

Workspace

Quick Start

Issue 01
Date 2023-04-03



Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI 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.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

Contents

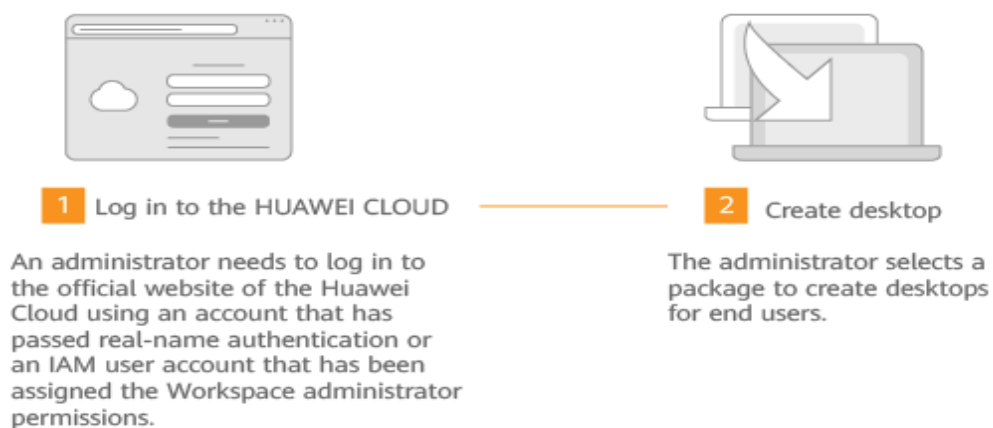
1 Operation Process.....	1
2 Preparations.....	3
3 Logging In to the Workspace Console.....	4
4 Purchasing a Desktop.....	6
4.1 Methods of Purchasing Desktops.....	6
4.2 Purchasing Yearly/Monthly-billed Desktops.....	6
4.3 Purchasing Yearly/Monthly-billed Desktop Pools.....	17
4.4 Purchasing Pay-per-Use Desktops.....	29
4.5 Purchasing Pay-per-Use Desktop Pools.....	39
5 Logging In to a Desktop.....	51
5.1 Using a Thin Client.....	51
5.2 Using a Soft Client.....	56
5.3 Using a Mobile Terminal.....	65
5.4 Logging In to a Desktop Using a Browser.....	70
A Change History.....	73

1 Operation Process

Operation Process for Administrators

An administrator can log in to the official website of the Huawei Cloud using a Huawei Cloud account that has passed the real-name authentication or an IAM account that has been assigned the Workspace administrator permissions to buy desktops, as shown in [Figure 1-1](#).

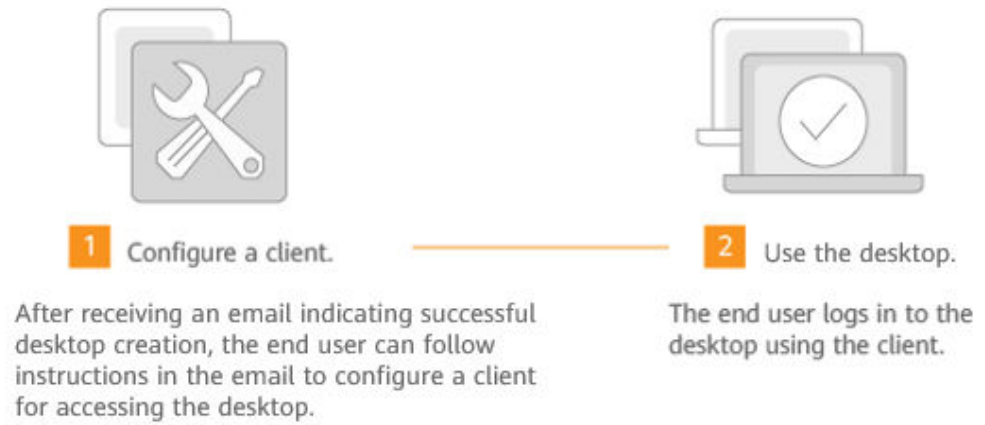
Figure 1-1 Operation process for administrators



Operation Process for End Users

End users can use Workspace desktops after completing basic configurations on clients, as shown in [Figure 1-2](#).

Figure 1-2 Operation process for end users



2 Preparations

Before using Workspace, you need to complete the preparations described in this document.

- [Registering a Huawei Account and Completing Real-Name Authentication](#)
- [\(Optional\) Creating an IAM User](#)

Registering a Huawei Account and Completing Real-Name Authentication

If you already have a Huawei account, skip this step. If you do not have a Huawei account, perform the following operations to create one:

- Step 1** Visit the [Huawei Cloud official website](#).
- Step 2** Click **Register** in the upper right corner and complete the registration as instructed.
- Step 3** After the registration, the system automatically redirects you to your personal information page.
- Step 4** Complete real-name authentication for individual or enterprise accounts. For details, see [Real-Name Authentication](#).

----End

(Optional) Creating an IAM User

If you have registered on Huawei Cloud, you can create an IAM user on the IAM console. For details, see [Creating an IAM User](#).

3 Logging In to the Workspace Console

Scenarios

Log in to the console and perform the following operations:


- Purchasing and managing cloud desktops: purchases and manages cloud desktops on the console
- Querying desktop information: queries details about desktop usage
- Managing end users: creates users, modifies user information, changes email addresses, resets passwords, resends notification emails, unlocks users, and deletes accounts on the console
- Managing policies: provides the protocol policy management function. Customers can configure policies to help users better use desktops.

Procedure

Step 1 Log in to the console as the administrator.

 **NOTE**

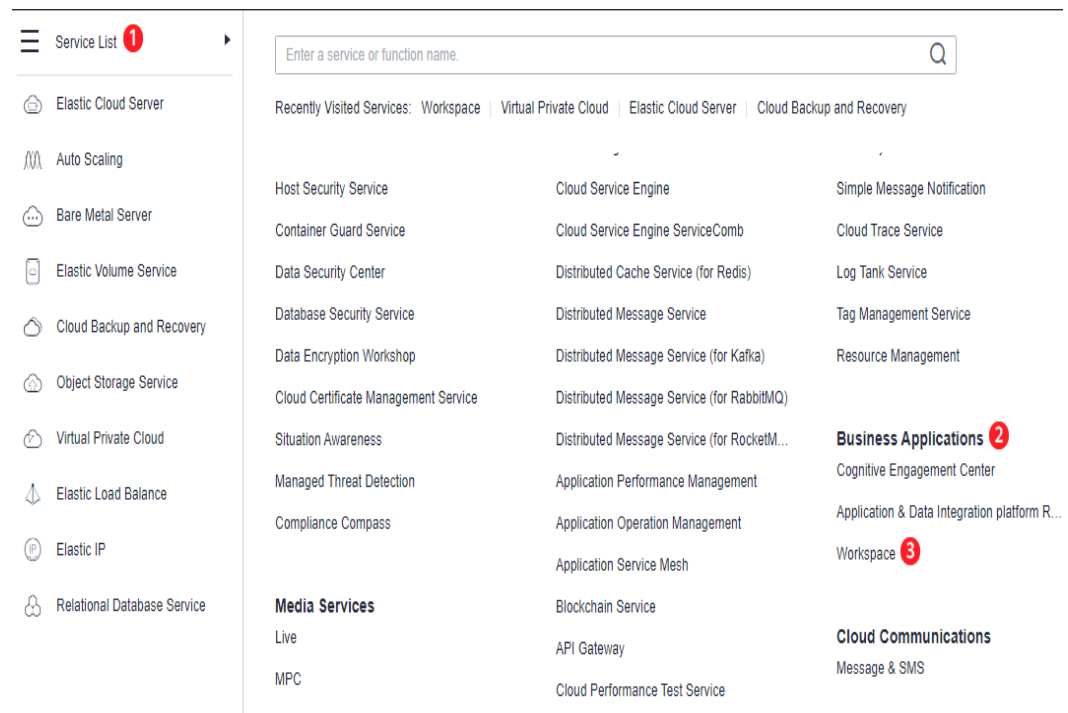
The administrator account can be the Huawei account that has passed real-name authentication in [Preparations](#), or the account of the IAM user assigned the Workspace administrator permissions in [Preparations](#).

Step 2 Click  in the upper left corner of the console and select a region and a project.

Step 3 Click  and choose **Business Applications** > **Workspace** in the service list.

The Workspace console is displayed, as shown in [Figure 3-1](#).

Figure 3-1 Workspace console



----End

4 Purchasing a Desktop

4.1 Methods of Purchasing Desktops

This section describes how to purchase a desktop.

You can purchase desktops using either of the following methods:

- **Yearly/Monthly** is a prepaid billing mode. You will be charged based on the usage duration that you specified.
- **Pay-per-use** is a postpaid billing mode. You will be charged based on the actual usage duration of desktops. This mode is recommended when desktop requirements fluctuate. You can purchase or delete desktops at any time.

4.2 Purchasing Yearly/Monthly-billed Desktops

Scenarios

An administrator can select the yearly/monthly billing mode and packages, and assign desktops to end users. After the administrator purchases a desktop, the system automatically sends a notification email to the user's mailbox.

Purchase Page

Step 1 [Logging In to the Workspace Console](#)

Step 2 On the **Dashboard** or **Desktop Management** page, click **Buy Desktop**.

The page for buying desktops is displayed.

----End

Basic Configurations

Step 1 Determine whether to connect to an existing Windows AD domain of the enterprise.

NOTICE

After you purchase a desktop for the first time, your selection (connecting to the Windows AD domain or canceling the connection to the Windows AD domain) cannot be changed. Exercise caution when performing this operation.

- If you select **No**, you can directly configure the desktop infrastructure by referring to [Step 2](#). After the desktop creation task is submitted, the Workspace service will be deployed.


After subscribing to the service, you can use the account authentication system of Huawei to authenticate users and manage user accounts on the Workspace console.

- Select **Yes** to configure the Windows AD domain. For details, see [Connecting to the Windows AD Domain](#). After the configuration information is saved, the Workspace service will be deployed.

After the service is subscribed, the existing unified AD of the enterprise is used to authenticate users and manage user accounts.

Step 2 Configure desktop information, as described in [Table 1 Desktop information](#).

Table 4-1 Desktop information

Parameter	Description	Example Value
Billing Mode	Select Yearly/Monthly .	Yearly/Monthly
Region	Desktops in different regions cannot communicate with each other over the intranet, and desktops need to be managed by region. You are advised to create desktops in the same region. NOTE A region is the location of the physical data center of Workspace. Different regions indicate different physical distances between the physical data center and users, as well as different network latency. To reduce latency and improve access speed, select the region closest to your workloads.	-
Project	Select a project as required. NOTE If no project is available, click  and choose Create Project . On the displayed page, create a subproject by referring to Creating a Subproject .	-

Parameter	Description	Example Value
AZ	An AZ is a physical region where resources use independent power supplies and networks. AZs are physically isolated but connected through an intranet. If an AZ becomes faulty, other AZs in the same region will not be affected. NOTE To achieve better disaster recovery, you are advised to create desktops in different AZs.	Random
CPU Architecture	Select the x86 architecture.	x86
Package Type	Select specifications as required.	Ultimate Ultimate 2 vCPUs 4 GB

Step 3 Configure an image.

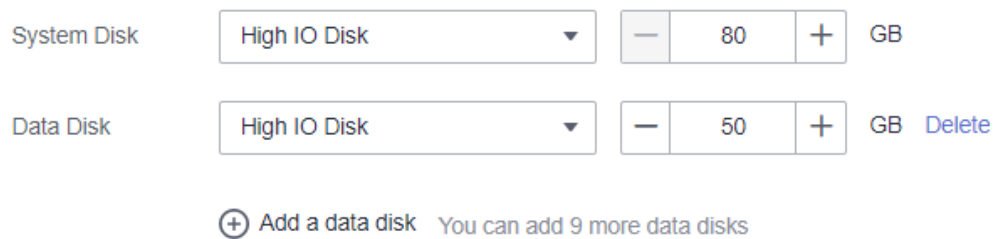
- **Image Type:** Select an image type as required.

