba Cloud prohibits you from using your instance for click farming, advertising, or fictitious transactions.
- Alibaba Cloud prohibits you from activating SELinux.
- Alibaba Cloud prohibits you from uninstalling hardware related drivers.
- Alibaba Cloud prohibits you from arbitrarily modifying the MAC address of the network adapter.

Suggestions

- For an ECS with more than 4 GiB RAM, we recommend that you use a 64-bit OS, because a 32-bit OS supports a maximum of 4 GiB RAM. Currently available 64-bit systems include:
  - Aliyun Linux
  - CoreOS
  - CentOS
  - Debian
  - FreeBSD
  - OpenSUSE
  - SUSE Linux
  - Ubuntu
  - Windows
- 32-bit Windows OS supports CPUs with up to 4 cores.
- A minimum of 2 GiB RAM is needed for buiding a website on a Windows instance, and an instance type with 1 vCPU core and 1 GiB RAM cannot be used for MySQL service.
- To guarantee service continuity and avoid service downtime, you must enable auto-start of service applications upon OS boot.
- For I/O-optimized instances, do not stop the aliyun-service process.
- We do not recommmend that you update the kernel and the OS. For more information, see *How to avoid Linux instance startup failure after kernel upgrade*.

Windows restrictions

- Do not close the built-in shutdownmon.exe process, which may delay the restart of your Windows server.
- Do not rename, delete, or disable the Administrator account.
- We do not recommend that you use virtual memory.

Linux restrictions

- Do not modify the content of the default /etc/issue file. Otherwise, if you create a custom image of the ECS instance and create a new ECS instance based on the image, the new instance cannot start because the operating system edition cannot be recognized.
- Proceed with caution when modifying permissions of the directories in the root partition, such as `/etc`, `/sbin`, `/bin`, `/boot`, `/dev`, `/usr` and `/lib`. Improper modification of permissions may cause errors. Such modifications may cause system errors.
- Do not rename, delete, or disable the Linux root account.
- Do not compile or perform any other operations on the Linux kernel.
- We do not recommend that you use swap partition.
- Do not enable the NetWorkManager service. This service conflicts with the internal network service of the system and causes network errors.

For more information, see *Limits*.

3 Limits

When using ECS, consider the following:

- ECS does not support virtual application installation or subsequent virtualization such as when using VMware. Currently, only *ECS Bare Metal Instance and Super Computing Clusters* supports virtualization.
- ECS does not support sound card applications.
- ECS does not support the installation of external hardware devices such as hardware dongles, USB drives, external hard drives, and the USB security keys issued by banks.
- ECS does not support SNAT and other IP packet address translation services. You can achieve this by using an external VPN or proxy.
- ECS does not support multicast protocol. If multicasting services are required, we recommend that you use unicast point-to-point method.
- Currently, Log Service does not support 32-bit Linux ECS instance. To know the regions that support Log Service, see *Service endpoint*. To know the server operating systems that support Log Service, see *Overview*.

Besides the preceding limit, the additional limits of ECS are mentioned in the following table.

ECS instances

Item	Limit	Supply for higher configuration or unlock configuration rights
Permission to create instances	*Complete real-name registration* to create ECS instances in the mainland China regions	Not supported
Default quota of Pay-As-You-Go ECS instances (including preemptible instances) in all regions for one account	10	Open a ticket
Launch templates in each region for one account	30	Not supported
Versions of one launch template	30	Not supported

Item	Limit	Supply for higher configuration or unlock configuration rights
Conversion of the billing method from Pay-As-You-Go to Subscription	Not supported in the following instance types or type families: • Generation II: n1, ne2, and e3 • All instance types of Generation I	Not supported
Default available instance types for creating Pay-As-You-Go ECS instances (New generation)	ecs.t1.small (1 vCPU core, 1 GiB)	Open a ticket
	ecs.s1.small (1 vCPU core, 2 GiB)	
	ecs.s1.medium (1 vCPU core, 4 GiB)	
	ecs.s2.small (2 vCPU core, 2 GiB)	
	ecs.s2.large (2 vCPU core, 4 GiB)	
	ecs.s2.xlarge (2 vCPU core, 8 GiB)	
	ecs.s3.medium (4 vCPU core, 4 GiB)	
	ecs.s3.large (4 vCPU core, 8 GiB)	
	ecs.m1.medium (4 vCPU core , 16 GiB)	
Default available instance types for creating Pay-As-You-Go ECS instances (Previous generation)	ecs.n1.tiny (1 vCPU core, 1 GiB)	Open a ticket
	ecs.n1.small (1 vCPU core, 2 GiB)	
	ecs.n1.medium (2 vCPU core, 4 GiB)	
	ecs.n1.large (4 vCPU core, 8 GiB)	

Item	Limit	Supply for higher configuration or unlock configuration rights
	ecs.n2.small (1 vCPU core, 4 GiB)	
	ecs.n2.medium (4 vCPU core, 8 GiB)	
	ecs.n2.large (4 vCPU core, 16 GiB)	
	ecs.e3.small (1 vCPU core, 8 GiB)	
	ecs.e3.medium (2 vCPU core, 16 GiB)	

Block storage

Item	Limit	Supply for higher configuration or unlock configuration rights
Permission to create Pay-As-You-Go cloud disks	*Complete real-name registration* to create cloud disks in the mainland China regions	Not supported
Quota of Pay-As-You-Go cloud disks in all regions for one account	Five times of the number of Pay-As-You-Go instances in all regions under one account	Open a ticket
Quota of system disks for one ECS instance	1	Not supported
Quota of data disks for one ECS instance	16 (including cloud disks and Shared Block Storage)	Not supported
Multi-node attachment of shared block storage	8	Not supported
Quota of shared block storage in all regions for one account	10	Open a ticket
Capacity of one Basic Cloud Disk	5 GiB ~ 2,000 GiB	Not supported

Item	Limit	Supply for higher configuration or unlock configuration rights
Capacity of one SSD Cloud Disk	20 GiB ~ 32,768 GiB	Not supported
Capacity of one Ultra Cloud disk	20 GiB ~ 32,768 GiB	Not supported
Capacity of one ephemeral SSD disk	5 GiB ~ 800 GiB	Not supported
Capacity of ephemeral SSD disks on one ECS instance	1,024 GiB	Not supported
Capacity of one NVMe SSD local disk	1,456 GiB	Not supported
Capacity of NVMe SSD local disks on one ECS instance	2,912 GiB	Not supported
Capacity of one SATA HDD local disk	5,500 GiB	Not supported
Capacity of SATA HDD local disks on one ECS instance	154,000 GiB	Not supported
Capacity of one SSD Shared Block Storage device	32,768 GiB	Not supported
Capacity of SSD Shared Block Storage devices on one ECS instance	128 TiB	Not supported
Capacity of one Ultra Shared Block Storage device	32,768 GiB	Not supported
Capacity of Ultra Shared Block Storage devices on one ECS instance	128 TiB	Not supported
Size limit of one system disk	Windows: 40 GiB − 500 GiB Linux (excluding CoreOS)+ FreeBSD: 20 GiB − 500 GiB CoreOS: 30 GiB − 500 GiB	Not supported
Size limit of one data disk	Basic Cloud Disk: 5 GiB − 2,000 GiB SSD Cloud Disk/ Ultra Cloud Disk/SSD Shared Block Storage/Ultra Shared	Not supported

Item	Limit	Supply for higher configuration or unlock configuration rights
	Block Storage: 20 GiB − 32,768 GiB Local disk: See *Local disks*.	
Attaching an independent local disk to an ECS instance with local disks	Not supported	Not supported
Configuration changes of an ECS instance with local disks	Only changes to public network bandwidth are permitted	Not supported
Mount point for system disks	/dev/xvda	Not supported
Mount points for data disks	/dev/xvd[b-z]	Not supported

Snapshots

Item	Limit	Supply for higher configuration or unlock configuration rights
Quota of snapshots	Number of elastic block storage devices * 64	Not supported

Images

Item	Limit	Supply for higher configuration or unlock configuration rights
Quota of custom images in all regions for one account	100	Open a ticket
Quota of accounts to share one custom image	100	Open a ticket
Requirements of images for instance types	32-bit images are not supported on an instance with 4 GiB or more RAM.	Not supported

Key pairs

Item	Limit	Supply for higher configuration or unlock configuration rights
Quota of key pairs in all regions for one account	500	Not supported
Instance types supporting key pairs	All instance types, except those non-I/O optimized instance types in Generation I	Not supported
Images supporting key pairs	Linux images only	Not supported

Security groups

Item	Limit	Supply for higher configuration or unlock configuration rights
Quota of ECS instances for one security group	1,000	Not supported
Quota of rules for one security groups	100	Not supported
Quota of security groups in all regions for one account	100	Open a ticket
Quota of security groups for one ECS instances	5	Open a ticket
Port	Access to TCP Port 25, which is the default port for the STMP service, is denied. It cannot be allowed by adding a security group rule.	Open a ticket. For more information, see *Apply to open TCP port 25*

ENI

Item	Limit	Supply for higher configuration or unlock configuration rights
Quota of ENI in one region for one account	100	Open a ticket

Tags

Item	Limit	Supply for higher configuration or unlock configuration rights
Quota of tags for one ECS instance	20	Not supported

API

Item	Limit	Supply for higher configuration or unlock configuration rights
Invocation quota of CreateInstance	At most 200 times per minute	Open a ticket

Note:

For more information about the limits for VPC, see *Limits*.

4 Connect to instances

4.1 Overview

Based on the network type and operating system of your ECS instance, and the operating system of your local machine, you can choose an ideal method to connect to an ECS instance.

Connect to a Linux instance

Choose an ideal method from the following table to create remote connection to your Linux instance.

Internet access	Operating system of the local machine	Connection option
Yes/No	Windows or Unix-like OS	*Connect to an instance by using the Management Terminal*
Yes	Windows	Use a remote connection tool to create remote connection: • Use an SSH key pair as the credential: *Connect to a Linux instance by using an SSH key pair* • Use a password as the credential: *Connect to a Linux instance by using a password*
Yes	Linux, Mac OS, or other Unix-like OS	Use commands to create remote connection: • Use an SSH key pair as the credential: *Connect to a Linux instance by using an SSH key pair* • Use a password as the credential: *Connect to a Linux instance by using a password*
Yes	iOS or Android	User apps, such as SSH Control Lite or JuiceSSH, to create remote connection:

Internet access	Operating system of the local machine	Connection option
		Connect to an instance on a mobile device

Connect to a Windows instance

Choose an ideal method from the following table to create remote connection to your Windows instance.

Internet access	Operating system of the local machine	Connection option
Yes/No	Windows or Unix-like OS	*Connect to an instance by using the Management Terminal*
Yes	Windows	Use mstsc to create remote connection: *Connect to a Windows instance*
Yes	Linux	Use a remote connection tool, such as rdesktop, to create remote connection: *Connect to a Windows instance*
Yes	Mac OS	Use Microsoft Remote Desktop Connection for Mac to create remote connection: *Connect to a Windows instance*
Yes	iOS or Android	Use Microsoft Remote Desktop to create a remote connection: *Connect to an instance on a mobile device*

4.2 Connect to an instance by using the Management Terminal

You can use the Management Terminal, also known as VNC, to connect to an ECS instance. Specifically, when the remote access software programs that you are using, such as PuTTy, Xshell, or SecureCRT, do not work.

Scenarios

The Management Terminal can be used to:

- Check the status of an ECS instance if it starts slowly.
- Reconfigure the firewall if a remote connection fails because of any software error within the ECS instance.
- End abnormal processes that consume excessive CPU usage or bandwidth.

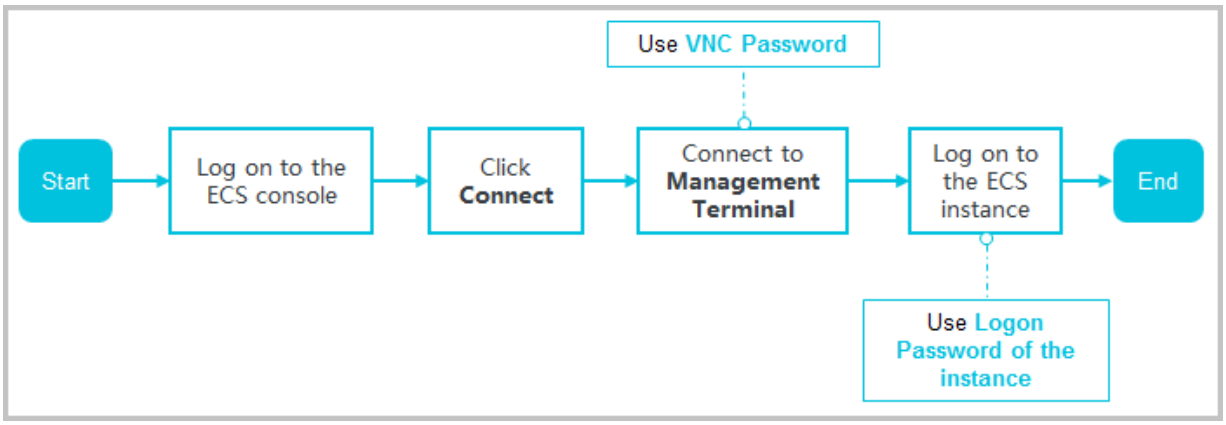
Note:
The Management Terminal can be used to connect to an instance even if no public IP address is assigned to your instance.

Prerequisites

- You have an ECS instance. For more information, see *Create an ECS instance*.
- You have set the logon password of the ECS instance. If not, use the *Reset Password* feature to set a password.

Procedure

The following figure illustrates how to use the Management Terminal to connect to an ECS instance.



To connect to the ECS instance by using the Management Terminal, follow these steps:

1. Log on to the *ECS console*.
2. In the left-side navigation pane, click **Instances**.
3. Select a region.
4. In the instance list, find your instance, and in the **Actions** column, click **Connect**.
5. In the **Management Terminal** page, follow the instructions to connect to the Management Terminal:

- If you log on as an Alibaba Cloud account to connect to the Management Terminal for the first time, follow these steps:

  1. In the **VNC Connection Password** dialog box, copy the password and click **Close**.

     Note:

     - The VNC password appears only once. You must save and secure password immediately for future use. If you need to change the VNC password, see *Change the VNC connection password*.
     - If you log on as a RAM user to connect to the Management Terminal for the first time , you will not see this dialog box.