 **NOTE**

- A public image is a widely used standard image provided by Workspace. It contains an OS and pre-installed public applications and is visible to all users. Public images are very stable and their OS and any included software have been officially authorized for use. If a public image does not contain the application environments or software you need, you can use a public image to create an application environment and then deploy required software. Currently, Windows public images are marketplace images.
 - A private image is created based on an existing cloud desktop or external image file and is visible only to the user who created it. It contains an OS, preinstalled public applications, and the user's personal applications. Using a private image to create a desktop saves more time.
 - Workspace supports public images running Windows, private images converted from desktops generated using Windows images, and private images converted from ECSs created using Windows image files. To use a private image to purchase a desktop, see [Converting a Desktop to an Image](#) and [Creating a Windows Desktop Private Image](#).
- **OS:** Select an OS type in the [supported OS list](#).

Step 4 Configure disks as required, as shown in [Figure 4-1](#).

Figure 4-1 Configuring disks



NOTE

- For details about the performance of different disk types, see [EVS Overview](#).
 - High I/O disks use serial attached SCSI (SAS) drives to store data.
 - Ultra-high I/O disks use solid state disk (SSD) drives to store data.
 - General purpose SSD disks use SSD drives to store data.
- After the desktop is created, you will be billed for the disk until the desktop is deleted.
- The disk size must be an integer multiple of 10.
- A maximum of 10 data disks can be configured.

Step 5 Set the required duration and evaluate the fee.

Set the required duration. The fee for one desktop is displayed here. If the selected

duration is marked with , it indicates that the selected package has a discount within the time range. Click **Discount Details** to view the discount details.

Step 6 Click **Next: Configure advanced settings**.

The page for configuring advanced settings is displayed.

----End

Advanced Settings

Step 1 (Optional) Configure an enterprise ID.

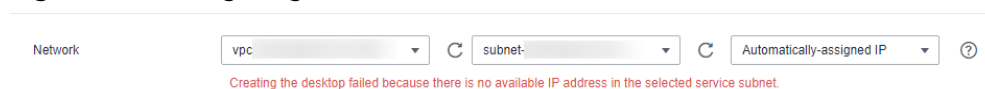
You are advised to use identifiable fields such as the enterprise name pinyin as the enterprise ID.

NOTE

- Customize an enterprise ID or use a randomly-generated ID upon the first purchase.
- Enterprise ID is the unique identifier of your tenant environment. End users need to enter the enterprise ID when logging in to the system.
- The enterprise ID can contain a maximum of 32 characters, including digits, letters, underscores (_), and hyphens (-).

Step 2 Configure the network.



Figure 4-2 Configuring the network



NOTICE

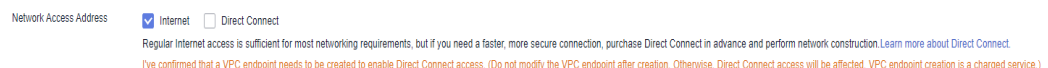
The 172 network segment is reserved for running internal services. Therefore, do not select a VPC network starting with 172. Otherwise, desktops cannot be purchased.

The resources required by Workspace will be created in the selected VPC subnet. After the desktop is purchased for the first time, the VPC cannot be modified, and only the service subnet can be managed.

- Configure the existing network.
Click  and select a service subnet. If you purchase a desktop for the first time, you need to select a VPC and a service subnet. For details about how to create a VPC and a service subnet, see [Creating a VPC and a Service Subnet](#).
- Configure a new network.
 - Click **Click here to manage subnets**. In the displayed **Modify the service subnet** dialog box, click **Create on Console** to create a service subnet. For details, see [Creating a Service Subnet for the VPC](#).
 - If you purchase a desktop for the first time, click **Create on Console** to create a VPC and a service subnet. For details, see [Creating a VPC and a Service Subnet](#).
 - Click  and configure the IP address type as required.
 - Automatically assign an IP address.
 - Manually assign an IP address.
 - Use an existing elastic network interface.

Step 3 Configure the network access mode, as shown in [Figure 4-3](#). By default, **Internet** is selected. You can select multiple options.

Figure 4-3 Network access

**NOTE**

- Internet access is sufficient for most networking requirements, but if you need a faster, more secure connection, purchase Direct Connect in advance and implement networking. [Learn more about Direct Connect](#). Load balancers will be automatically created when Direct Connect access is enabled. (Do not modify the load balancers.)
- Direct Connect network segment configuration: Enter the network segment where the desktop client (such as TC) is located. You can enter multiple network segments and separate them with semicolons (;).

Step 4 Configure an EIP for network access.

- **Buy now**
 - **By Bandwidth:** applicable when the traffic is heavy or stable and the bandwidth ranges from 1 Mbit/s to 200 Mbit/s. You can customize the bandwidth as prompted.

 **NOTE**

Specify the bandwidth upper limit. You are charged based on the actual outbound traffic, regardless of the usage duration.

- **By Traffic:** applicable when the traffic is small or fluctuates greatly and the bandwidth size ranges from 5 Mbit/s to 200 Mbit/s. You can customize the bandwidth as prompted.

 **NOTE**

You are charged based on the purchased duration and bandwidth size.

- **Use existing:** Bind an existing EIP to the desktop.
- **Not required:** To enable desktop Internet access, go to **Internet Access Management** on the Workspace console.

Step 5 Click **Next:Assign desktops**.

The page for assigning desktops is displayed.

----End

Assigning Desktops

Step 1 Select the user import mode and configure information of the user to whom a desktop is to be assigned.

 **NOTE**

If an existing AD domain is used, you need to create users on the AD server before assigning desktops.

Select **Manual** or **Batch** as required, as shown in [Table 4-2](#).

Table 4-2 Desktop assignment

User Authorization Mode	Parameter	Operation
Desktop Assignment Type	<ul style="list-style-type: none"> • Manually 	Select Select User or Create User .

User Authorization Mode	Parameter	Operation
	<ul style="list-style-type: none"> ● Batch 	<ol style="list-style-type: none"> 1. Select Batch. 2. Locate the row that contains Import User List, and click Download a user list template. 3. Enter the serial number, username, permission group, and desktop name in the table as required. 4. Click Upload to upload the user list that has been filled in as required. <p>NOTE The size of the file to be uploaded cannot exceed 1 MB. The username and desktop name must be different.</p>
	<ul style="list-style-type: none"> ● Not assigned <p>NOTE</p> <ul style="list-style-type: none"> - If you purchase one desktop, the desktop name is the name of the desktop. - When multiple desktops are purchased, the desktop name prefix is used to generate desktop names in ascending order. For example, if the prefix is desktop and you create three desktops, the names of the created desktops are desktop01, desktop02, and desktop03. - To assign a desktop to a user, select the desired desktop on the desktop management page and choose More > Assign users. 	<ol style="list-style-type: none"> 1. Select Not assigned. 2. Enter the name of the desktop that is not assigned to a user based on site requirements.

User Authorization Mode	Parameter	Operation
User Authorization	When selecting users, you can search for activated users by setting filter criteria.	<ul style="list-style-type: none"> • You can search for a user/group based on the user/group name. • Select the target username and click OK.

User Authorization Mode	Parameter	Operation
	<p>Create user > User Activation > Manual Input</p> <ul style="list-style-type: none"> ● Username is used for user authentication during desktop login. Rules for naming a username: <ul style="list-style-type: none"> - The name can contain 1 to 20 characters. - A name containing only digits is allowed. - The name can contain uppercase letters, lowercase letters, digits, periods (.), hyphens (-), and underscores (_), and must start with a lowercase letter or uppercase letter. - The value cannot be empty. ● Email is used to receive desktop provisioning emails and related notifications. Rules for verifying an email address: <ul style="list-style-type: none"> - Enter a valid email address through system verification. - The value can contain a maximum of 64 characters. - The value cannot be empty. ● The mobile number is used to receive desktop provisioning emails and related notifications. Rules for verifying a mobile number: <ul style="list-style-type: none"> - <i>[+][Country/Region code][Mobile number]</i> - For a mobile number in the Chinese mainland, you can omit <i>[+][Country/Region code]</i> and directly enter the mobile number. - The mobile number can contain spaces, slashes (/), and hyphens (-). 	<ul style="list-style-type: none"> ● Configure the user information, description, and account expiration settings as prompted. ● Click Add User. NOTE Enter the email address or mobile number, or both. ● Permission groups can be configured in batches. ● The desktop name is automatically generated. ● Click Add Desktop to add a desktop. ● Configure the number of desktops as prompted.

User Authorization Mode	Parameter	Operation
	<p>Create user > Manager Activation > Manual Input</p> <ul style="list-style-type: none"> • Username is used for user authentication during desktop login. Rules for naming a username: <ul style="list-style-type: none"> - The name can contain 1 to 20 characters. - A name containing only digits is allowed. - The name can contain uppercase letters, lowercase letters, digits, periods (.), hyphens (-), and underscores (_), and must start with a lowercase letter or uppercase letter. - The value cannot be empty. • The initial password is authenticated when a user logs in to the desktop. Keep the initial password secure. <ul style="list-style-type: none"> - The password contains 8 to 32 characters. - The value can contain letters, digits, and the following special characters: !@\$%^-_=+[{ }];,./? - The password cannot be the username or the reverse username. <p>NOTE If your tenant connects to an AD domain, Manager Activation is unavailable by default.</p>	

User Authorization Mode	Parameter	Operation
	Create user > Manager Activation > Batch Import <ul style="list-style-type: none"> Upload the users recorded in the table and create them in batches. 	<ol style="list-style-type: none"> Click Download Template on the right of Import user information to download the user list template. Enter the serial number, username, email address, mobile number, expiration time, and description in the table as required. Click Upload to upload the user list that has been filled in as required. Confirm the creation. <p>NOTE The size of the file to be uploaded cannot exceed 1 MB. A maximum of 200 records can be uploaded at a time. Only .xlsx and .xls files are supported.</p>
	Create user > User Activation > Batch Import <ul style="list-style-type: none"> Upload the users recorded in the table and create them in batches. 	

Step 2 Click **Next: Confirm the settings**.

The confirmation page is displayed.

----End

Confirming the Settings

Step 1 Select **Enterprise Project** as needed.

 **NOTE**

You can use an enterprise project to centrally manage your cloud resources and members by project.

Step 2 Set the duration as required.

Step 3 (Optional) Select **Auto renewal** if needed.

 NOTE

- Note the [auto-renewal rules](#) when enabling auto-renewal.
- Auto-renewal duration:
 - **Monthly:** You can renew the subscription for one month each time. The number of renewal times is not limited.
 - **Yearly:** You can renew the subscription for one year each time. The number of renewal times is not limited.

Step 4 Read the disclaimer and select **I have read and agree to the Image Disclaimer**.

Step 5 Click **Buy Now**.

The page for purchasing desktops is displayed.

Step 6 Check the cloud order service and the fee to be paid.

Step 7 After you select a payment method and pay for your order, the desktop has been purchased.

After the desktop is provisioned, administrators can view the purchased desktop in the desktop list.

----End

Follow-up Operations

- The login details for the newly created desktop will be emailed to the end user. The end user can activate the account, download the client, and configure and use the desktop as instructed. Administrators can restrict desktop network interaction as required. For details, see [Configuring Workspace to Access the Public Network](#) and [Configuring Workspace to Access the Intranet](#).
- If a Windows AD domain has been connected and an OU has been created on the Windows AD server, create the OU on the console by referring to [OU Management](#).
- For details about performing auto-renewal on the console, see [Auto-renewal](#).

4.3 Purchasing Yearly/Monthly-billed Desktop Pools

Scenarios

An administrator can select the yearly/monthly billing mode and packages to purchase desktop pools.

Purchase Page

Step 1 [Logging In to the Workspace Console](#)

Step 2 On the **Desktops** page, choose **Desktop Pools** and click **Purchase Desktop Pool**.

The page for buying desktop pools is displayed.

 **NOTE**

When you purchase a desktop pool for the first time, the system prompts you to perform authorization.

- **IMS permissions**
Workspace supports image creation. Therefore, the permission to access IMS is required.
- **Administrator permissions for related cloud services**
Workspace supports scheduled disk recomposing and auto scaling. Therefore, the tenant administrator permissions are required.
- **VPC service permissions**
Workspace allows created networks to run on VPCs. Therefore, the permission to access the VPC service is required.

After the permission granting is approved, an agency named **workspace_admin_trust** will be created on IAM. To ensure normal service usage, do not delete or modify the **workspace_admin_trust** agency when performing scheduled tasks or using the desktop pool. For details, see [System Entrustment Description](#).


----End

Basic Configurations

Step 1 Configure desktop information, as described in [Table 1 Desktop information](#).

Table 4-3 Desktop information

Parameter	Description	Example Value
Billing Mode	Select Yearly/Monthly .	Yearly/Monthly
Region	<p>Desktops in different regions cannot communicate with each other over the intranet, and desktops need to be managed by region. You are advised to create desktops in the same region.</p> <p>NOTE A region is the location of the physical data center of Workspace. Different regions indicate different physical distances between the physical data center and users, as well as different network latency. To reduce latency and improve access speed, select the region closest to your workloads.</p>	-

Parameter	Description	Example Value
Project	Select a project as required. NOTE If no project is available, click  and choose Create Project . On the displayed page, create a project by referring to Creating a Project .	-
Pool Name	User-defined desktop pool name.	-
Pool Type	Select Dynamic pool or Static pool . For details about the concepts, see " Related Concepts " in <i>Product Introduction</i> .	Dynamic pool
Description	Enter the remarks of the current desktop pool to mark the usage of the desktop pool.	-
AZ	An AZ is a physical region where resources use independent power supplies and networks. AZs are physically isolated but connected through an intranet. If an AZ becomes faulty, other AZs in the same region will not be affected. NOTE To achieve better disaster recovery, you are advised to create desktops in different AZs.	Random
CPU Architecture	Select the x86 architecture.	x86
Package Type	Select specifications as required.	Ultimate Ultimate 2 vCPUs 4 GB

Step 2 Configure an image.

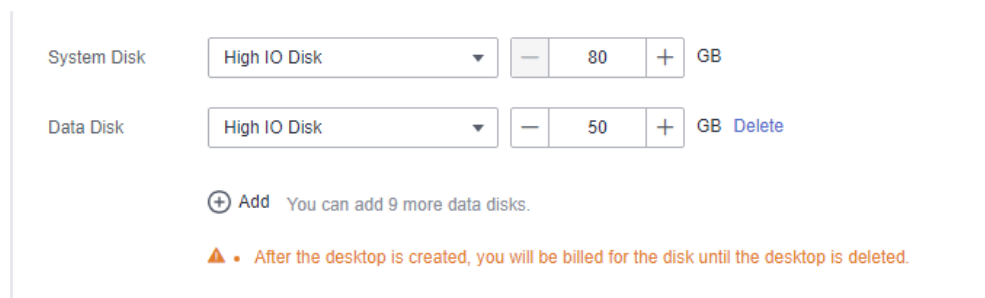
- **Image Type:** Select an image type as required.

 **NOTE**

- A public image is a widely used standard image provided by Workspace. It contains an OS and pre-installed public applications and is visible to all users. Public images are very stable and their OS and any included software have been officially authorized for use. If a public image does not contain the application environments or software you need, you can use a public image to create an application environment and then deploy required software. Currently, Windows public images are marketplace images.
 - A private image is created based on an existing cloud desktop or external image file and is visible only to the user who created it. It contains an OS, preinstalled public applications, and the user's personal applications. Using a private image to create a desktop saves more time.
 - Workspace supports public images running Windows, private images converted from desktops generated using Windows images, and private images converted from ECSs created using Windows image files. To use a private image to purchase a desktop, see [Converting a Desktop to an Image](#) and [Creating a Windows Desktop Private Image](#).
- **OS:** Select an OS type in the [supported OS list](#).

Step 3 Configure disks as required, as shown in [Figure 4-4](#).

Figure 4-4 Configuring disks




 **NOTE**

- For details about the disk type performance, see [Elastic Volume Service Product Introduction](#).
 - High I/O disks use serial attached SCSI (SAS) drives to store data.
 - Ultra-high I/O disks use solid state disk (SSD) drives to store data.
 - General purpose SSD disks use SSD drives to store data.
- After the desktop is created, you will be billed for the disk until the desktop is deleted.
- The disk size must be an integer multiple of 10.
- A maximum of 10 data disks can be configured.

Step 4 Set the number of desktops to be purchased and the required duration, and evaluate the fee.

Select the number of desktops to be purchased and the required duration. If the

selected duration is marked with , it indicates that the selected package has a discount within the time range. Click **Discount Details** to view the discount details.

Step 5 Click **Next: Configure advanced settings**.

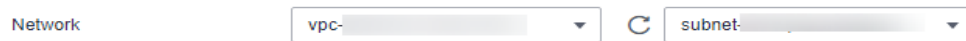
The page for configuring advanced settings is displayed.

----End

Advanced Settings

Step 1 Configure the network, as shown in [Figure 4-5](#).

Figure 4-5 Configuring the network



Click ▼ and select a VPC and a subnet.

Step 2 Configure the automatic creation mode of desktop pool autoscaling.

- **Created upon access:** When a user accesses the system and no idle desktop is available, the system automatically creates a desktop.

A maximum of x desktops can be automatically created: The maximum number of desktops that can be automatically created during pool desktop purchase and access is determined by the remaining quota of the user. Set this parameter as required.

- **Pre-create:** When the number of idle desktops is lower than the threshold, a specified number of desktops are automatically created.
 - If the number of idle desktops is less than x , the value is the number of idle desktops in the desktop pool.
 - x indicates the number of desktops to be pre-created.
 - A maximum of x desktops can be pre-created.

For example, if the number of idle desktops is less than 5 and 10 desktops need to be pre-created. A maximum of 10 desktops can be pre-created.

When the number of idle desktops is less than 5, the system pre-creates 10 desktops. When the number of idle desktops is less than 5 again, the system detects that the number of pre-created desktops reaches the threshold and no more desktops can be created.

NOTE

1. Desktops that are automatically created are on-demand desktops.
2. Desktop pools without on-demand packages, such as the enterprise edition, cannot be automatically created.

Step 3 Configure pool desktop unbinding upon disconnection.

- **Disconnection and unbinding:** After a client user disconnects from a desktop, the desktop can be retained for a period of time. After the retention period expires, the desktop is automatically unbound from the user and reset.
- The desktop retention period after disconnection ranges from 10 to 43,200 minutes.

NOTE

The desktop is reset after it is automatically unbound. Save the desktop data in a timely manner to avoid data loss.

Step 4 (Optional) Click **Advanced** and configure a tag, as shown in [Table 4-4](#).

 **NOTE**

- You are advised to use predefined tags from TMS to add the same tag to different cloud resources.
- A maximum of 10 tags can be added.

Table 4-4 Tag naming rules

Parameter	Rule
Tag key	<ul style="list-style-type: none"> • The value can contain up to 36 characters. • A tag key can contain letters, digits, spaces, and special characters (_.:=-@), but cannot start or end with a space or start with _sys_.
Tag value	<ul style="list-style-type: none"> • The value can contain up to 43 characters. • A tag value can contain letters, digits, spaces, and special characters (_.:=-@).

Step 5 Click **Next:Assign desktops**.

The page for assigning desktops is displayed.

----End

(Optional) Assigning Desktops

Step 1 Select the user authorization mode and configure the user to whom a desktop will be assigned.

 **NOTE**

If an existing AD domain is used, you need to create users on the AD server before assigning desktops.

Select a user authorization mode as required, as shown in [Table 4-5](#).

Table 4-5 User Authorization Mode

User Authorization Mode	Parameter	Operation
Select User	<ul style="list-style-type: none"> • You can search for activated users using filters. 	<ul style="list-style-type: none"> • You can search for a user based on the user type and username. • Select the target username and click OK.

User Authorization Mode	Parameter	Operation
<p>Create user > User Activation > Manual Input</p>	<ul style="list-style-type: none"> ● User information: Username is used for user authentication during desktop login. Rules for naming a username: <ul style="list-style-type: none"> - The name can contain 1 to 20 characters. - A name containing only digits is allowed. - The name can contain uppercase letters, lowercase letters, digits, periods (.), hyphens (-), and underscores (_), and must start with a lowercase letter or uppercase letter. - The value cannot be empty. ● Email is used to receive desktop provisioning emails and related notifications. Rules for verifying an email address: <ul style="list-style-type: none"> - Enter a valid email address through system verification. - The value can contain a maximum of 55 characters. - The value cannot be empty. ● The mobile number is used to receive desktop provisioning emails and related notifications. Rules for verifying a mobile number: <ul style="list-style-type: none"> - <i>[+][Country/Region code][Mobile number]</i> - For a mobile number in the Chinese mainland, you can omit <i>[+][Country/Region code]</i> and directly enter the mobile number. - The mobile number can contain spaces, slashes (/), and hyphens (-). 	<ul style="list-style-type: none"> ● Configure the user information, description, and account expiration settings as prompted. ● Click Add User. NOTE Enter the email address or mobile number, or both. ● Permission groups can be configured in batches. ● Configure the number of desktops as prompted.

User Authorization Mode	Parameter	Operation
<p>Create user > Manager Activation > Manual Input</p>	<ul style="list-style-type: none"> ● Username is used for user authentication during desktop login. Rules for naming a username: <ul style="list-style-type: none"> - The name can contain 1 to 20 characters. - A name containing only digits is allowed. - The name can contain uppercase letters, lowercase letters, digits, periods (.), hyphens (-), and underscores (_), and must start with a lowercase letter or uppercase letter. - The value cannot be empty. ● The initial password is authenticated when a user logs in to the desktop. Keep the initial password secure. <ul style="list-style-type: none"> - The password contains 8 to 32 characters. - The password must contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters (!@\$%^_-=+[{ } ; , / ?) - The password cannot be the username or the reverse username. <p>NOTE If your tenant connects to an AD domain, Manager Activation is unavailable by default.</p>	

User Authorization Mode	Parameter	Operation
Create user > Manager Activation > Batch Import	<ul style="list-style-type: none"> Upload the users recorded in the table and create them in batches. 	<ol style="list-style-type: none"> Click Download Template on the right of Import user information to download the user list template.
Create user > User Activation > Batch Import	<ul style="list-style-type: none"> Upload the users recorded in the table and create them in batches. 	<ol style="list-style-type: none"> Enter the serial number, username, email address, mobile number, expiration time, and description in the table as required. Click Upload to upload the user list that has been filled in as required. Confirm the creation. <p>NOTE The size of the file to be uploaded cannot exceed 1 MB. A maximum of 200 records can be uploaded at a time. Only .xlsx and .xls files are supported.</p>

Step 2 The desktop is being assigned to users.

- Permission groups are used to distinguish users' permissions on computers.
 - Windows desktop permissions:
 - Administrator group: Users in this group have system administrator permissions, that is, full permissions on a computer. They can perform all management tasks, including managing all users, on the computer.
 - Common user group: Users in this group have basic operation permissions on a computer, for example, running applications. A user in this group cannot modify the OS settings or data of other users, or shut down a server computer.
 - UOS desktop permissions:

Step 3 Select a user group authorization mode and configure a user group to which pool desktops are assigned, as shown in [Table 4-6](#).

Table 4-6 User Group Authorization Mode

User Group Authorization Mode	Parameter	Operation
Select User Group	<ul style="list-style-type: none"> Users can be grouped to simplify user management. 	<ul style="list-style-type: none"> You can find the corresponding user group based on the entered user group name and click OK to add the selected user group name to the list of user groups to which pool desktops are assigned.

User Group Authorization Mode	Parameter	Operation
Create User Group	<ul style="list-style-type: none"> • Create a user group to manage pool desktop users. <ul style="list-style-type: none"> - The value can contain letters, digits, periods (.), hyphens (-), and underscores (_). - The value cannot be empty. - The value can contain a maximum of 64 characters. • There are two user group types: <ul style="list-style-type: none"> - Common user group: the user group management system provided by Workspace, which provides batch user management capabilities and is applicable when interconnection with AD user groups is not required. - AD user group: user group for interconnecting with the enterprise AD, which is applicable when user permissions are managed using the enterprise AD user group. 	<ol style="list-style-type: none"> 1. Enter the user group name. 2. Select a user group type as required. 3. Confirm the creation.