  2. In the **Enter VNC Password** dialog box, paste the VNC connection password that you have copied, and click **OK**.

- If you log on as a RAM user to connect to the Management Terminal for the first time or in case you have forgotten your VNC connection password, follow these steps to connect to the Management Terminal:

  — *Change the VNC connection password*.

  — In the upper-left corner of the **Management Terminal** page, select **Send Remote Command** > **Connect to Management Terminal**.

  — In the **Enter VNC Password** dialog box, enter the new password and click **OK**.

- If this is not your first connection to the Management Terminal, enter the VNC connection password in the **Enter VNC Password** dialog box and click **OK**.

6. To log on to the ECS instance, follow these steps according to the operating system:

   - For a Linux instance: Enter the user name (`root`) and the logon password.

     Note:

     - If you forget the logon password of your instance, *reset the password*.
     - The logon password input is invisible.
     - If you want to do different operations within the instance, in the upper-left corner of the **Management Terminal** page, select **Send Remote Command** > **CTRL + ALT + Fx**, of which **Fx** can be any key from **F1** to **F10**, to switch the interfaces for different operations.

- In case you see a black screen, the Linux instance may be in sleep mode. To exit sleep mode, click the mouse or press any key.

- For a Windows instance: In the upper-left corner of the **Management Terminal** page, select **Send Remote Command** > **CTRL+ALT+DELETE**. The Windows logon interface is displayed. Enter the user name (**`Administrator`**) and the logon password.

> **Note:**
> If you forget the logon password of your instance, *reset the password*.

Other Operations

Change the VNC connection password

If you forget the VNC connection password, follow these steps to change the password.

> **Note:**
> If the instance that you are connecting to is not I/O optimized, you must restart your instance in the ECS console to apply new VNC password. The restart operation stops your instance and interrupts your business operations. Therefore, proceed with caution.

1. Open the **Management Terminal** page.
2. Close the VNC **Connection Password** dialog box or the **Enter VNC Password** dialog box.
3. In the upper-right corner of the **Management Terminal** page, click **Modify Management Terminal Password**.
4. Enter a new password, which must be six characters in length and may contain uppercase letters, lowercase letters, and digits. Special characters are not supported.
5. A new password can be effective in the following events:

   - For an I/O-optimized instance, the new password takes effect immediately.
   - For a non-I/O-optimized instance, *restart the instance* in the ECS console.

> **Note:**
> Restarting the operating system does not apply the new password.

Input commands

If you are connecting to a Linux instance, use the **Input Commands** feature to type long text, such as a complex command or a URL.

Follow these steps:

1. Open the **Management Terminal** page.
2. In the upper-right corner of the **Management Terminal** page, click **Input Commands**.
3. In the **Copy Commands** dialog box, enter the commands and click **OK**.
4. Press the **Enter** key to run the commands.

FAQ

- Can multiple users simultaneously connect to the Management Terminal?

  No. Only one user can connect to the Management Terminal at a time.

- Why am I unable to connect to an instance by using the Management Terminal even after changing the password?

  Make sure that you enter the correct VNC password. If the instance that you are connecting to is not I/O optimized, you must restart the instance in the ECS console. This action helps the new VNC password to take effect.

- Why do I see a black screen after logging on to my instance?

  A black screen indicates that the instance is in sleep mode.

  For a Linux instance, click mouse or press any key to activate the screen.

  For a Windows instance, click **Send remote command** > **CTRL+ALT+DELETE** to view logon interface.

- Why am I unable to access the Management Terminal?

  To resolve logon issues, open your browser and connect to the Management Terminal. Press **F12** to open the developer tool. The Management Terminal information can be analyzed to locate errors under the Console tab.

- Can I use IE or Firefox to access the Management Terminal?

  You can access the Management Terminal only if you have IE10 or later versions installed . Only certain versions of Firefox are supported. You can resolve this issue by updating or changing your browser to a recommended version.

  Note:

  We recommend that you use Google Chrome because it offers the best support for the Management Terminal function.

4.3 Connect to a Linux instance by using an SSH key pair

How to use a key pair to log on to a Linux instance depends on the local operating system.

- *Windows OS*
- *Linux OS or other systems supporting SSH commands*

Note:
You can use a password to connect to a Linux instance. For more information, see *Connect to a Linux instance by using a password* and *Connect to an instance by using the Management Terminal*.

Windows OS

In this section, it is demonstrated how to use a key pair to log on to a Linux instance on a Windows system, using the popular SSH tools PuTTY and PuTTYgen as an example.

Prerequisites

- PuTTY and PuTTYgen must have been installed. You can download them at:
  - *PuTTY*
  - *PuTTYgen*
- You must have a Linux instance that has been bound to an instance. You can allocate an SSH key pair when creating an instance or *bind an SSH key pair to an instance*.
- Add the following rule in the security group to enable the access to the TCP Port 22 of the instance. For more information, see *Add security group rules*.

Network Type	NIC	Rule Direction	Authorization Policy	Protocol Type	Port Range	Authorization Type	Authorization Object	Priority
VPC	N/A	Inbound	Allow	SSH(22)	22/22	Address Field Access	0.0.0.0/0	1
Classic	Internet							

Procedure

1. Optional. If you are using a key pair generated by Alibaba Cloud, of which the private key is a .pem file, you must convert it to a .ppk file. If your private key is a .ppk file, you can skip this step.

Note:

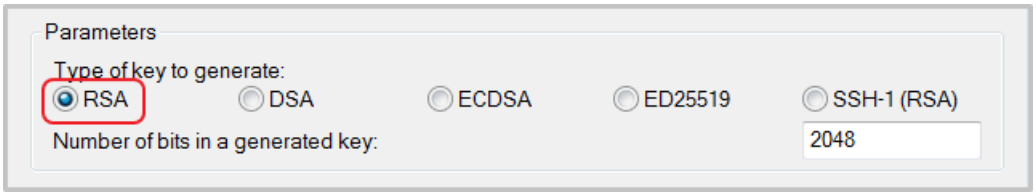
When you *create an SSH key pair*, download the .pem private key.

a. Start PuTTYgen. In this example, we use PuTTYgen version 0.68.

b. Under **the** > **Type of key to generate option,** select RSA.

Note:

The value of Number of bits in a generated key can be left as is. The software automatically update the value based on the imported private key information.



c. Click **Load** to find your *.pem* file.

Note:

By default, PuTTYgen only displays files with an extension of *.ppk*.

d. Select the downloaded private key file from Alibaba Cloud, or the ready private key file, and click **Open**.

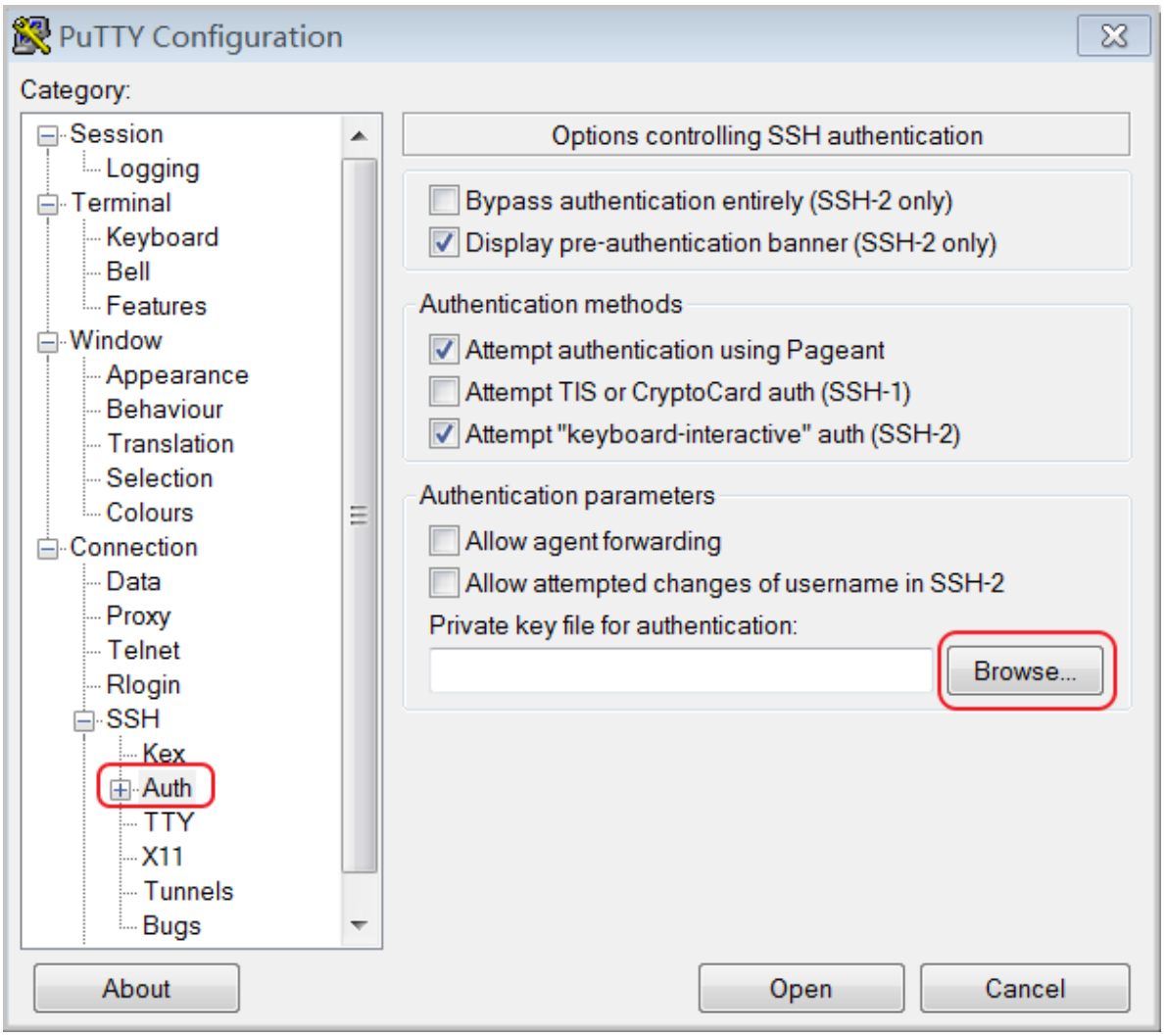
e. Click **OK** to close the confirmation dialog box.

f. Click **Save private key**. PuTTYgen displays warning about saving the key without a password. Click **Yes**.

g. Specify the same name for the private key with the key pair, and save the settings. PuTTY automatically adds the .ppk file.

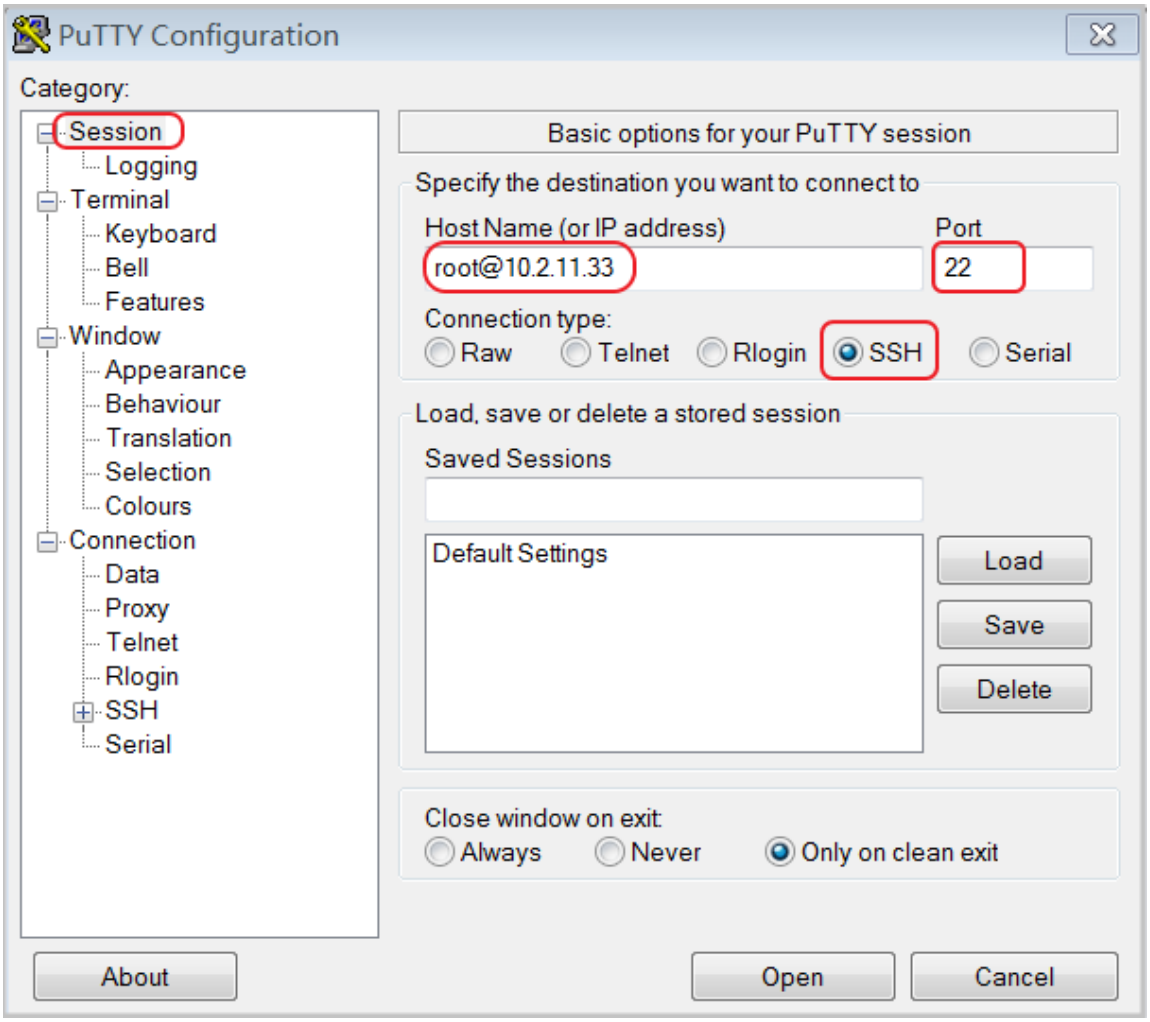
2. Start PuTTY.

3. Select **Connection >** > **SSH >** > **Auth.**Click **Browse…** and select the .ppk file generated in Step 1.



4. Click **Session**.

   - In **`Host Name (or IP address)`**, enter your account and the public IP address of the instance to be connected to. The format is `root@IP address`.
   - In **`Port`** enter the port number 22.
   - For **`Connection type`**, select SSH.