Step 4 Assign a desktop pool to a user group.

- Permission groups are used to distinguish users' permissions on computers.
 - Windows desktop permissions:

- Administrator group: Users in this group have system administrator permissions, that is, full permissions on a computer. They can perform all management tasks, including managing all users, on the computer.
- Common user group: Users in this group have basic operation permissions on a computer, for example, running applications. A user in this group cannot modify the OS settings or data of other users, or shut down a server computer.
- UOS desktop permissions:

Step 5 Click **Next: Confirm the settings**.

The confirmation page is displayed.

----End

Confirming the Settings

Step 1 Select **Enterprise Project** as needed.

NOTE

You can use an enterprise project to centrally manage your cloud resources and members by project.

Step 2 Set the duration as required.

Step 3 (Optional) Select **Auto renewal** if needed.

NOTE

- For details about the auto-renewal fee deduction rules, see [Auto-Renewal Rules](#).
- Auto-renewal duration:
 - **Monthly**: You can renew the subscription for one month each time. The number of renewal times is not limited.
 - **Yearly**: You can renew the subscription for one year each time. The number of renewal times is not limited.

Step 4 Read the disclaimer and select **I have read and agree to the Image Disclaimer**.

Step 5 Click **Buy Now**.

The page for purchasing desktops is displayed.

Step 6 Check the cloud order service and the fee to be paid.

Step 7 After you select a payment method and pay for your order, the desktop pool has been purchased.

After the desktop pool is provisioned, administrators can choose **Desktop Management > Desktop Pool** to view the purchased desktop pool.

----End

Follow-up Operations

- The login details for the newly created desktop will be emailed to the end user. The end user can activate the account, download the client, and configure and use the desktop as instructed. Administrators can restrict

desktop network interaction as required. For details, see [Configuring Workspace to Access the Public Network](#) and [Configuring Workspace to Access the Intranet](#).

- If a Windows AD domain has been connected and an OU has been created on the Windows AD server, create the OU on the console by referring to [OU Management](#).
- For details about performing auto-renewal on the console, see [Auto-renewal](#).

4.4 Purchasing Pay-per-Use Desktops

Scenarios

An administrator can select the pay-per-use billing mode and packages, and assign desktops to end users. After the administrator purchases a desktop, the system automatically sends a notification email to the user's mailbox.

Purchase Page

Step 1 [Logging In to the Workspace Console](#)

Step 2 On the **Dashboard** or **Desktop Management** page, click **Buy Desktop**.

The page for buying desktops is displayed.

----End

Selecting Whether to Connect to the Windows AD

NOTICE

After you purchase a desktop for the first time, your selection (connecting to the Windows AD domain or canceling the connection to the Windows AD domain) cannot be changed. Exercise caution when performing this operation.

- If you select **No**, you can directly configure the desktop infrastructure by referring to [Basic Configurations](#). After the desktop creation task is submitted, the Workspace service will be deployed.

After subscribing to the service, you can use the account authentication system of Huawei to authenticate users and manage user accounts on the Workspace console.


- Select **Yes** to configure the Windows AD domain. For details, see [Connecting to the Windows AD Domain](#). After the configuration information is saved, the Workspace service will be deployed.

After the service is subscribed, the existing unified AD of the enterprise is used to authenticate users and manage user accounts.

Basic Configurations

Step 1 Configure desktop information, as described in [Table 2 Basic configurations](#).

Table 4-7 Basic configurations

Parameter	Description	Example Value
Billing Mode	Select Pay-per-use .	Pay-per-use
Region	Desktops in different regions cannot communicate with each other over the intranet, and desktops need to be managed by region. You are advised to create desktops in the same region. NOTE A region is the location of the physical data center of Workspace. Different regions indicate different physical distances between the physical data center and users, as well as different network latency. To reduce latency and improve access speed, select the region closest to your workloads.	-
Project	Select a project as required. NOTE If no target project is available, click  and choose Create Project . The page for creating a project is displayed. Create a project by referring to Creating a Project .	-
AZ	An AZ is a physical region where resources use independent power supplies and networks. AZs are physically isolated but connected through an intranet. If an AZ becomes faulty, other AZs in the same region will not be affected. NOTE To achieve better disaster recovery, you are advised to create desktops in different AZs.	General Random
CPU Architecture	Select x86 .	x86
Package Type	Select specifications as required.	Ultimate Ultimate 2 vCPUs 4 GB

Step 2 Configure an image.

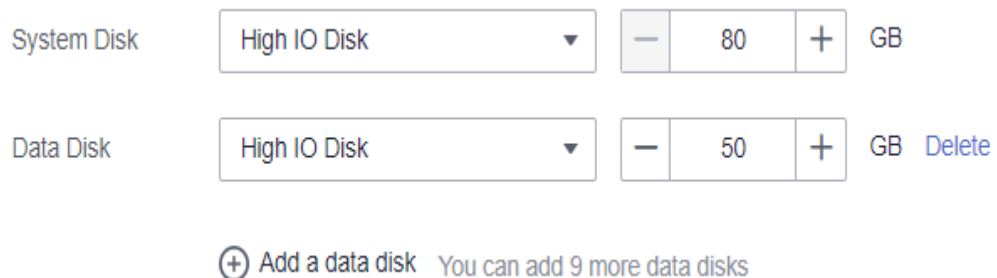
- **Image Type:** Select an image type as required.

 **NOTE**

- A public image is a widely used standard image provided by Workspace. It contains an OS and pre-installed public applications and is visible to all users. Public images are very stable and their OS and any included software have been officially authorized for use. If a public image does not contain the application environments or software you need, you can use a public image to create an application environment and then deploy required software. Currently, Windows public images are marketplace images.
 - A private image is created based on an existing cloud desktop or external image file and is visible only to the user who created it. It contains an OS, preinstalled public applications, and the user's personal applications. Using a private image to create a desktop saves more time.
 - The pay-per-use desktop supports public images running Windows, private images converted from desktops generated using Windows images, and private images converted from ECSs created using Windows image files. To use a private image to purchase a desktop, see [Converting a Desktop to an Image](#) and [Creating a Windows Desktop Private Image](#).
- **OS:** Select a Windows OS type in the [supported OS list](#).

Step 3 Configure disks as required, as shown in [Figure 4-6](#).

Figure 4-6 Configuring disks



 **NOTE**

- For details about the disk type performance, see [EVS Product Introduction](#).
 - High I/O disks use serial attached SCSI (SAS) drives to store data.
 - Ultra-high I/O disks use solid state disk (SSD) drives to store data.
 - General purpose SSD disks use SSD drives to store data.
- After the desktop is created, you will be billed for the disk until the desktop is deleted.
- The disk size must be an integer multiple of 10.
- A maximum of 10 data disks can be configured.

Step 4 Click **Next: Configure advanced settings**.

The page for configuring advanced settings is displayed.

----End

Advanced Settings

Step 1 (Optional) Configure an enterprise ID.

You are advised to use identifiable fields such as the enterprise name pinyin as the enterprise ID.

NOTE

- Customize an enterprise ID or use a randomly-generated ID upon the first purchase.
- Enterprise ID is the unique identifier of your tenant environment. End users need to enter the enterprise ID when logging in to the system.
- The enterprise ID contains a maximum of 32 characters, which can only be digits and letters.

Step 2 Configure the network.



Figure 4-7 Configuring the network



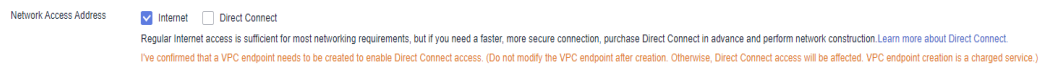
NOTICE

The 172 network segment is reserved for running internal services. Therefore, do not select a VPC network starting with 172. Otherwise, desktops cannot be purchased.

The resources required by Workspace will be created in the selected VPC subnet. After the desktop is purchased for the first time, the VPC cannot be modified, and only the service subnet can be managed.

- Configure the existing network.
 - Click  and select a service subnet. If you purchase a desktop for the first time, you need to select a VPC and a service subnet. For details about how to create a VPC and a service subnet, see [Creating a VPC and a Service Subnet](#).
- Configure a new network.
 - Click **Click here to manage subnets**. In the displayed **Modify the service subnet** dialog box, click **Create on Console** to create a service subnet. For details, see [Creating a Service Subnet for the VPC](#).
 - If you purchase a desktop for the first time, click **Create on Console** to create a VPC and a service subnet. For details, see [Creating a VPC and a Service Subnet](#).
 - Click  and configure the IP address type as required.
 - Automatically assign an IP address.
 - Manually assign an IP address.
 - Use an existing elastic network interface.

Step 3 Configure the network access mode, as shown in [Figure 4-8](#). By default, **Internet** is selected. You can select multiple options.

Figure 4-8 Network access**NOTE**

- Internet access is sufficient for most networking requirements, but if you need a faster, more secure connection, purchase Direct Connect in advance and implement networking. [Learn more about Direct Connect](#), load balancers will be automatically created when Direct Connect access is enabled. (Do not modify the load balancers.)
- Direct Connect network segment configuration: Enter the network segment where the desktop client (such as TC) is located. You can enter multiple network segments and separate them with semicolons (;).

Step 4 Configure an EIP for network access.

- **Buy now**

- **By Bandwidth:** applicable when the traffic is heavy or stable and the bandwidth ranges from 1 Mbit/s to 200 Mbit/s. You can customize the bandwidth as prompted.

NOTE

Specify the bandwidth upper limit. You are charged based on the actual outbound traffic, regardless of the usage duration.

- **By Traffic:** applicable when the traffic is small or fluctuates greatly and the bandwidth size ranges from 5 Mbit/s to 200 Mbit/s. You can customize the bandwidth as prompted.

NOTE

You are charged based on the purchased duration and bandwidth size.

- **Use existing:** Bind an existing EIP to the desktop.
- **Not required:** To enable desktop Internet access, go to **Internet Access Management** on the Workspace console.

Step 5 Click **Next:Assign desktops**.

The page for assigning desktops is displayed.

----End

Assigning Desktops

Step 1 Select the user import mode and configure information of the user to whom a desktop is to be assigned.

NOTE

If an existing AD domain is used, you need to create users on the AD server before assigning desktops.

Select **Manual** or **Batch** as required, as shown in [Table 4-8](#).

Table 4-8 Desktop assignment

User Authorization Mode	Parameter	Operation
Desktop Assignment Type	<ul style="list-style-type: none"> • Manually 	Select Select User or Create User .
	<ul style="list-style-type: none"> • Batch 	<ol style="list-style-type: none"> 1. Select Batch. 2. Locate the row that contains Import User List, and click Download a user list template. 3. Enter the serial number, username, permission group, and desktop name in the table as required. 4. Click Upload to upload the user list that has been filled in as required. <p>NOTE The size of the file to be uploaded cannot exceed 1 MB. The username and desktop name must be different.</p>
	<ul style="list-style-type: none"> • Not assigned <p>NOTE</p> <ul style="list-style-type: none"> - If you purchase one desktop, the desktop name is the name of the desktop. - When multiple desktops are purchased, the desktop name prefix is used to generate desktop names in ascending order. For example, if the prefix is desktop and you create three desktops, the names of the created desktops are desktop01, desktop02, and desktop03. - To assign a desktop to a user, select the desired desktop on the desktop management page and choose More > Assign users. 	<ol style="list-style-type: none"> 1. Select Not assigned. 2. Enter the name of the desktop that is not assigned to a user based on site requirements.

User Authorization Mode	Parameter	Operation
User Authorization	When selecting users, you can search for activated users by setting filter criteria.	<ul style="list-style-type: none"> • You can search for a user/group based on the user/group name. • Select the target username and click OK.

User Authorization Mode	Parameter	Operation
	<p>Create user > User Activation > Manual Input</p> <ul style="list-style-type: none"> ● Username is used for user authentication during desktop login. Rules for naming a username: <ul style="list-style-type: none"> - The name can contain 1 to 20 characters. - A name containing only digits is allowed. - The name can contain uppercase letters, lowercase letters, digits, periods (.), hyphens (-), and underscores (_), and must start with a lowercase letter or uppercase letter. - The value cannot be empty. ● Email is used to receive desktop provisioning emails and related notifications. Rules for verifying an email address: <ul style="list-style-type: none"> - Enter a valid email address through system verification. - The value can contain a maximum of 64 characters. - The value cannot be empty. ● The mobile number is used to receive desktop provisioning emails and related notifications. Rules for verifying a mobile number: <ul style="list-style-type: none"> - <i>[+][Country/Region code][Mobile number]</i> - For a mobile number in the Chinese mainland, you can omit <i>[+][Country/Region code]</i> and directly enter the mobile number. - The mobile number can contain spaces, slashes (/), and hyphens (-). 	<ul style="list-style-type: none"> ● Configure the user information, description, and account expiration settings as prompted. ● Click Add User. NOTE Enter the email address or mobile number, or both. ● Permission groups can be configured in batches. ● The desktop name is automatically generated. ● Click Add Desktop to add a desktop. ● Configure the number of desktops as prompted.

User Authorization Mode	Parameter	Operation
	<p>Create user > Manager Activation > Manual Input</p> <ul style="list-style-type: none"> • Username is used for user authentication during desktop login. Rules for naming a username: <ul style="list-style-type: none"> - The name can contain 1 to 20 characters. - A name containing only digits is allowed. - The name can contain uppercase letters, lowercase letters, digits, periods (.), hyphens (-), and underscores (_), and must start with a lowercase letter or uppercase letter. - The value cannot be empty. • The initial password is authenticated when a user logs in to the desktop. Keep the initial password secure. <ul style="list-style-type: none"> - The password contains 8 to 32 characters. - The value can contain letters, digits, and the following special characters: !@\$%^-_=+[{ }];,./? - The password cannot be the username or the reverse username. <p>NOTE If your tenant connects to the enterprise ID, the Manager Activation method is unavailable by default.</p>	

User Authorization Mode	Parameter	Operation
	Create user > Manager Activation > Batch Import <ul style="list-style-type: none"> Upload the users recorded in the table and create them in batches. 	<ol style="list-style-type: none"> Click Download Template on the right of Import user information to download the user list template. Enter the serial number, username, email address, mobile number, expiration time, and description in the table as required. Click Upload to upload the user list that has been filled in as required. Confirm the creation. <p>NOTE The size of the file to be uploaded cannot exceed 1 MB. A maximum of 200 records can be uploaded at a time. Only .xlsx and .xls files are supported.</p>
	Create user > User Activation > Batch Import <ul style="list-style-type: none"> Upload the users recorded in the table and create them in batches. 	

Step 2 Click **Next: Confirm the settings**.

The confirmation page is displayed.

----End

Confirming the Settings

Step 1 Select **Enterprise Project** as needed.

 **NOTE**

You can use an enterprise project to centrally manage your cloud resources and members by project.

Step 2 After verifying the information, read the disclaimer and select **I have read and agree to the Image Disclaimer**.

Step 3 Click **Buy Now**. After the task is submitted, click **Return to cloud desktop list** to check whether the desktop has been created.

If the creation fails, check the failure cause. For details, see [Viewing Desktops That Fail to Be Created](#).

 **NOTE**

The login details for the newly purchased desktop will be emailed to the end user. The end user can refer to the email to activate the account, download the client, and configure and use the desktop. Administrators can view the purchased desktop in the desktop list.

----End

Follow-up Operations

- The login details for the newly created desktop will be emailed to the end user. The end user can activate the account, download the client, and configure and use the desktop as instructed. Administrators can restrict desktop network interaction as required. For details, see [Configuring Workspace to Access the Public Network](#) and [Configuring Workspace to Access the Intranet](#).
- If a Windows AD domain has been connected and an OU has been created on the Windows AD server, create the OU on the console by referring to [OU Management](#).

4.5 Purchasing Pay-per-Use Desktop Pools

Scenarios

Administrators can select the pay-per-use billing mode and packages to purchase desktop pools.

Purchase Page

Step 1 [Logging In to the Workspace Console](#)

Step 2 On the **Desktops** page, choose **Desktop Pools** and click **Purchase Desktop Pool**.

The page for buying desktop pools is displayed.

 **NOTE**

When you purchase a desktop pool for the first time, the system prompts you to perform authorization.

- **IMS permissions**
Workspace supports image creation. Therefore, the permission to access IMS is required.
- **Administrator permissions for related cloud services**
Workspace supports scheduled disk recomposing and auto scaling. Therefore, the tenant administrator permissions are required.
- **VPC service permissions**
Workspace allows created networks to run on VPCs. Therefore, the permission to access the VPC service is required.


After the permission granting is approved, an agency named **workspace_admin_trust** will be created on IAM. To ensure normal service usage, do not delete or modify the **workspace_admin_trust** agency when performing scheduled tasks or using the desktop pool. For details, see [System Entrustment Description](#).

----End

Basic Configurations

Step 1 Configure desktop information, as described in [Table 4-9](#).

Table 4-9 Basic Configurations

Parameter	Description	Example Value
Billing Mode	Select Pay-per-use .	Pay-per-use
Region	Desktops in different regions cannot communicate with each other over the intranet, and desktops need to be managed by region. You are advised to create desktops in the same region. NOTE A region is the location of the physical data center of Workspace. Different regions indicate different physical distances between the physical data center and users, as well as different network latency. To reduce latency and improve access speed, select the region closest to your workloads.	-
Project	Select a project as required. NOTE If no target project is available, click  and choose Create Project . The page for creating a project is displayed. Create a project by referring to Creating a Project .	-

Parameter	Description	Example Value
Pool Name	User-defined desktop pool name.	-
Pool Type	Select Dynamic pool or Static pool . For details about the concepts, see Related Concepts in <i>Service Overview</i> .	-
AZ	An AZ is a physical region where resources use independent power supplies and networks. AZs are physically isolated but connected through an intranet. If an AZ becomes faulty, other AZs in the same region will not be affected. NOTE To achieve better disaster recovery, you are advised to create desktops in different AZs.	Random
CPU Architecture	Select x86 .	x86
Package Type	Select specifications as required.	Ultimate Ultimate 2 vCPUs 4 GB

Step 2 Configure an image.

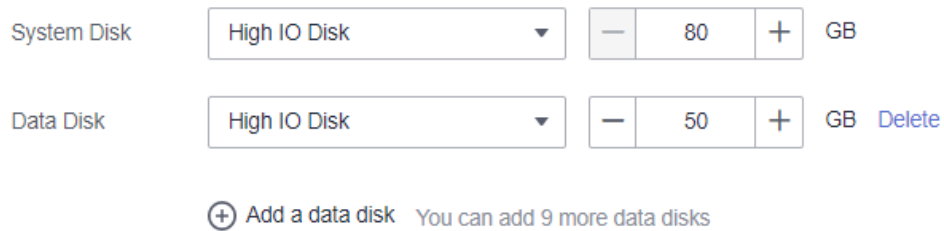
- **Image Type:** Select an image type as required.

 **NOTE**

- A public image is a widely used standard image provided by Workspace. It contains an OS and pre-installed public applications and is visible to all users. Public images are very stable and their OS and any included software have been officially authorized for use. If a public image does not contain the application environments or software you need, you can use a public image to create an application environment and then deploy required software. Currently, Windows public images are marketplace images.
 - A private image is created based on an existing cloud desktop or external image file and is visible only to the user who created it. It contains an OS, preinstalled public applications, and the user's personal applications. Using a private image to create a desktop saves more time.
 - The pay-per-use desktop supports public images running Windows, private images converted from desktops generated using Windows images, and private images converted from ECSs created using Windows image files. To use a private image to purchase a desktop, see [Converting a Desktop to an Image](#) and [Creating a Windows Desktop Private Image](#).
- **OS:** Select a Windows OS type in the [supported OS list](#).

Step 3 Configure disks as required, as shown in [Figure 4-9](#).

Figure 4-9 Configuring disks



NOTE

- For details about the disk type performance, see [EVS Disk Types and Performance](#).
 - High I/O disks use serial attached SCSI (SAS) drives to store data.
 - Ultra-high I/O disks use solid state disk (SSD) drives to store data.
 - General purpose SSD disks use SSD drives to store data.
- After the desktop is created, you will be billed for the disk until the desktop is deleted.
- The disk size must be an integer multiple of 10.
- A maximum of 10 data disks can be configured.

Step 4 Click **Next: Configure advanced settings**.

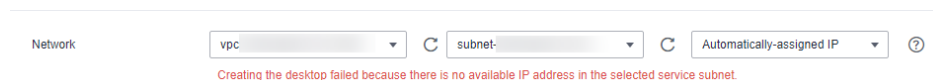
The page for configuring advanced settings is displayed.

----End

Advanced Settings

Step 1 Configure the network, as shown in [Figure 4-10](#).

Figure 4-10 Configuring the network



Click ▼ and select a VPC and a subnet.

Step 2 Configure the automatic creation mode of desktop pool autoscaling.

- **Created upon access:** When a user accesses the system and no idle desktop is available, the system automatically creates a desktop.

A maximum of x desktops can be automatically created: The maximum number of desktops that can be automatically created during pool desktop purchase and access is determined by the remaining quota of the user. Set this parameter as required.
- **Pre-create:** When the number of idle desktops is lower than the threshold, a specified number of desktops are automatically created.
 - If the number of idle desktops is less than x , the value is the number of idle desktops in the desktop pool.
 - x indicates the number of desktops to be pre-created.
 - A maximum of x desktops can be pre-created.

For example, if the number of idle desktops is less than 5 and 10 desktops need to be pre-created. A maximum of 10 desktops can be pre-created.

When the number of idle desktops is less than 5, the system pre-creates 10 desktops. When the number of idle desktops is less than 5 again, the system detects that the number of pre-created desktops reaches the threshold and no more desktops can be created.

 **NOTE**

Desktops that are automatically created are on-demand desktops.

Step 3 Configure pool desktop unbinding upon disconnection.

- Disconnection and unbinding: After a client user disconnects from a desktop, the desktop can be retained for a period of time. After the retention period expires, the desktop is automatically unbound from the user and reset.
- The retention duration upon disconnection ranges from 10 to 43,200 minutes.

 **NOTE**

The desktop is reset after it is automatically unbound. Save the desktop data in a timely manner to avoid data loss.

Step 4 (Optional) Click **Advanced** and configure a tag, as shown in [Table 4-10](#).

 **NOTE**

- You are advised to use predefined tags from TMS to add the same tag to different cloud resources.
- To learn more about tags, see [Tag Management Service User Guide](#).
- A maximum of 20 tags can be added.

Table 4-10 Tag naming rules

Parameter	Rule
Tag key	<ul style="list-style-type: none"> • The value can contain up to 36 characters. • A tag key can contain letters, digits, spaces, and special characters (_.:/+@), but cannot start or end with a space or start with _sys_.
Tag value	<ul style="list-style-type: none"> • The value can contain up to 43 characters. • A tag value can contain letters, digits, spaces, and special characters (_.:/+@).

Step 5 Click **Next: Assign desktops**.

The page for assigning desktops is displayed.

Step 6 Select a naming rule.

 **NOTE**

For details about how to create a naming rule, see [Desktop Naming Rules](#).

----End

Assigning Desktops

Step 1 Select the user authorization mode and configure the user to whom a desktop will be assigned.

 **NOTE**

If an existing AD domain is used, you need to create users on the AD server before assigning desktops.

Select a user authorization mode as required, as shown in [Table 4-11](#).

Table 4-11 User Authorization Mode

User Authorization Mode	Parameter	Operation
Select User	<ul style="list-style-type: none"> You can search for activated users using filters. 	<ul style="list-style-type: none"> You can search for a user based on the user type and username.