5. Click **Open** to start accessing your Linux instance.

When the window shows `Connection established.`, it indicates you have successfully logged on to the instance using the key pair.

Linux OS or other systems supporting SSH commands

In this section, it is demonstrated how to use a key pair to log on to a Linux instance on a Linux system or a system supporting SSH commands, such as MobaXterm for Windows.

Prerequisites

You must have a Linux instance that has been bound to an SSH key pair. You can *allocate an SSH key pair when creating an instance* , or *bind an SSH key pair to an instance*.

Add the following rule in the security group to enable the access to the TCP Port 22 of the instance. For more information, see *Add security group rules*.

Network Type	NIC	Rule Direction	Authorization Policy	Protocol Type	Port Range	Authorization Type	Authorization Object	Priority
VPC	N/A	Inbound	Allow	SSH(22)	22/22	Address Field Access	0.0.0.0/0	1
Classic	Internet							

Procedure

1. Locate directory of your private key, for example, `/root/xxx.pem`.

   Note:
   When you *create an SSH key pair*, download the .pem private key. xxx.pem is the private key file.

2. To modify the attributes of the private key, run the command: `chmod 400 [directory of the private key file]`. For example, `chmod 400 /root/xxx.pem`.
3. To connect to the instance, run the command `ssh -i directory of the private key file] root@Internet IP address`. For example, `ssh -i /root/xxx.pem root@10.10.10.100`.

4.4 Connect to a Linux instance by using a password

You can connect to a Linux instance by using different authentication methods:

- If you are using an SSH key pair, see *Connect to a Linux instance by using an SSH key pair*.
- If you are using a password, you can *connect to an instance by using the Management Terminal* or by using software applications or command lines.

Prerequisites

Before you begin, make sure the following:

- The instance must be in the **Running** status. If not, *start it*.
- You have set a logon password for the instance. If the password is lost, *reset the password*.
- The instance can access Internet:
  - In a VPC, a public IP address is assigned to the instance or *an EIP address is bound to the instance*.
  - In the classic network, a public IP address is assigned to the instance by using either of the following methods:

  - For a Subscription or a Pay-As-You-Go instance, you can select Assign public IP when creating the instance.
  - For a Subscription instance without public IP address, you can assign one by *upgrading bandwidth*.
- The following security group rules must be added to the security group that the instance joins. For more information, see *Add security group rules*.

Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
VPC	N/A	Inbound	Allow	SSH (22)	22/22	Address Field Access	0.0.0.0/0	1
Classic	Internet							

Procedure

Based on the operating system of your local machine, you have various options to connect to a Linux instance by using the SSH protocol:

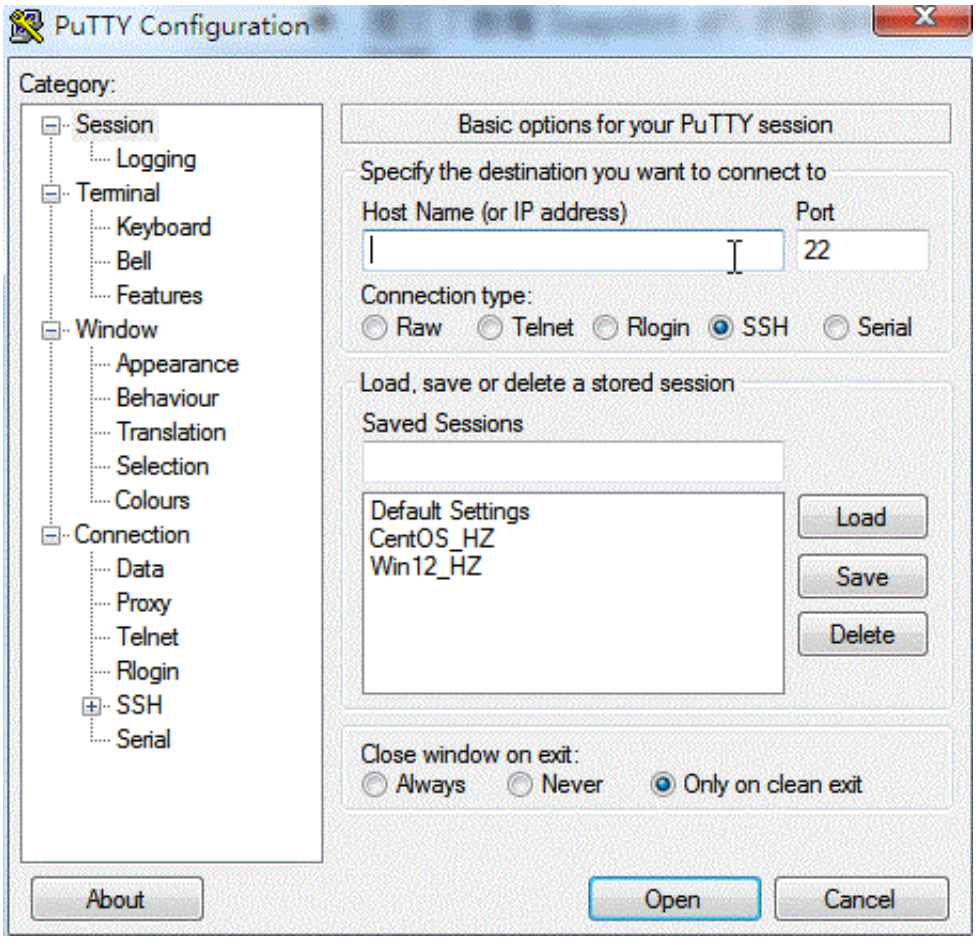
- *Windows OS*
- *Linux or Mac OS X*
- *Android or iOS*

Windows OS

If your local machine is running Windows OS, you can use a remote connection tool, such as PuTTY, to connect to a Linux instance. In this article, we use PuTTY as an example to describe how to connect to a Linux instance by using the password authentication method. Before you start, download *PuTTY*.

Follow these steps to connect to a Linux instance:

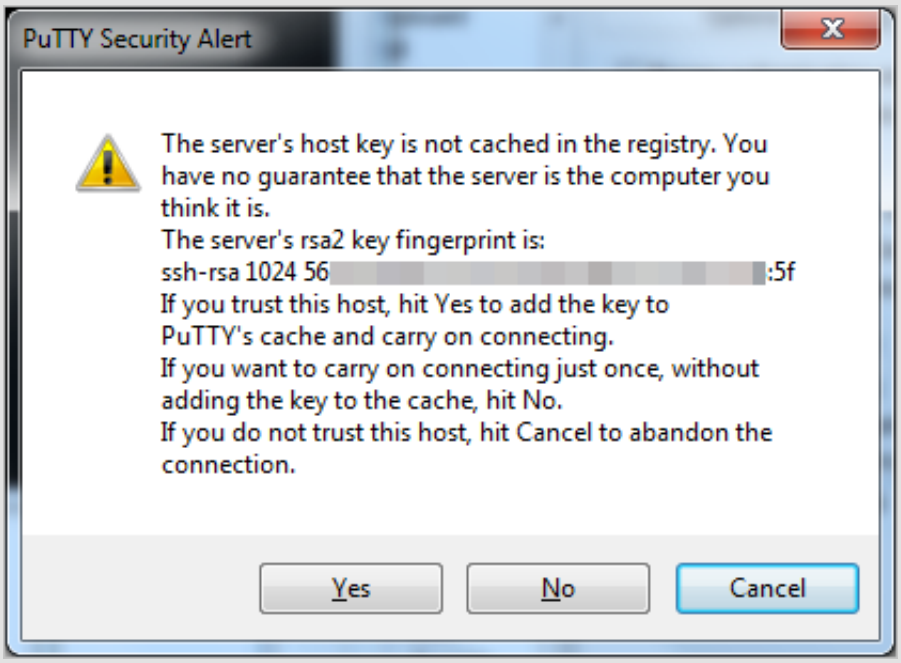
1. Start putty.exe.
2. In the left-side navigation pane, click **Session**, and configure the following parameters:
   - **Host Name**: Type the public IP address or EIP address of the instance.
   - **Port**: Type 22.
   - **Connection Type**: Select SSH.
   - (Optional) **Saved Session**: If you do not want to repeat the configurations during the next logon, add a name for the session, and click **Save**.



3. Click **Open** to connect, and in the PuTTY Security Alert dialog box, click Yes.

Note:

For the first connection to an ECS instance, you have the PuTTY Security Alert as follows, which means PuTTY cannot guarantee the instance is the one that you think it is, so it can only provide the public key fingerprint of the instance for you to decide to trust the instance or not. If you select **Yes**, the public key will be added to the PuTTY's cache and you will not be alerted again during your next connection. If you select Yes but are alerted again, a *man-in-the-middle attack (MITM)* may occur. For more information, see *PuTTY User Manual*.



4. As prompted, type the username and password for the Linux instance, and press the Enter key.

> **Note:**
> The password is not displayed on screen.

When you see the following message, you have successfully connected to an instance.

```
Welcome to Alibaba Cloud Elastic Compute Service !
```

Now, you can start working on your instance.

Linux or Mac OS X

If your local machine is running Linux OS or Mac OS X, follow these steps:

1. Run the command `ssh root@[Public IP address or EIP address of the instance]`.
2. Type the password and press the Enter key.

When you see the following message, you have successfully connected to an instance.

```
Welcome to Alibaba Cloud Elastic Compute Service !
```

Now, you can start working on your instance.

Android or iOS

If your local machine is running Android OS or iOS, you can use various apps to connect to a Linux instance. For more information, see *Connect to an instance on a mobile device*.

Reference

You can run a script to install a graphical desktop on an instance running CentOS. For more information, see *Automatic installation tool for Linux instance*.

4.5 Connect to a Windows instance

If your Windows instance can access Internet, you can use remote connection tools to connect to it. Otherwise, you can use the *Management Terminal*.

Prerequisites

Before you start, complete the following:

- The instance is in the **Running** status. If not, *start it*.
- You have set a logon password for the instance. If the password is lost, *reset the password*.
- The instance can access Internet:
  - In a VPC, a public IP address is assigned to the instance or *an EIP address is bound to the instance*.
  - In the classic network, a public IP address is assigned to the instance by using either of the following methods:
    - For a Subscription or a Pay-As-You-Go instance, you can select Assign public IP when creating the instance.
    - For a Subscription instance without public IP address, you can assign one by *upgrading bandwidth*.
- The following security group rules must be added to the security group that the instance joins. For more information, see *Add security group rules*.

Network Type	NIC	Rule Direction	Authorization Policy	Protocol Type	Port Range	Authorization Type	Authorization Object	Priority
VPC	N/A	Inbound	Allow	RDP(3389)	3389/3389	Address Field Access	0.0.0.0/0	1
Classic	Internet							

Procedure

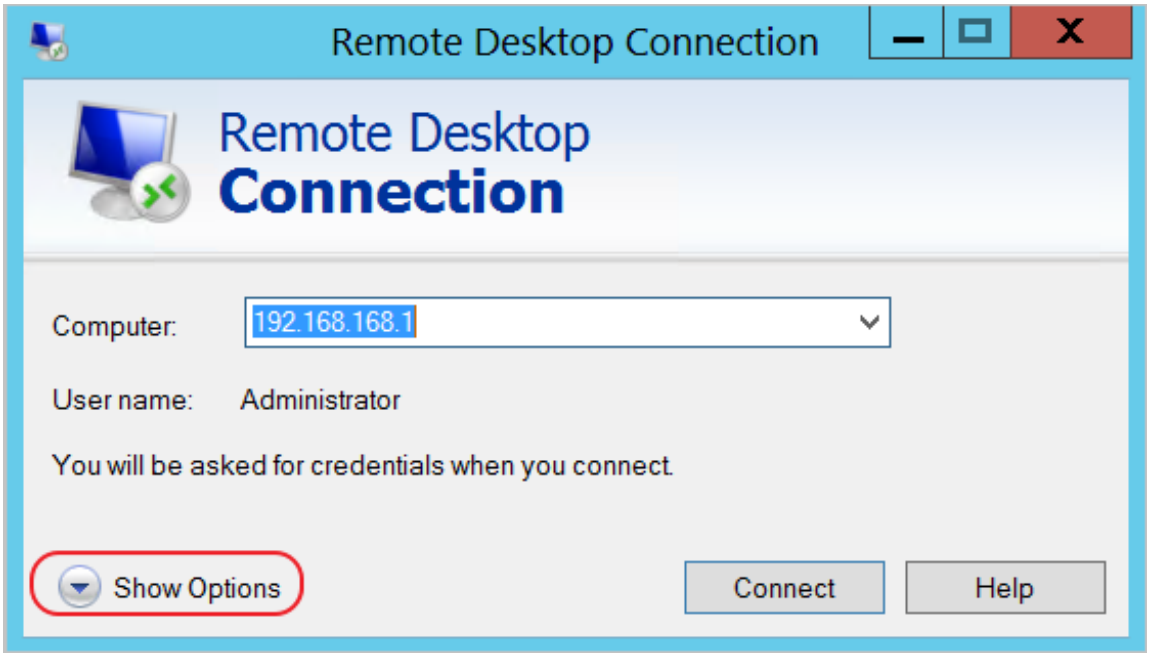
Based on the operating system of your local machine, you have various options to connect to a Windows instance:

- *Windows OS*
- *Linux*
- *Mac OS*
- *Android or iOS*

Windows OS

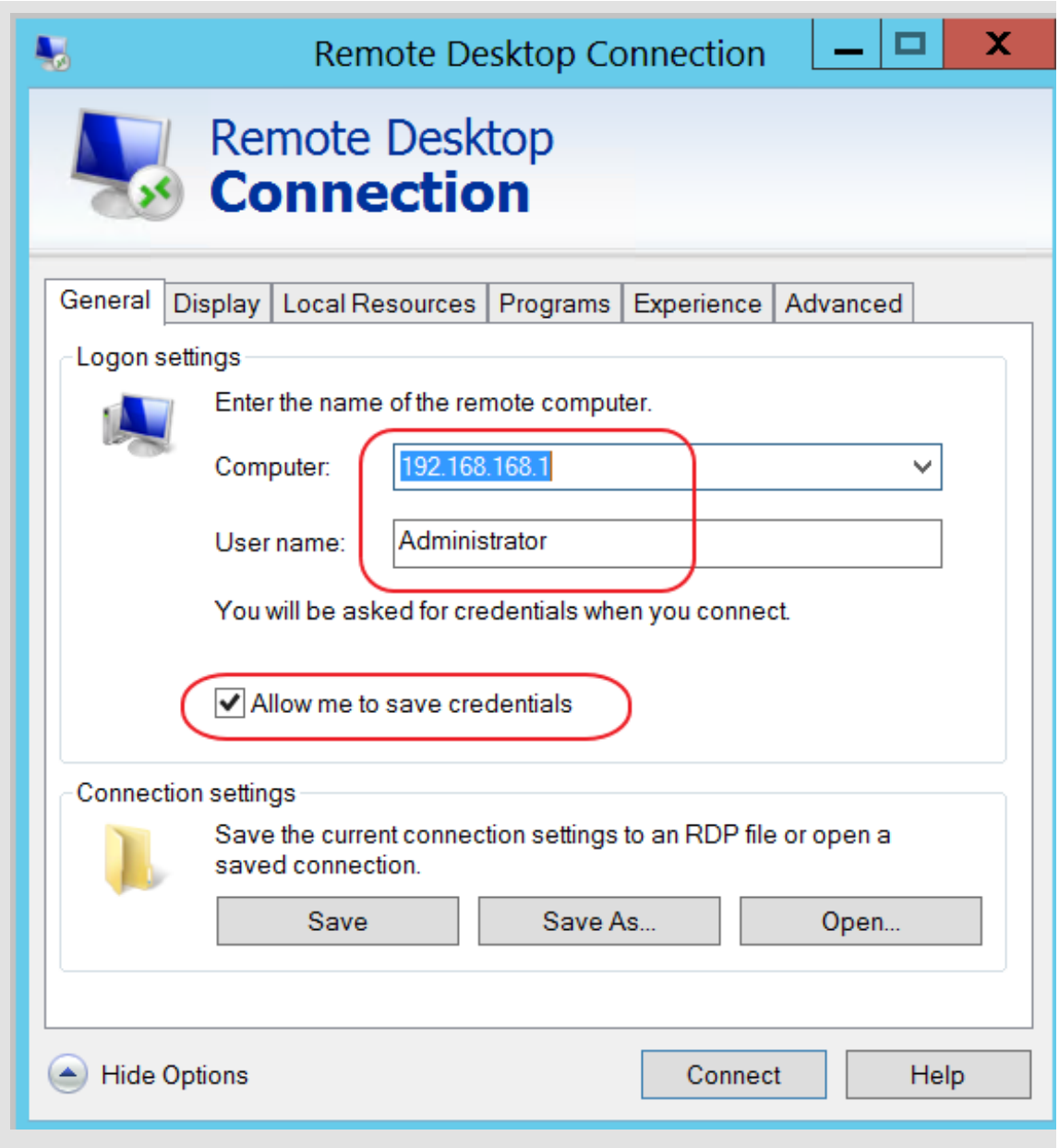
If the local machine is running Windows OS, you can use the mstsc to create a remote connection to a Windows instance.

1. Use any one of the following methods to start **mstsc**:
   - Select **Start** > **icon** > **Remote Desktop Connection**.
   - Click the **Start** icon and search for mstsc.
   - Press the shortcut key **Windows Logo** + **R** to open the **Run** windows, type **`mstsc`**, and then press the Enter key.
2. In the **Remote Desktop Connection** dialog box, follow these steps:
   a. Click the **Show Options** drop-down box.



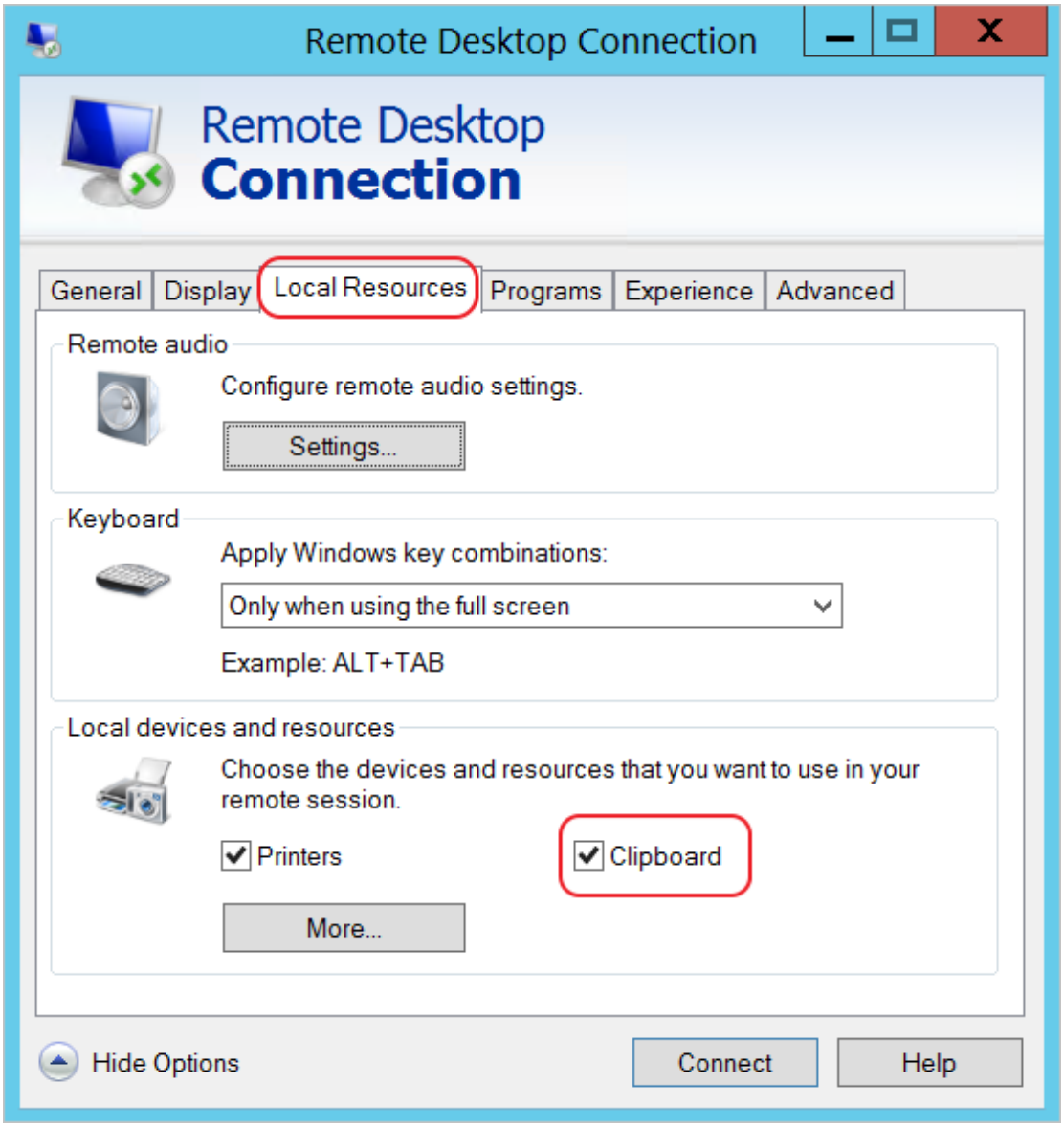
   b. Type the public IP address or EIP address of the instance.
   c. Type the user name. The default user name is **`Administrator`**

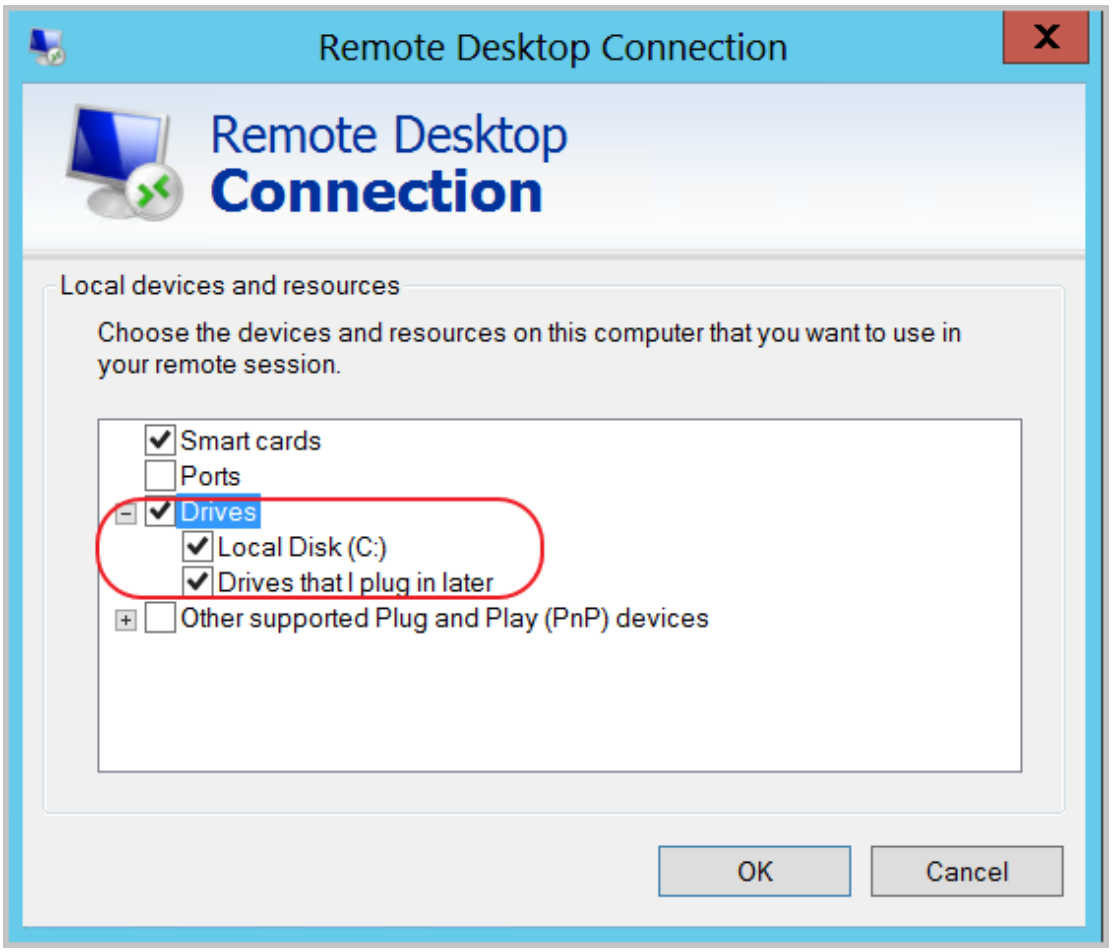
> **Note:**
> If you want to log on to the instance next time without repeating these steps, select **Allow me to save credentials**.



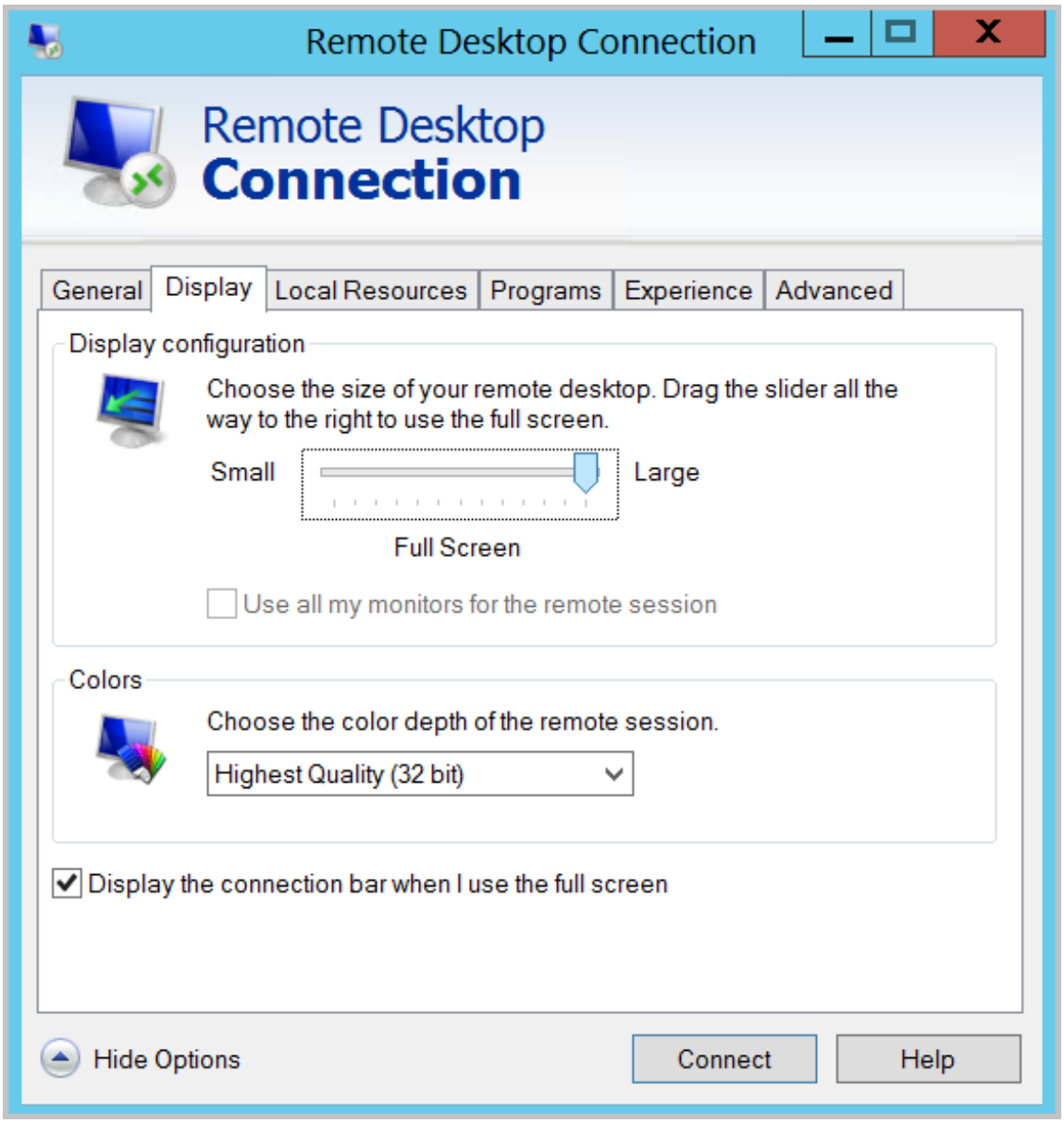
d. Optional. If you want to copy text or files from the local machine to the instance, click the **Local Resources** tab to see options for sharing local computer resources.