User Authorization Mode	Parameter	Operation
<p>Create User > By users for User Activation and Manually for User Import</p>	<ul style="list-style-type: none"> ● User information: Username is used for user authentication during desktop login. Rules for naming a username: <ul style="list-style-type: none"> - The name can contain 1 to 20 characters. - A name containing only digits is allowed. - Only letters, digits, and three types of special characters (-_.) are allowed. The value must start with a letter or digit and cannot end with a period (.) or underscore (_). - The value cannot be empty. ● The email address is used to receive desktop provisioning emails and related notifications. Rules for verifying an email address: <ul style="list-style-type: none"> - Enter a valid email address through system verification. - The value can contain a maximum of 55 characters. - The value cannot be empty. ● The mobile number is used to receive desktop provisioning emails and related notifications. Rules for verifying a mobile number: <ul style="list-style-type: none"> - <i>[+][Country/Region code][Mobile number]</i> - For a mobile number in the Chinese mainland, you can omit <i>[+][Country/Region code]</i> and directly enter the mobile number. - The mobile number can contain spaces, slashes (/), and hyphens (-). 	<ul style="list-style-type: none"> ● Configure the user information, description, and account expiration settings as prompted. ● Click Add User. <p>NOTE Enter the email address or mobile number, or both.</p> <ul style="list-style-type: none"> ● Permission groups can be configured in batches. ● Configure the number of desktops as prompted.

User Authorization Mode	Parameter	Operation
<p>Create User > By administrators for User Activation and Manually for User Import</p>	<ul style="list-style-type: none"> ● Username is used for user authentication during desktop login. Rules for naming a username: <ul style="list-style-type: none"> - The name can contain 1 to 20 characters. - A name containing only digits is allowed. - Only letters, digits, and three types of special characters (-_.) are allowed. The value must start with a letter or digit and cannot end with a period (.) or underscore (_). - The value cannot be empty. ● The initial password is authenticated when a user logs in to the desktop. Keep the initial password secure. <ul style="list-style-type: none"> - The password contains 8 to 32 characters. - The password must contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters (!@\$%^_-=+[{ } ; , / ?) - The password cannot be the username or the reverse username. <p>NOTE If your tenant connects to an AD domain, Manager Activation is unavailable by default.</p>	

User Authorization Mode	Parameter	Operation
<p>Create User > By administrators for User Activation and Batch for User Import</p>	<ul style="list-style-type: none"> Upload the users recorded in the table and create them in batches. 	<ol style="list-style-type: none"> Click Download Template on the right of Import user information to download the user list template. Enter the serial number, username, email address, mobile number, expiration time, and description in the table as required.
<p>Create User > By users for User Activation and Batch for User Import</p>	<ul style="list-style-type: none"> Upload the users recorded in the table and create them in batches. 	<ol style="list-style-type: none"> Click Upload to upload the user list that has been filled in as required. Confirm the creation. <p>NOTE The size of the file to be uploaded cannot exceed 1 MB. A maximum of 200 records can be uploaded at a time. Only .xlsx files can be uploaded.</p>

Step 2 Assign the desktop to the user.

- Permission groups are used to distinguish users' permissions on computers.
 - Windows desktop permissions:
 - Administrator group: Users in this group have system administrator permissions, that is, full permissions on a computer. They can perform all management tasks, including managing all users, on the computer.
 - Common user group: Users in this group have basic operation permissions on a computer, for example, running applications. A user in this group cannot modify the OS settings or data of other users, or shut down a server computer.
- You can click **Batch Settings** to modify the permission group of the selected user.

Step 3 Select a user group authorization mode and configure a user group to which pool desktops are assigned, as shown in [Table 4-12](#).

Table 4-12 User Group Authorization Mode

User Group Authorization Mode	Parameter	Operation
Select User Group	<ul style="list-style-type: none"> • Users can be grouped to simplify user management. 	<ul style="list-style-type: none"> • You can find the corresponding user group based on the entered user group name and click OK to add the selected user group name to the list of user groups to which pool desktops are assigned.

User Group Authorization Mode	Parameter	Operation
Create User Group	<ul style="list-style-type: none"> ● Create a user group to manage pool desktop users. <ul style="list-style-type: none"> - The value can contain letters, digits, periods (.), hyphens (-), and underscores (_). - The value cannot be empty. - The value can contain a maximum of 64 characters. ● There are two user group types: <ul style="list-style-type: none"> - Common user group: the user group management system provided by Workspace, which provides batch user management capabilities and is applicable when interconnection with AD user groups is not required. - AD user group: user group for interconnecting with the enterprise AD, which is applicable when user permissions are managed using the enterprise AD user group. 	<ol style="list-style-type: none"> 1. Enter the user group name. 2. Select a user group type as required. 3. Confirm the creation.

Step 4 Assign the desktop pool to the user group.

- Permission groups are used to distinguish users' permissions on computers.
 - Windows desktop permissions:

- Administrator group: Users in this group have system administrator permissions, that is, full permissions on a computer. They can perform all management tasks, including managing all users, on the computer.
- Common user group: Users in this group have basic operation permissions on a computer, for example, running applications. A user in this group cannot modify the OS settings or data of other users, or shut down a server computer.
- You can click **Batch Settings** to modify the permission group of the selected user group.

Step 5 Click **Next: Confirm the settings**.

The confirmation page is displayed.

----End

Confirming the Settings

Step 1 Select **Enterprise Project** as needed.

 **NOTE**

You can use an enterprise project to centrally manage your cloud resources and members by project.

Step 2 After verifying that the information is correct, click **Buy Now**. After the task is submitted, click **Back to Desktop Pool List** to check whether the desktop has been created.

If the creation fails, check the failure cause. For details, see [Viewing the Desktop Pool That Fails to Be Created](#).

 **NOTE**

The login details for the newly purchased desktop pool will be emailed to the end user. The end user can refer to the email to activate the account, download the client, and configure and use the desktop. Administrators can choose **Desktops > Desktop Pools** to view the purchased desktop pool.

----End

Follow-up Operations

- The login details for the newly created desktop will be emailed to the end user. The end user can activate the account, download the client, and configure and use the desktop. Administrators can restrict desktop network interaction as required. For details, see [Configuring Workspace to Access the Public Network](#) and [Configuring Workspace to Access the Intranet](#).
- If a Windows AD domain has been connected and an OU has been created on the Windows AD server, create the OU on the console by referring to [OU Management](#).

5 Logging In to a Desktop

5.1 Using a Thin Client

Scenarios

Log in to a user's computer from a cloud client on a TC.

NOTE

The initial configuration described in this section needs to be performed only once on each terminal.


Procedure

Step 1 Power on the TC.

Step 2 Upon the first login, choose **Start > Control Center** to open Workspace.

Go to the **Server Configuration** page.

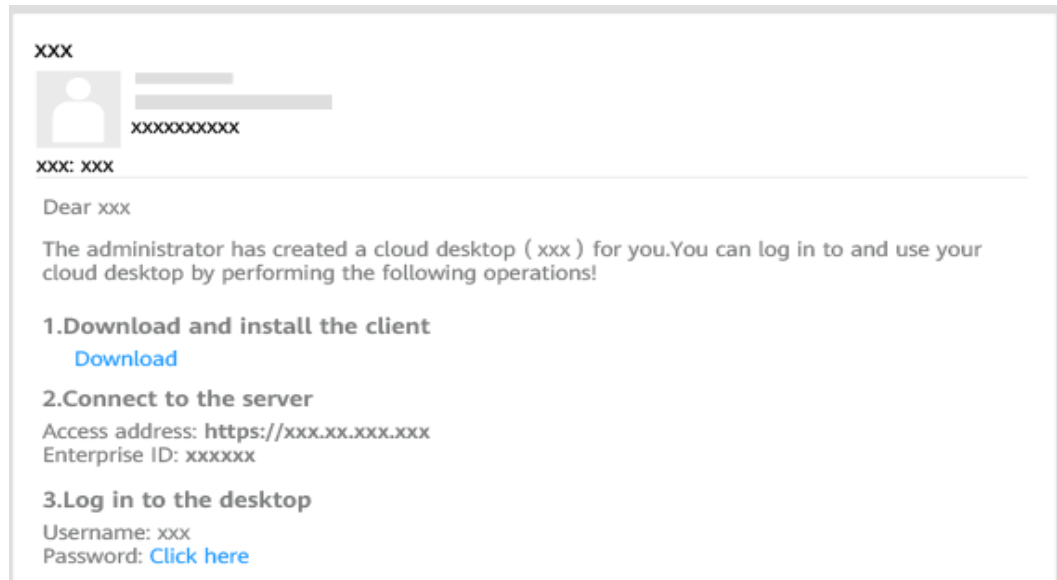
NOTE

After some TCs are powered on, the software list page including the Workspace client is displayed. You can click  to access the server configuration page of Workspace. Refer to the actual information displayed on the TC.

Step 3 Obtain the desktop login information email sent by the system.

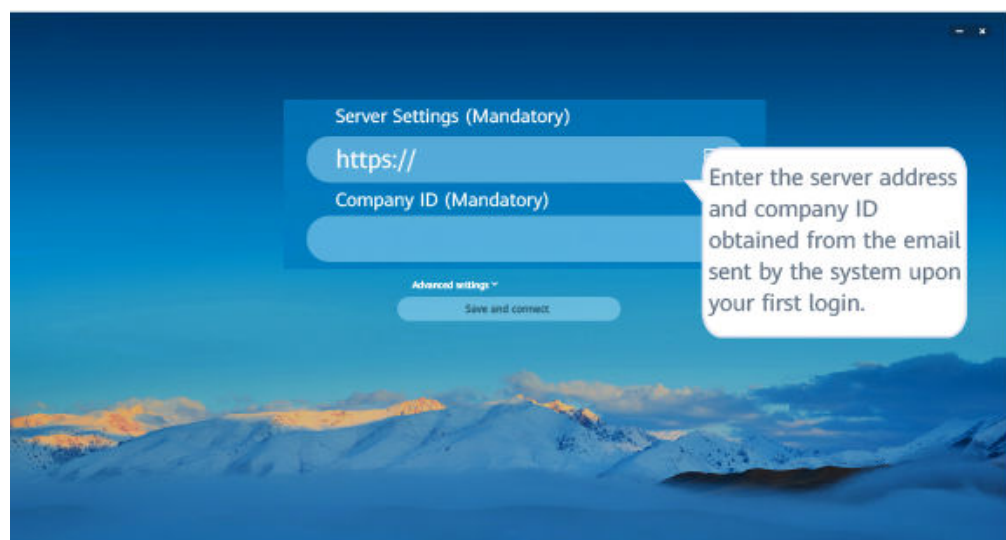
NOTE

The notification email for AD connection is slightly different from that when the AD is not connected. Refer to the actual notification email.



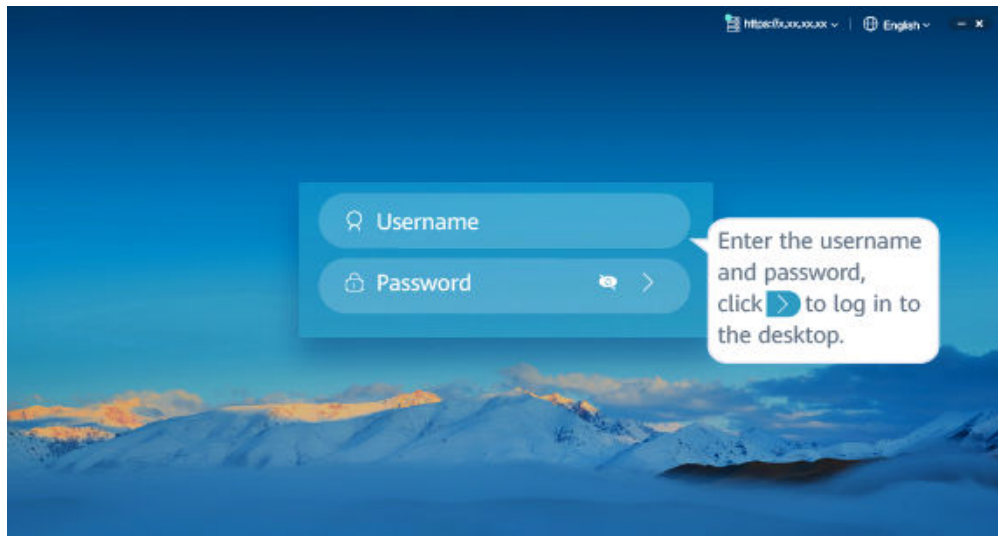
Step 4 Configure the server IP address and enterprise ID.

- **Figure 5-1** Configuring the server IP address and enterprise ID



Step 5 Log in to the desktop, as shown in **Figure 5-2**.

Figure 5-2 Logging in to a desktop



NOTE

- If the account has multiple desktops, enter the username and password and click **Log In**. The desktop list page is displayed. You need to click the target desktop to access it.
- If multi-factor authentication has been enabled, you need to pass the multi-factor authentication again before accessing the cloud desktop.

Step 6 (Optional) Perform multi-factor authentication.

You need to perform authentication again only when the administrator has enabled **multi-factor authentication**.

- After multi-factor authentication is enabled, you need to bind a virtual MFA device to the desktop upon the first login.



- a. Download and install an application that supports TOTP on a smart device, such as a mobile phone.
- b. On the MFA tool page of the smart device, select the QR code scanning mode or manual input mode to bind the device.

 NOTE

Your operation is subject to the application you use.

- If you choose to scan the QR code, scan the QR code in the **Scanning** area of the multi-factor authorization page of the Workspace client.
 - If you choose to manually input, on the MFA tool page of the smart device, enter the account and key in the **Manually** area of the multi-factor authorization page of the Workspace client.
- c. Enter the dynamic verification code generated by the virtual MFA device bound to the smart device in the verification code text box on the Workspace client.



 NOTE

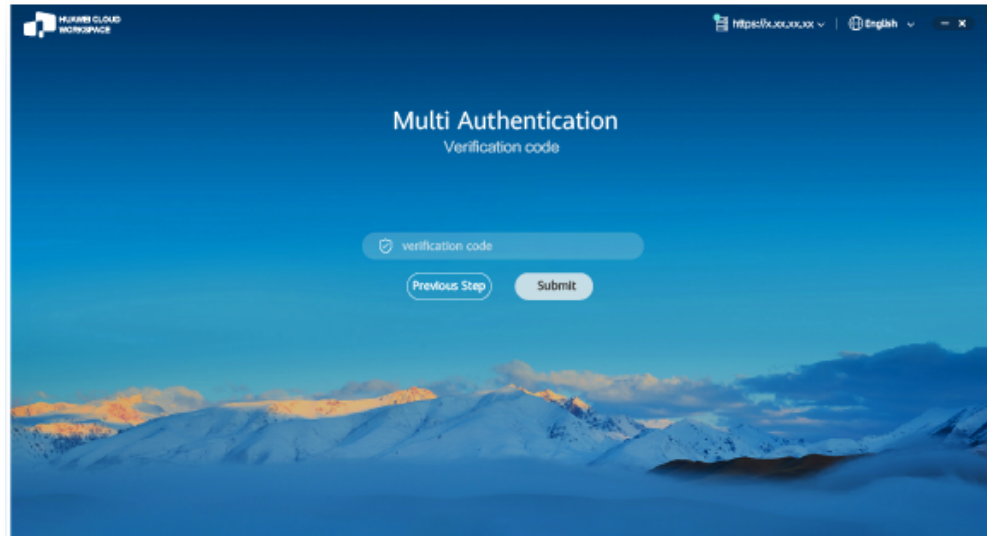
The preceding verification code page is only an example. The actual page varies depending on the application in use.

- d. On the multi-factor authorization page of the Workspace client, click **Binding**.

 NOTE

If the account has multiple desktops, the desktop list page will be displayed after you click **Binding**. You need to click the target desktop to access it.

- After multi-factor authentication is enabled, use the proprietary authentication system of Huawei Cloud. If this is not the first time of login to the desktop, use the proprietary authentication system of the enterprise and directly enter the verification code for authentication.



- a. Open an application that supports TOTP on a smart device, such as a mobile phone, and access the MFA tool page.
- b. Enter the dynamic verification code generated by the virtual MFA device bound to the smart device in the verification code text box on the Workspace client.



NOTE

The preceding verification code page is only an example. The actual page varies depending on the application in use.

- c. On the multi-factor authorization page of the Workspace client, click **Submit**.

 **NOTE**

If the account has multiple desktops, the desktop list page will be displayed after you click **Submit**. You need to click the target desktop to access it.

----End

5.2 Using a Soft Client

Scenarios

Log in to a user's computer from a cloud client on an SC.

 **NOTE**

The initial configuration described in this section needs to be performed only once on each terminal.

Prerequisites

[Table 5-1](#) lists the file needed.

Table 5-1 Software packages

Software Package	Description	How to Obtain
Workspace_mac.dmg	Used to install the PC client for macOS.	<ol style="list-style-type: none"> 1. Go to the Workspace client download page on the Huawei Cloud official website. 2. Download the macOS client.
Workspace_Win.msi	Used to install the PC client for Windows.	<ol style="list-style-type: none"> 1. Go to the Workspace client download page on the Huawei Cloud official website. 2. Click to download the client for Windows.
Workspace_amd64.deb	Used to install the client for AMD64. NOTE The Kylin OS and UOS are supported.	<ol style="list-style-type: none"> 1. Go to the Workspace client download page on the Huawei Cloud official website. 2. Download the client for AMD64.
Workspace_arm64.deb	Used to install the client for ARM64. NOTE The Kylin OS and UOS are supported.	<ol style="list-style-type: none"> 1. Go to the Workspace client download page on the Huawei Cloud official website. 2. Download the client for ARM64.


Procedure

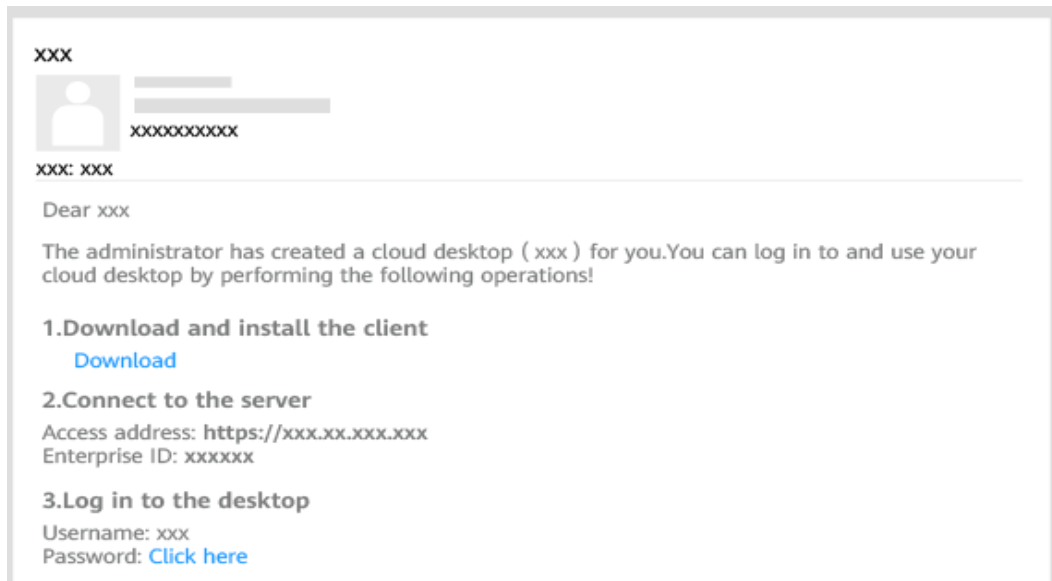
NOTE

- The PC supports the following OSs:
 - 64-bit Windows 10
 - 64-bit macOS 10.14–12.4
 - ARM64 (Kylin OS and UOS, 64-bit)
 - AMD64 (Kylin OS and UOS, 64-bit)
- When security software displays a dialog box, allow the installation to continue.

Step 1 Obtain the desktop login information email sent by the system.

NOTE

- The notification email for AD connection is slightly different from that when the AD is not connected. Refer to the actual notification email.
- If you set **User Activation** to **By administrators** and do not enter the email address and mobile number, choose **Users > Users** in the navigation pane of the console after the purchase, locate the row that contains the user, and click  in the **Desktop Count** column to obtain desktop login information.



Step 2 Install the Workspace client.

- If a macOS PC is used, you need to install a macOS client.
 - a. Copy the obtained **Workspace_mac.dmg** to a folder on the macOS PC, for example, Desktop.
 - b. Double-click the installation package.
The installation configuration window is displayed.
 - c. Double-click the **install** icon.
 - d. Click **Continue**.
 - e. Click **Install**.

If you do not want to install the SC in the default location, click **Change Install Location**.

- f. In the displayed window, enter the username and password, and click **Install Software**.

The installation takes about one minute.

- g. Click **Close**.

The macOS SC has been installed.

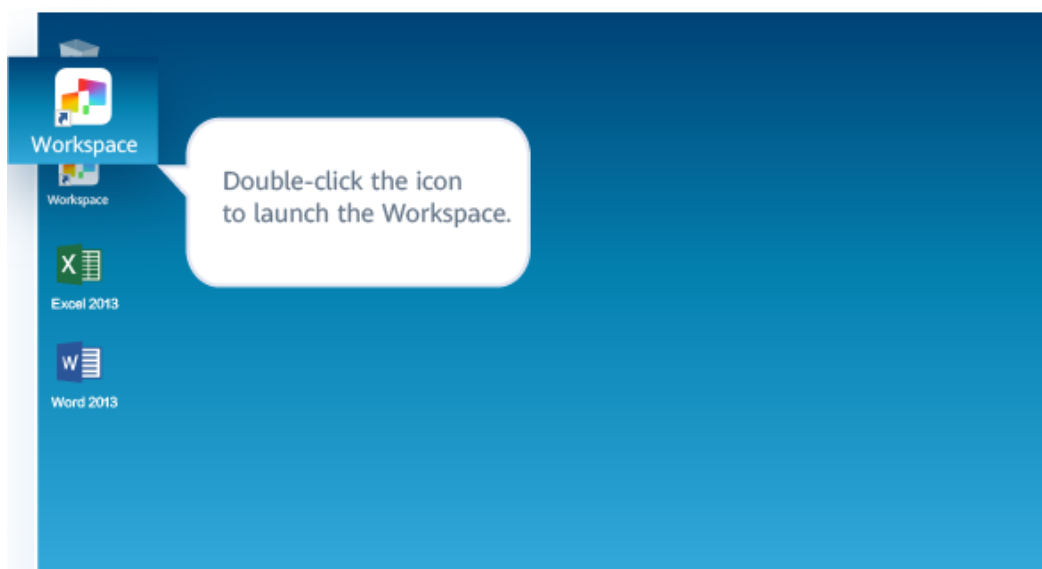
- If a Windows PC is used, you need to install a Windows client.
Double-click the obtained **Workspace_Win.msi** client software package and install it as prompted.

Step 3 Start the client.

NOTE

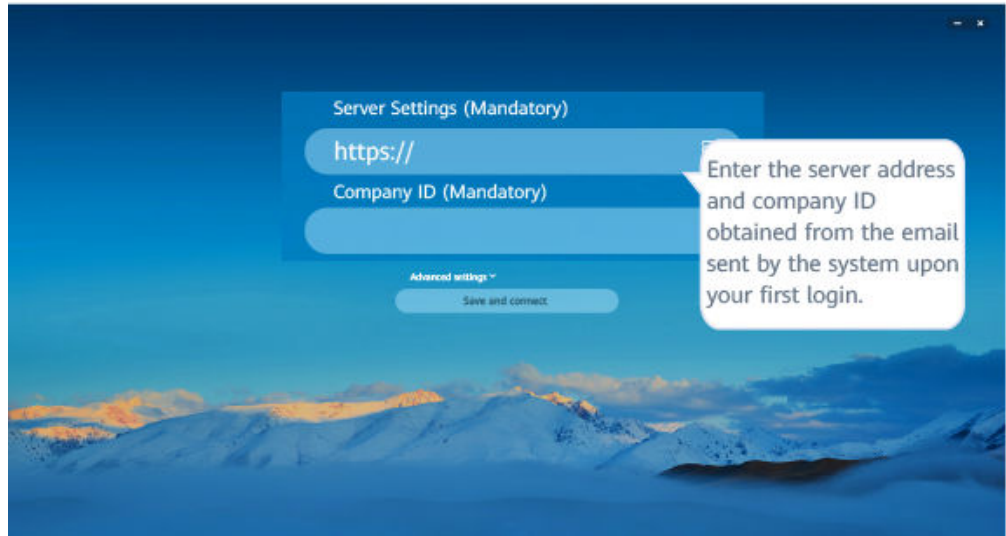
If a macOS PC is used, you need to set the system preference before starting the client for the first time. Otherwise, you cannot enter characters on the cloud desktop.