- If you want to copy text only, select **Clipboard**.
- If you also want to copy files, select **More** and select drive letters from which you want to copy files to your instance and click OK.


Remote Desktop Connection
Remote Desktop
Connection
General
Display
Local Resources
Programs
Experience
Advanced
Remote audio
Configure remote audio settings.
Settings...
Keyboard
Apply Windows key combinations:
Only when using the full screen
Example: ALT+TAB
Local devices and resources
Choose the devices and resources that you want to use in your remote session.
Printers
Clipboard
More...
Hide Options
Connect
Help



e. Optional. Click the **Display** tab and resize the remote desktop window. Full Screen is recommended.



f. Click **Connect**.

Now, you can operate on the instance.

Linux

If the local machine is running Linux OS, you can use a remote connection tool to create a remote connection to a Windows instance. This article takes rdesktop as an example to describe how to connect a Windows instance from a local machine running Linux.

1. Download and start rdesktop.

2. Run the command to connect to a Windows instance. Replace the parameter values with your own configurations.

```
rdesktop -u administrator -p password -f -g 1024*720 192.168.1.1 -r
clipboard:PRIMARYCLIPBOARD -r disk:sunray=/home/yz16184
```

The parameter descriptions are as follows.

Parameters	Description
-u	The user name. The default user name for Windows instance is Administrator.
-p	The password used to log on to the windows instance.
-f	Full screen by default. Use **Ctrl**+**Alt**+**Enter** to switched the mode.
-g	Resolution. Asterisks (*) are used for separation. If omitted, full-screen display by default.
192.168.1.1	The IP address of the server that requires remote connection. Replace it with the public IP or EIP address of your windows instance.
-d	Domain name. For example, if the domain name is INC, then the parameter is `-d inc`.
-r	Multimedia reorientation. For example: • Turn on the sound:`--r sound`. • Use a local sound card:-r sound: `-r sound : local`. • Open the U Disk: `-r disk:usb=/mnt/usbdevice`.
-r clipboard:PRIMARYCLIPBOARD	Realizes direct word copying and pasting between Linux and Windows instances of local devices. Supports Chinese words copying and pasteing.
-r disk:sunray=/home/yz16184	Specifies that a directory on Linux system of a local device maps to a hard disk on a Windows instance. In this way, you can no longer rely on Samba or FTP to transfer files.

For more information about all the parameters of the `rdesktop` command, see *rdesktop documentation*.

Mac OS

To connect to a Windows instance from a local machine running Mac OS, see *Get started with Remote Desktop on Mac* in the Microsoft website.

Android or iOS

If your local machine is running Android OS or iOS, you can use various apps to connect to a Linux instance. For more information, see *Connect to an instance on a mobile device*.

4.6 Connect to an instance on a mobile device

This documentation describes how to connect to an ECS instance on a mobile device. The procedure varies with the operating system of your instance.

- *Connect to a Linux instance*: We take SSH Control Lite as an example to describe how to connect to a Linux instance on an iOS device, and JuiceSSH to describe how to connect to a Linux instance on an Android device.
- *Connect to Windows instances*: We take Microsoft Remote Desktop as an example to describe how to connect to a Windows instance on an iOS or Android device.

Connect to a Linux instance

Prerequisites

Confirm the following before connecting to your instance:

- The instance is **Running** .
- The instance has a public IP address and is accessible from public network.
- You have set the logon password for the instance. If the password is lost, you must *reset the instance password*.
- The security group of the instance has the *the following security group rules*:

Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
VPC	No configuration required	Inbound	Allow	SSH(22)	22/22	Address Field Access	0.0.0.0/0	1

Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
Classic	Internet							

- You have downloaded and installed the appropriate app:
  - The iOS device has SSH Control Lite installed.
  - The Android device has JuiceSSH installed.

Procedure

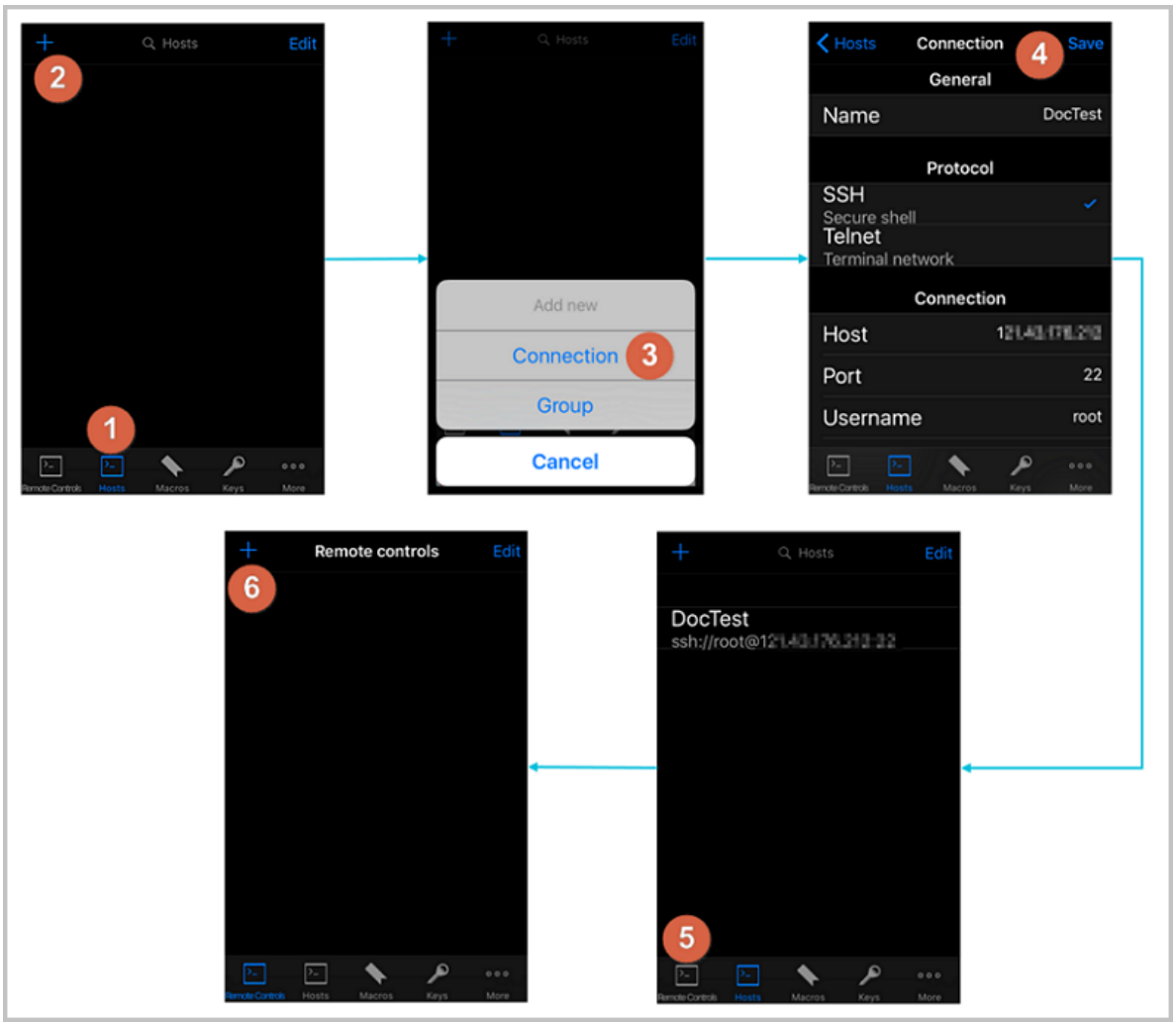
For iOS devices, see *Use SSH Control Lite to connect to a Linux instance*. In this example, user name and password are used for authentication.

For Android devices, see *Use JuiceSSH to connect to a Linux instance*. In this example, user name and password are used for the authentication.

Use SSH Control Lite to connect to a Linux instance

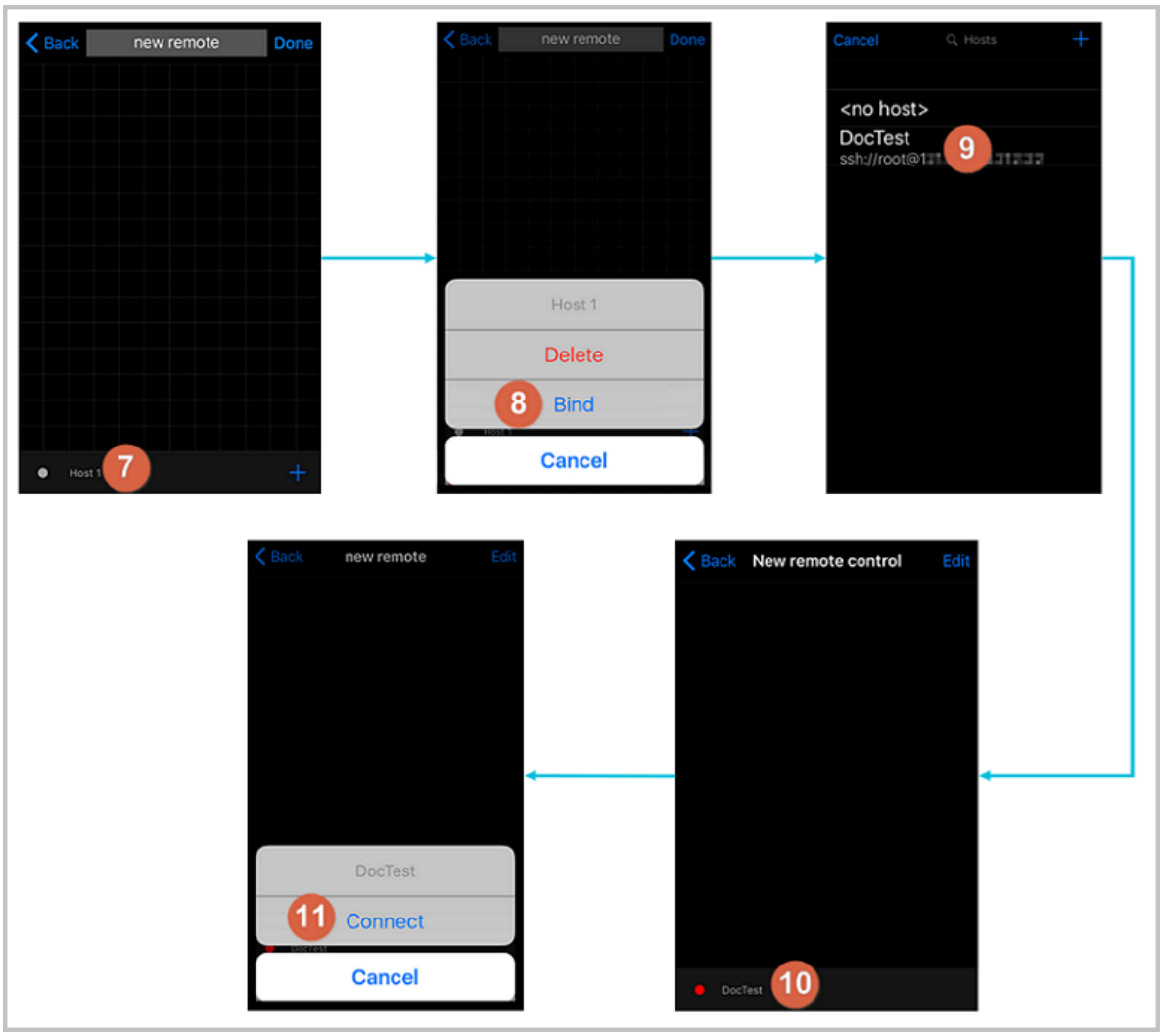
1. Start SSH Control Lite, and tap **Hosts**.
2. Tap the **+** icon in the upper left corner of the **Hosts** page.
3. In the action sheet, tap **Connection**.
4. On the **Connection** page, set the connection information and tap . The following connection information is required:
   - **`Name`**: Specify the Host name. `DocTest` is used in this example. .
   - **`Protocol`**: Use the default value SSH.
   - **`Host`**: Type the public IP address of the Linux instance to connect to.
   - **`Port`**: Type the port number for SSH protocol. 22 is used in this example.
   - **`Username`**: Type `root` for the user name.
   - **`Password`**: Type the logon password of the instance.
5. In the tool bar, tap **Remote Controls**.
6. On the **Remote Controls** page, tap the **+** icon in the upper left corner to create a remote connection session. `New remote` is used in this example.

   The following figure shows Steps 1 through 6.



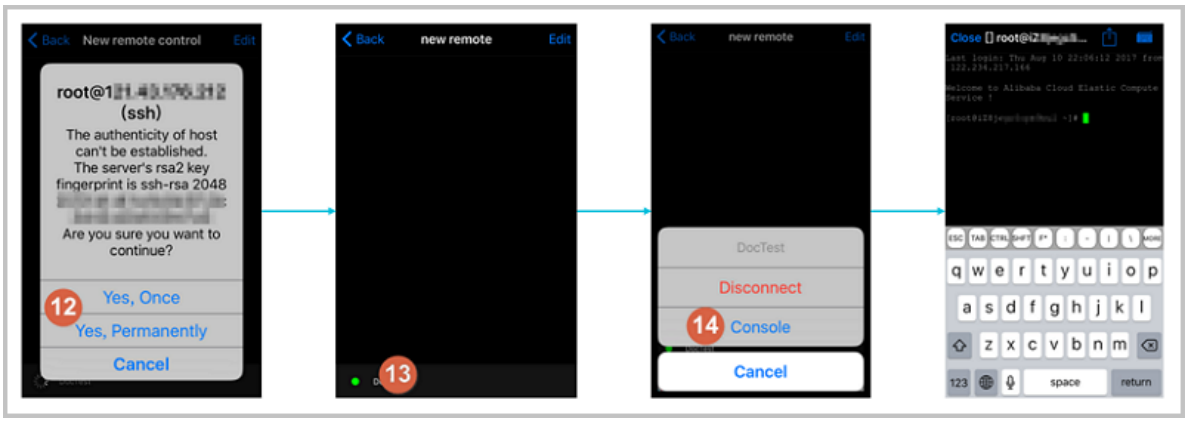
7. On the **New remote** page, tap **Host1**.
8. In the action sheet, tap **Bind**.
9. Select the new Linux instance. In this example, select `DocTest`.
10. On the **New remote** page, tap **Done** to switch it to the **Edit** mode, and then tap **DocTest**.
11. In the action sheet, tap **Connect**.

The following figure shows Steps 7 through 11.



12. In the action sheet, select **Yes, Once** or **Yes, Permanently**. Once the connection is successful, the indicator in front of **DocTest** turns green.
13. On the **New remote** page, tap **DocTest**.
14. In the action sheet, tap **Console** to open Linux instance console.

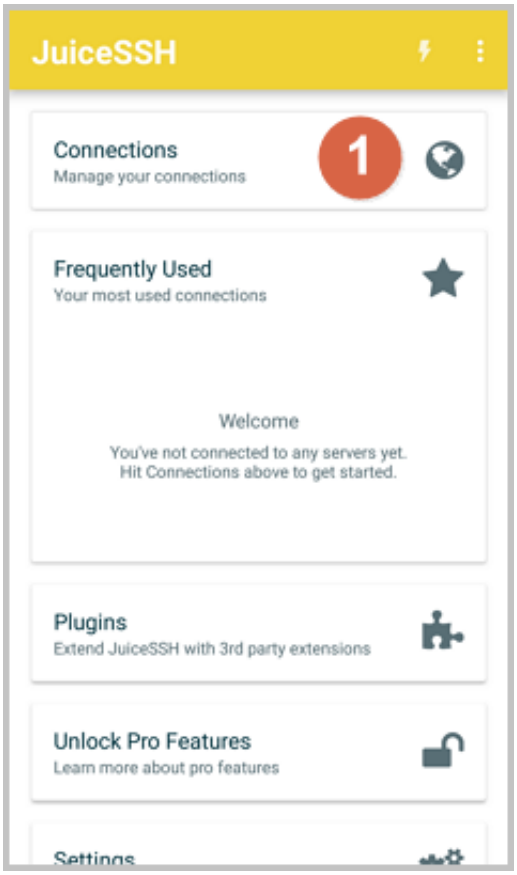
The following figure shows Steps 12 through 14:



Now, you are connected to the Linux instance.

Use JuiceSSH to connect to a Linux instance

1. Start JuiceSSH, and tap **Connections**.



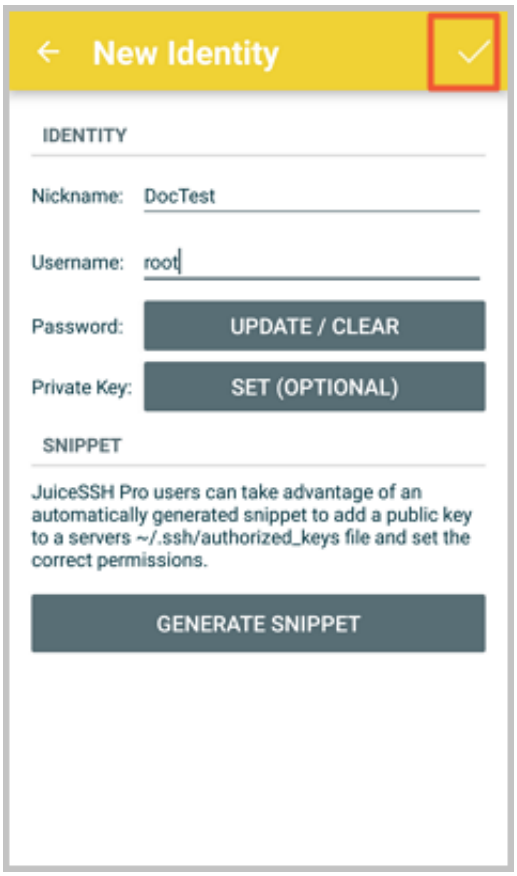
2. Under the **Connections** tab, tap the **+** icon.

3. On the **New Connection** page, add the connection information and tap the icon. The following connection information is required:

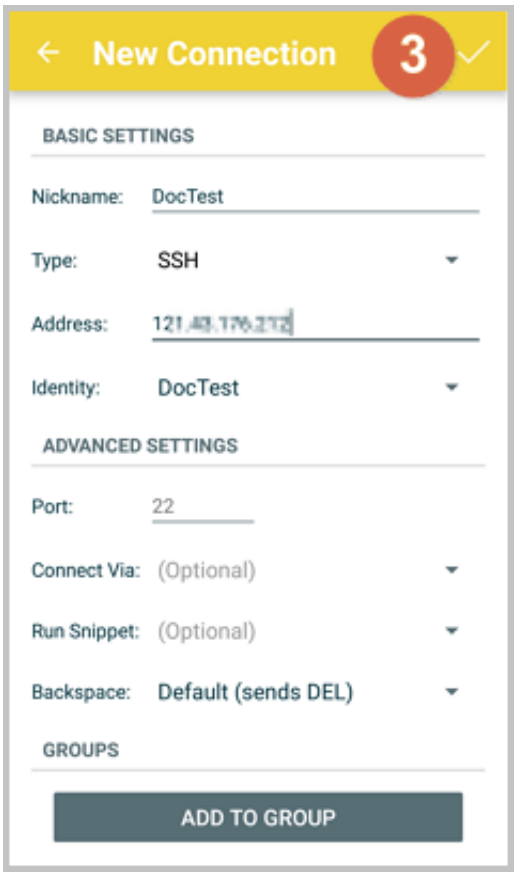
   - **`Nickname`**: Specify the name of the connection session. `DocTest` is used in this example.
   - **`Type`**: Use the default value SSH.
   - **`Address`**: Type the public IP address of the Linux instance to connect to.
   - To set**`I Identity`**, follow these steps:

     1. Tap **Identity**, and tap **New** in the drop-down list.
     2. On the **New Identity** page, add the following information and tap the icon. The following connection information is required:

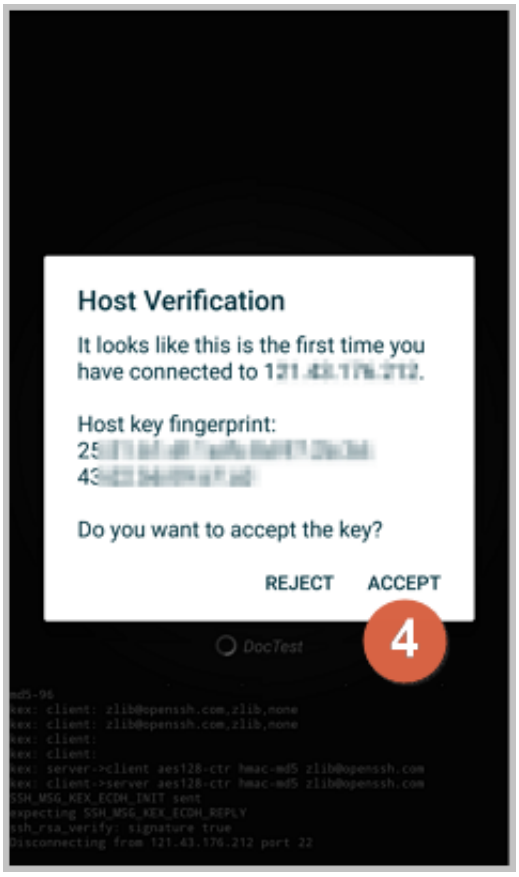
        - **`Nickname`**: Optional. You may set a nickname to ease management. `DocTest` is used in this example.
        - **`Username`**: Type `root` for the user name.
        - **`Password`**: Tap **SET(OPTIONAL)**, and type the logon password of the instance.



- **`Port`**: Type the port number for SSH protocol. In this example, 22 is used.

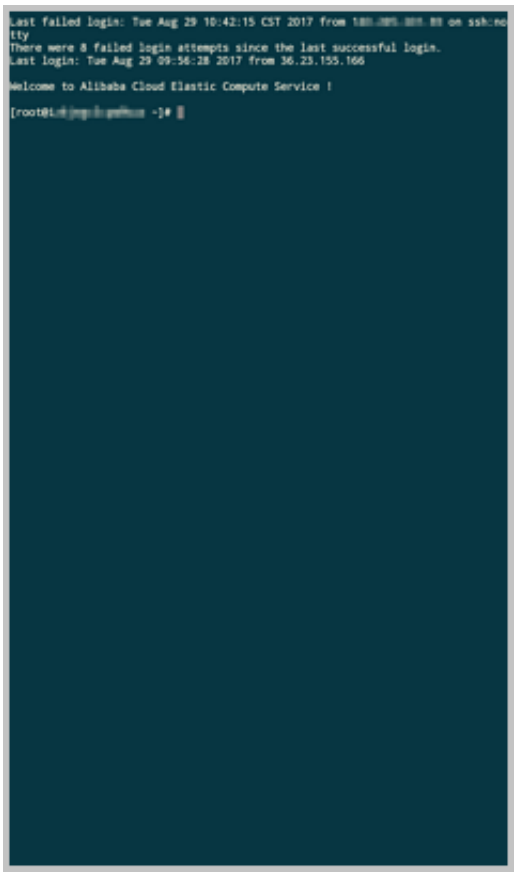


4. Confirm the message, and tap **ACCEPT**.



5. (Optional) For the first connection, the app would offer you some tips about font setting and the like. Confirm the message, and tap **OK - I'VE GOT IT!**.

Now, you are connected to the Linux instance.



Connect to Windows instances

In this section, we take Microsoft Remote Desktop as an example to describe how to use an app to connect to a Windows instance on a mobile device.

Prerequisites

Confirm the following before connecting to your instance:

- The instance is **Running**.
- The instance has a public IP address and is accessible from public network.
- You have set the logon password for the instance. If the password is lost, you must *reset the instance password*.
- The security group of the instance has *the following security group rules*:

Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
VPC	No configurat	Inbound	Allow	RDP(3389)	3389/3389	Address field access	0.0.0.0/0	1

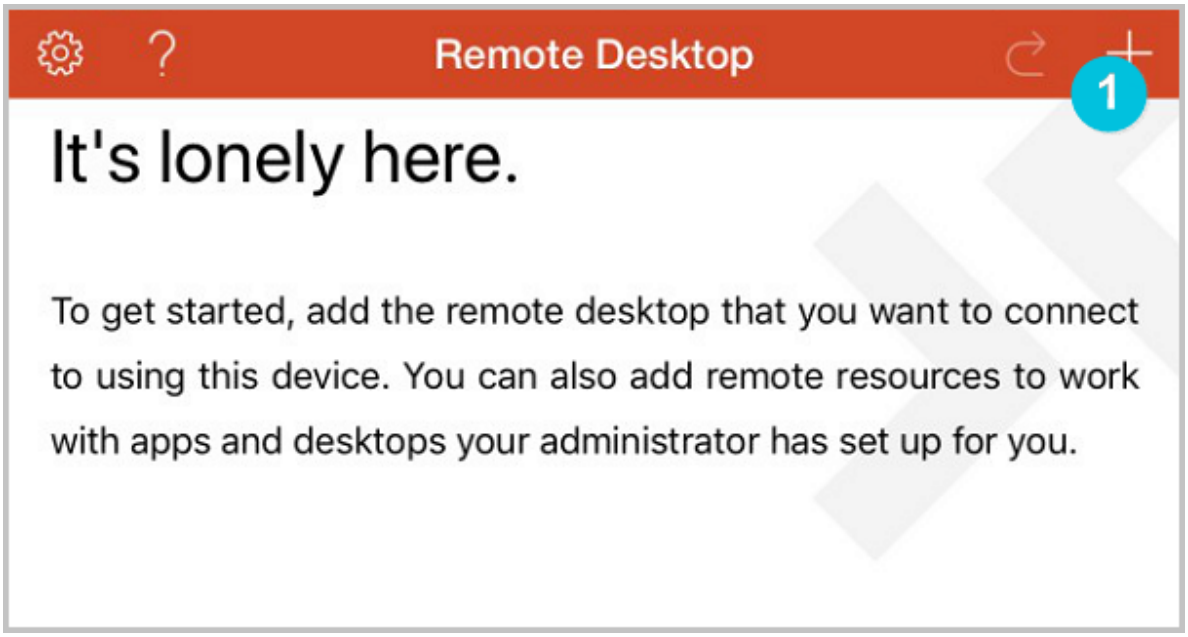
Network type	NIC	Rule direction	Authorization policy	Protocol type	Port range	Authorization type	Authorization object	Priority
	ion required							
Classic	Internet							

- You have downloaded and installed Microsoft Remote Desktop.
  - For iOS devices, download the app from iTunes.
  - For Android devices, download the app from Google Play.

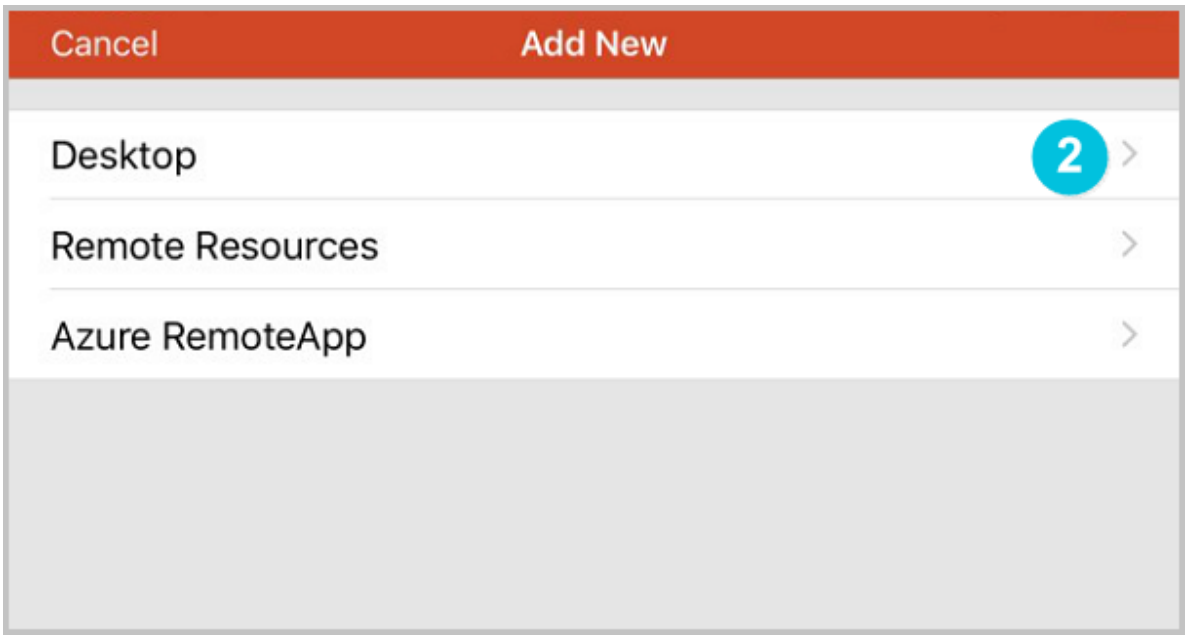
Procedure

To connect to a Windows instance by using Microsoft Remote Desktop, follow these steps:

1. Start RD Client. In the navigation bar, tap the **+** icon.

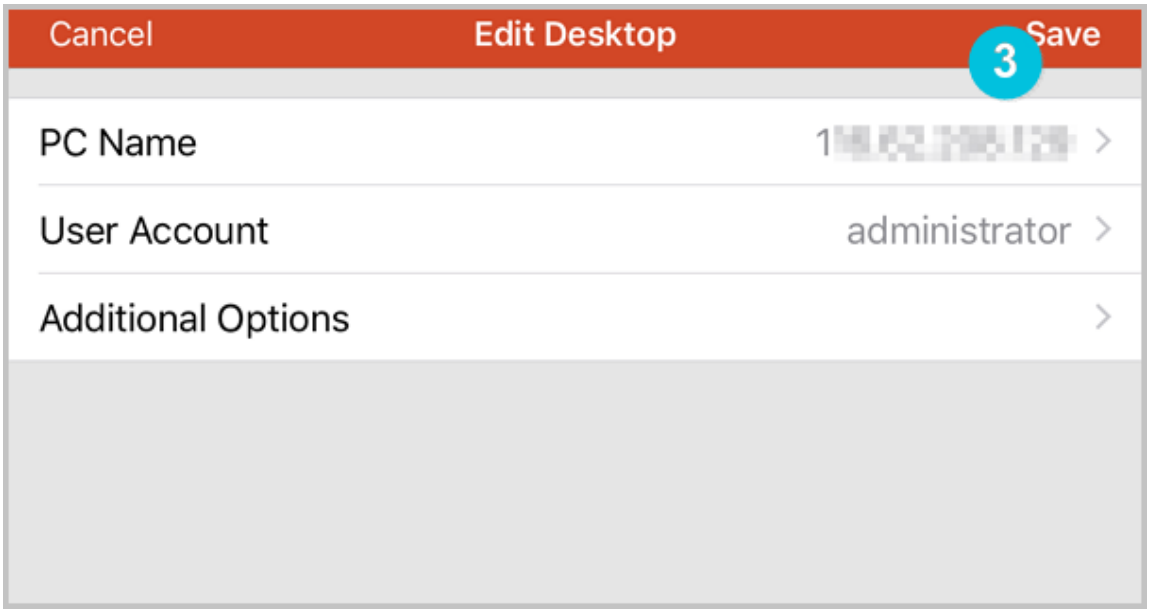


2. On the **Add New** page, select **Desktop**.

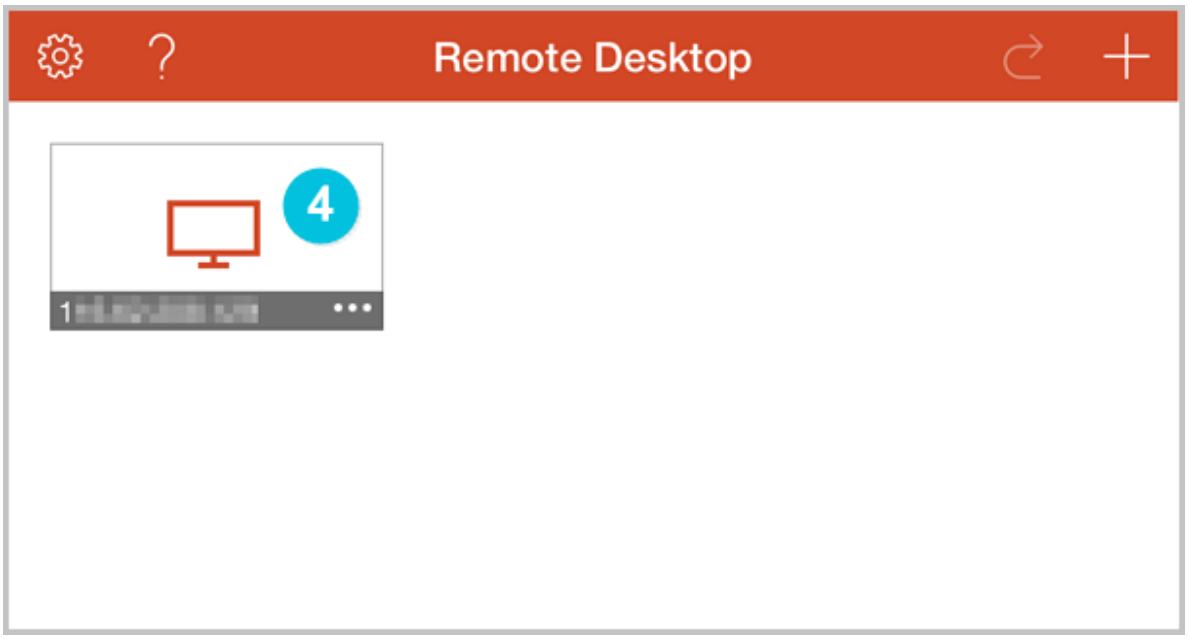


3. On the **Edit Desktop** page, type the connection information and tap **Save**. The following connection information is required:

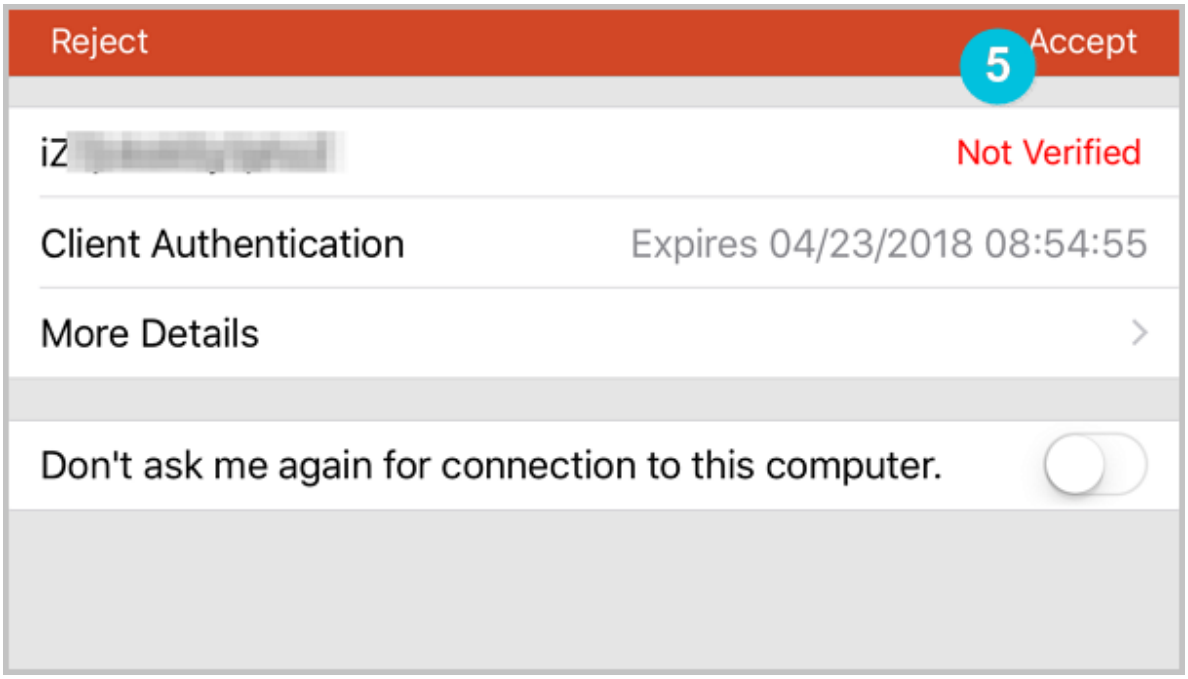
   - **`PC Name`**: Type the public IP address of the Windows instance to connect to.
   - **`User Account`**: Type the account name `administrator` and the logon password of the Windows instance.



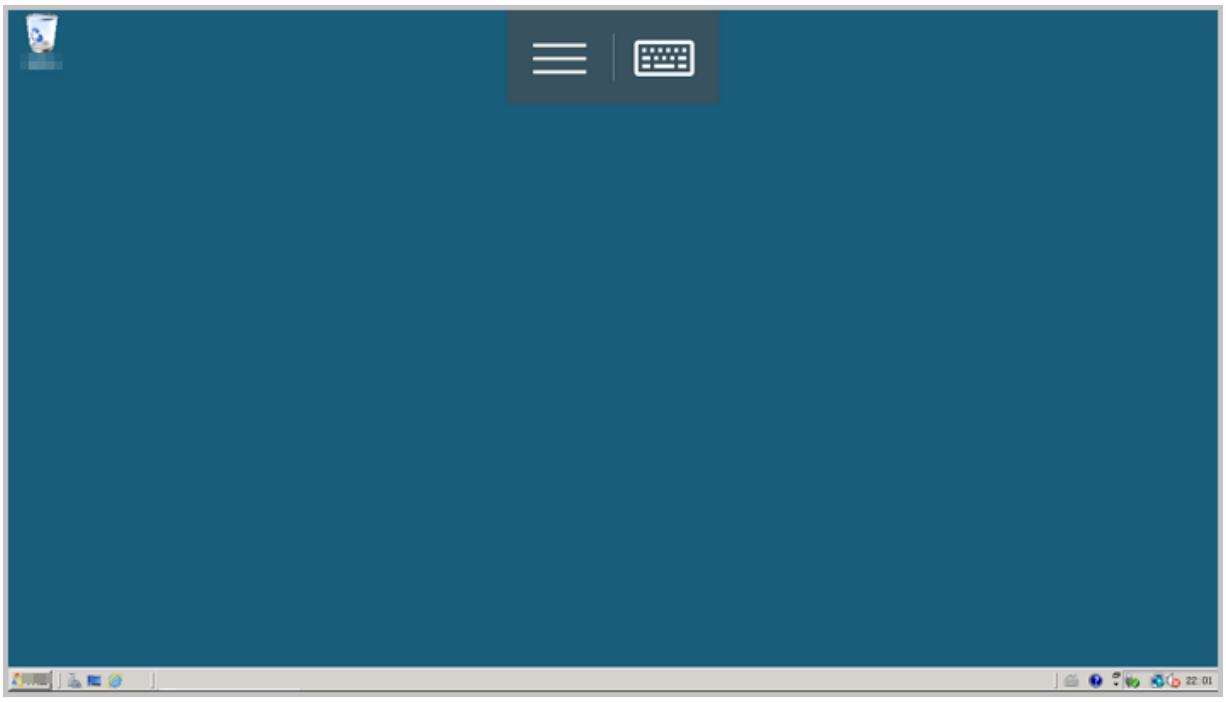
4. On the **Remote Desktop** page, tap the icon of a Windows instance.



5. On the confirmation page, confirm the message and tap **Accept**.



Now, you are connected to the Windows instance.



5 Cloud assistant

5.1 Create commands

You can use cloud assistance commands to perform routine tasks for ECS instances. These tasks include fast execution of automatic maintenance scripts, process polling, resetting of user password, installation and uninstallation of software, application update, and patch installation. Command types can either be Bat or PowerShell for Windows, or Shell for Linux.

Limits

- Within an Alibaba Cloud region, you can create at most 100 cloud assistant commands.
- A script cannot exceed 16 KB after Base64 encoding.

Create commands

To create a command on the ECS Console, take the following steps:

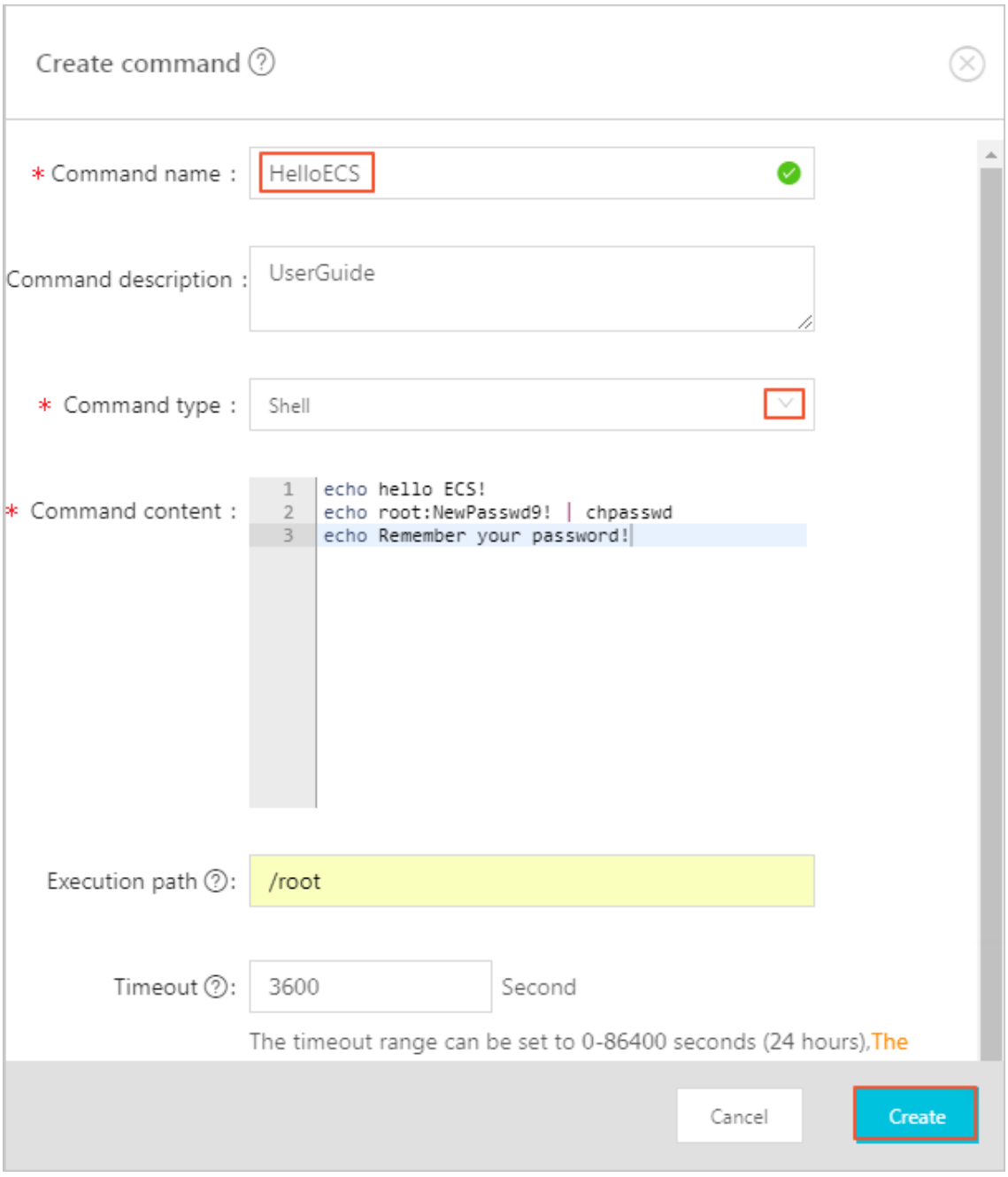
1. Log on to the ECS Console *ECS console* .
2. From the left-side navigation bar, select **Cloud Assistant**.
3. Select a region.
4. Click **Create Command**, and in the right-side pop-up window.
   a. Input a **command name**, such as HelloECS.
   b. Input a **command description**, such as UserGuide.
   c. Click the <x id="1"> icon, and select command type from the drop-down list. For Windows instances, you can select either **Bat** or **PowerShell**. For Linux instances, you must select **Shell**.
   d. Modify or paste the contents of your command, such as:

```
echo hello ECS!
echo root:NewPasswd9! | chpasswd
echo Remmember your password!
```

   e. Determine the **execution path** of the command. The execution paths of Bat and PowerShell commands are by default set to the directory where the cloud assistant client is stored, such as `C:\ProgramData\aliyun\assist\$(version)`. Shell commands are by default in the `/root` directory.
   f. Set the maximum timeout time (in seconds) for commands in an instance. The default value is set to 3600s. When a command you created cannot be run for some reason, the

command times out. After the command times out, the command process will be forcibly terminated.

g. After confirming the command, click **OK**.



You can also use the ESC API *CreateCommand* to create a cloud assistant command.

Next step

Invoke commands

5.2 Run commands

After creating a cloud assistant command, you can run the command on one or more instances. The command execution status and results for each instance are not influenced by the same command being run on other instances. You can also configure the execution interval for the command.

Limits

- In one Alibaba Cloud region, you can run a maximum of 500 cloud assistant commands in a single day.
- You can run a command on a maximum of 50 instances at once.
- The status of the target instance must be **In Progress** (`Running`).
- The target instance must have *cloud assistant client* installed.
- The target instance must be *VPC-Connected*.
- The period for running cloud assistant commands cannot be less than 10 seconds.
- The scheduled time for periodic command execution is set to China Standard Time (UTC +08 :00) based on the system time obtained from the ECS instances. Make sure that the time or time zone of your ECS instance is consistent with your own expectations.

Run commands

To execute a command on the ECS console, take the following steps:

1. Log on to the ECS console*ECS console* .
2. Select **Cloud Assistant** from the left-side navigation pane.
3. Select a region.
4. Search for the Cloud Assistant command you want to run. Select **Execute** from the right-side **Actions**. In the right-side pop-up window:
   a. Click **View Command Content** to confirm the command contents.
   b. Click **Select Instance**. In the pop-up window:
      A. Select one or more instances.
      B. Click  to select an instance.

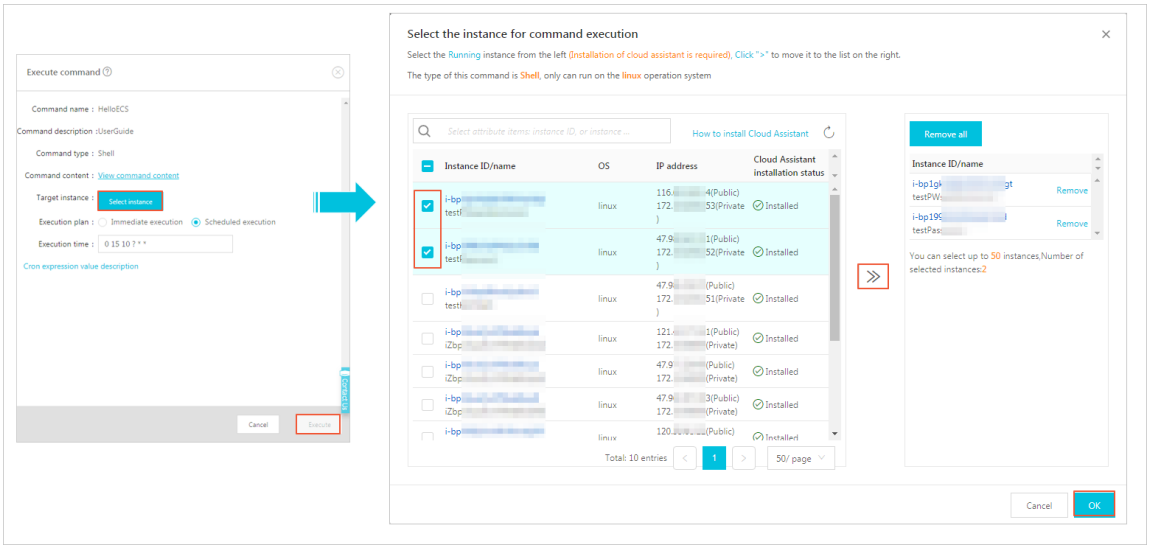
Note:
Bat or PowerShell commands can only be selected for Windows instances, and Shell commands can only be selected for Linux instances. All instances must have the Cloud

> Assistant Client **installed**. Otherwise, the instance cannot be selected even after you click the icon.

C. Click **OK**.

c. Select **Immediate Execution** or **Scheduled Execution**:

- **Immediate Execution**: The cloud assistant will run the command immediately on the instances once.
- **Scheduled Execution**: Use the cron expression to run the command periodically. Fill in the **Execution Time**. For more information, see *Cron Expression Value Description*.



5. Click **Execute**.

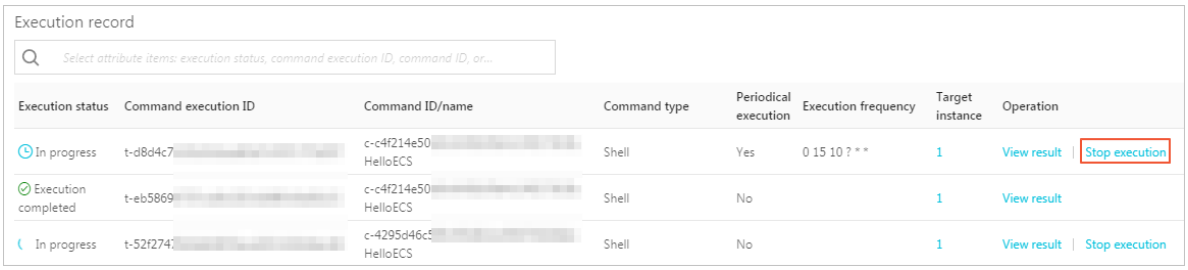
You can also use the ECS API *InvokeCommand* to execute a cloud assistant command.

Stop command execution

Prerequisite: Either it must be a periodic command, or the command must have a command execution status of **Running** (`Running`).

To stop a command on the management console, take the following steps:

1. Log on to the management console *ECS console* .
2. Select **Cloud Assistant** from the left-side navigation pane.
3. Select a region.
4. In the **Execution Record** area, search for the command you need to stop, and select **Stop Command** from **Actions**.



Next step

Query execution results and status

5.3 Query execution results and status

There is no difference between running a cloud assistant command on the console and running a command while logged into the instance. In both cases, a command can be run successfully only after all of the command's conditions are satisfied. Cloud assistant commands executed at the same time can provide different command execution results and statuses if the following errors occur: lack of relevant dependencies, network disruptions, command semantic errors, script debugging errors, or abnormal instance statuses. We recommend that you review the command execution results and status after running a command to ensure the target operation has completed properly.

Prerequisites

The command must be run at least once.

Check the results of the command execution

To view command execution result on the ECS Console, you must take the following steps:

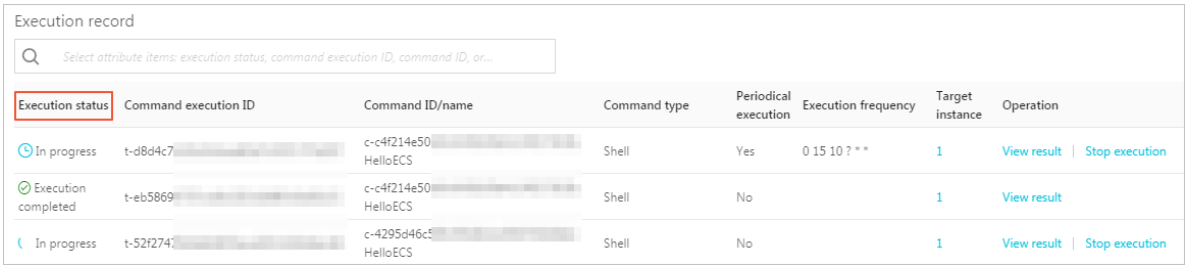
1. Log on to the ECS Console*ECS console* .
2. In the left-side navigation bar, select **Cloud Assistant**.
3. Select a region.
4. In the **Execution Record** area, search for the execution record of the necessary command execution, and select **View Results** from **Actions**.
5. In the pop-up window, select an execution record and click  to expand the command execution record.

You can also use the ECS API *DescribeInvocationResults* to view command results.

View command execution status

To view command execution status in the ECS Console, you must take the following steps:

1. Log on to the ECS Console *ECS console* .
2. In the left-side navigation bar, select **Cloud Assistant**.
3. Select a region.
4. In the **Execution Record** area, search for the execution record of the necessary command execution, and then in the **Execution Status** bar view the command execution status.



You can also use the ECS API *DescribeInvocations* to view command execution status.

5.4 Manage commands

After creating cloud assistant commands, you can set the command name and description, clone commands, or delete unnecessary commands to guarantee a sufficient command quota.

Modify the name and description of a command

To set the command name and description in the ECS console, perform the following steps:

1. Log on to the *ECS console* .
2. Select **Cloud Assistant** from the left-side navigation pane.
3. Select a region.
4. Move the mouse cursor to the command you want to edit, and click the icon that appears in the prompted window.
   - **Command name**: Input the new command name.
   - **Command description**: Input the new command description.
5. Click **OK**.

You can also use the ECS API *ModifyCommand* to modify command information.

Clone a command

The clone command is equivalent to add a new version for an existing cloud assistant command. You can retain all the information of the cloned command as it was previously. Alternatively, you can set a new name, description, type, content, execution path, or timeout time for it. To clone a command in the ECS console, perform the following steps:

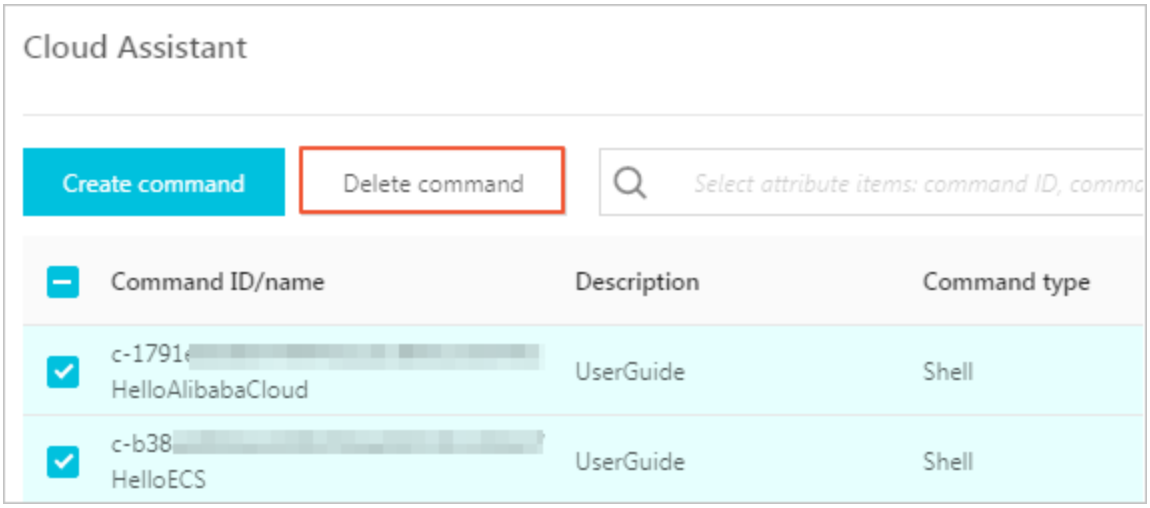
1. Log on to the *ECS console* .
2. Select **Cloud Assistant** from the left-side navigation pane.
3. Select a region.
4. Find the cloud assistant command you want to clone, and from the **Operation** list, click **Clone**.
5. In the **Clone command** dialogue box, complete the following optional steps:
   a. Enter a new **Command name**, such as HelloECS.
   b. Enter a new **Command description**, such as UserGuide.
   c. Click the icon  to replace the command type from the drop-down list. For Windows instances, you can select **Bat** or **Power Shell**. For Linux instances, you can select **Shell**.
   d. Edit or paste new command content.
   e. Determine a new command **Execution path**. The default execution path for Bat or PowerShell commands is the directory where the cloud assistant client is installed, such as `C:\ProgramData\aliyun\assist\$(version)`. The default execution path for Shell commands is the `/root` directory.
   f. Configure the timeout time in seconds for the command. The default value is set to 3600 . When a command you created cannot be executed for the amount of time set by this parameter, the command times out. When the timeout time of the command expires, the command process will be forcibly terminated.
   g. After you confirm the modification, click **Create**.

Delete commands

Within an Alibaba Cloud region, you can create a maximum of 100 cloud assistant commands. We suggest that you regularly clean your commands to guarantee a sufficient command quota. To delete a command on the ECS console, perform the following steps:

1. Log on to the *ECS console* .
2. Select **Cloud Assistant** from the left-side navigation pane.
3. Select a region.

4. Locate the cloud assistant command you want to delete:
   - To delete a single command, from the **Operation** list, select **Delete**.
   - To delete multiple commands, select the target instances, and click **Delete command**.



5. In the **Delete command** dialogue box, click **OK**.

You can also use the ECS API *DeleteCommand* to delete commands.