Choose **System Preferences > Security & Privacy > Input Monitoring**, select **HDPViewer**, and switch the input mode to English.



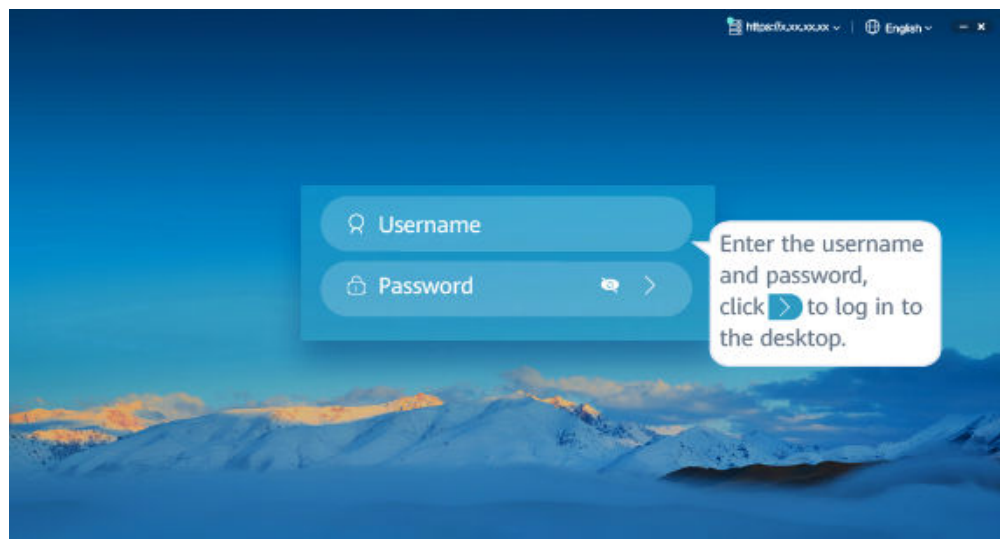
Step 4 Configure the server IP address and enterprise ID.

- **Figure 5-3** Configuring the server IP address and enterprise ID



Step 5 Log in to the desktop, as shown in [Figure 5-4](#).

Figure 5-4 Logging in to a desktop



NOTE

- If the account has multiple desktops, enter the username and password and click **Log In**. The desktop list page is displayed. You need to click the target desktop to access it.
- If multi-factor authentication has been enabled, you need to pass the multi-factor authentication again before accessing the cloud desktop.

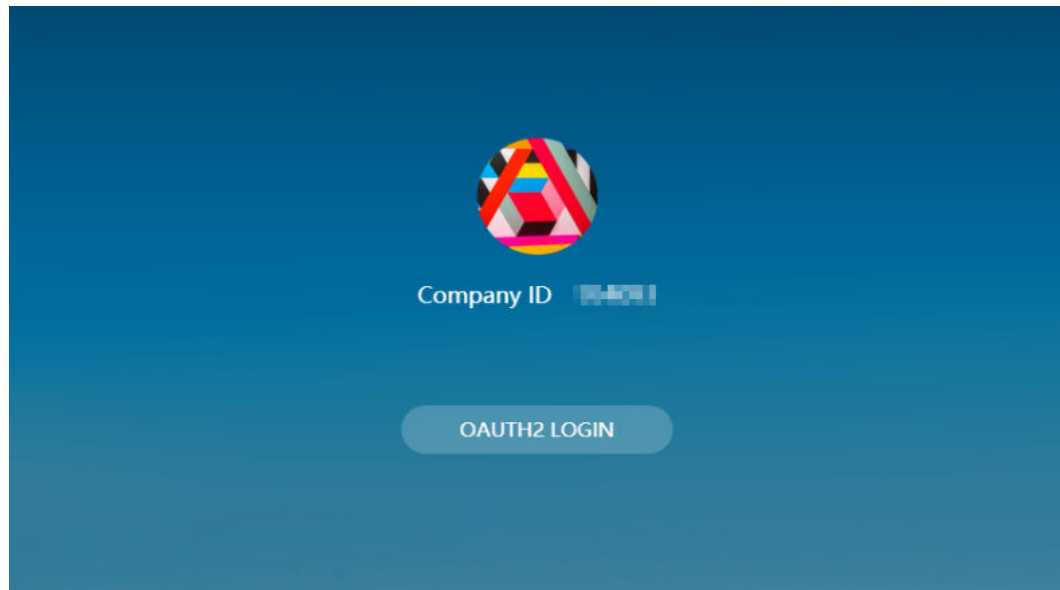
Step 6 (Optional) Perform third-party SSO.

The administrator configures the OAuth 2.0 authentication mode for logging in to the cloud desktop. For details, see the OAuth 2.0 procedure in [Third-Party SSO](#).

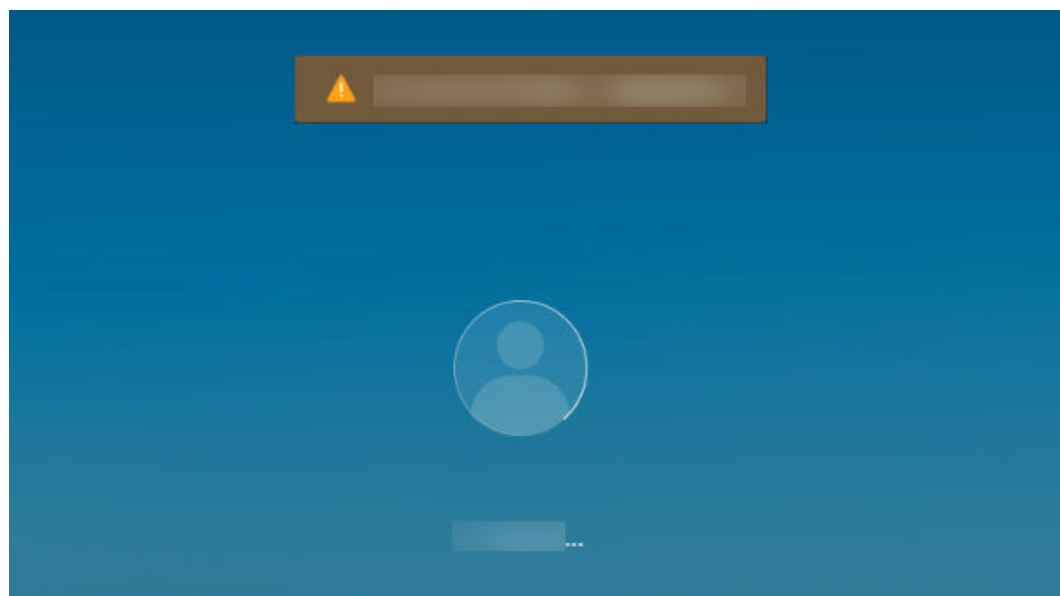
- After third-party authentication is enabled, the OAuth 2.0 login mode is used.

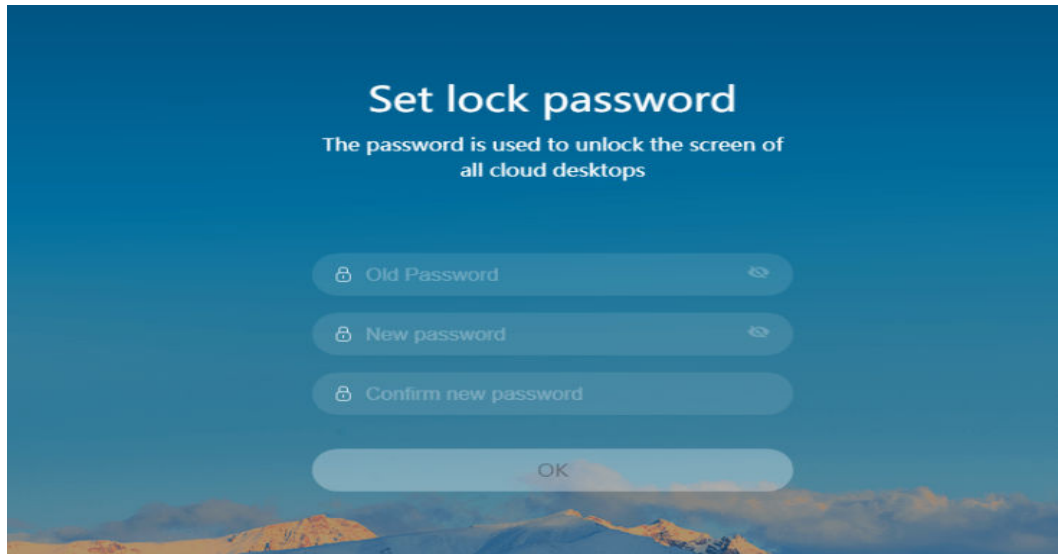
 NOTE

The username on the third-party platform must be the same as that on the cloud desktop. Otherwise, the verification fails.



- Enter the username and password of the third-party application platform to log in to the cloud desktop.
- If the third-party platform authentication mode is used, the system prompts you to reset the password when you log in to the cloud desktop for the first time.





NOTE

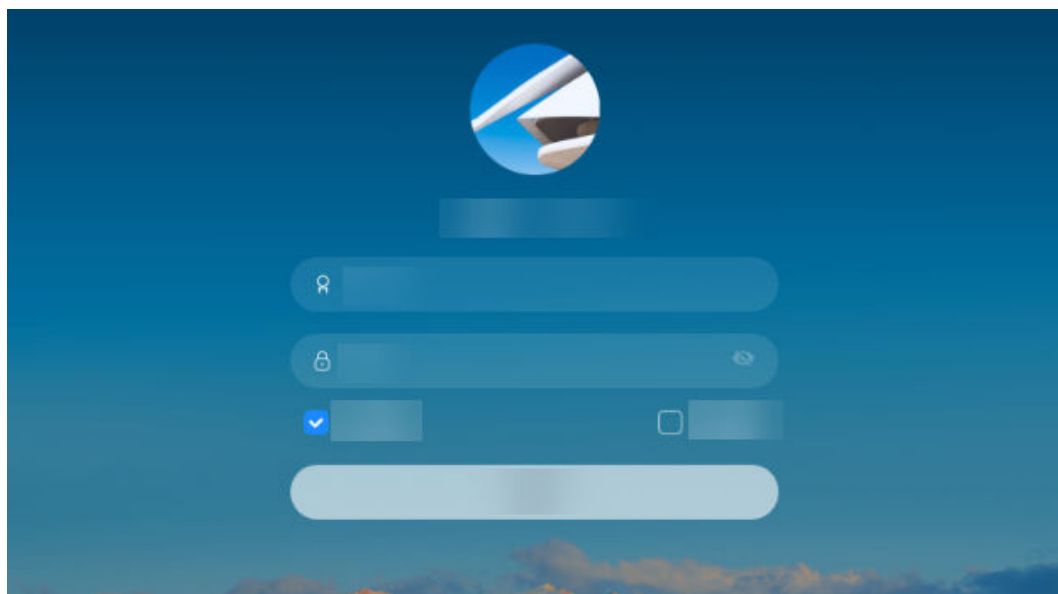
- In the AD scenario, when you log in to the cloud desktop, the page for resetting the password is not displayed.
- The reset password is the password for unlocking the cloud desktop.
- In the AD scenario, after you go to the desktop list page and click the target desktop, you need to enter the password of the cloud desktop again for login.

The administrator configures the LDAP authentication mode for logging in to the cloud desktop. For details, see [Third-Party SSO](#).

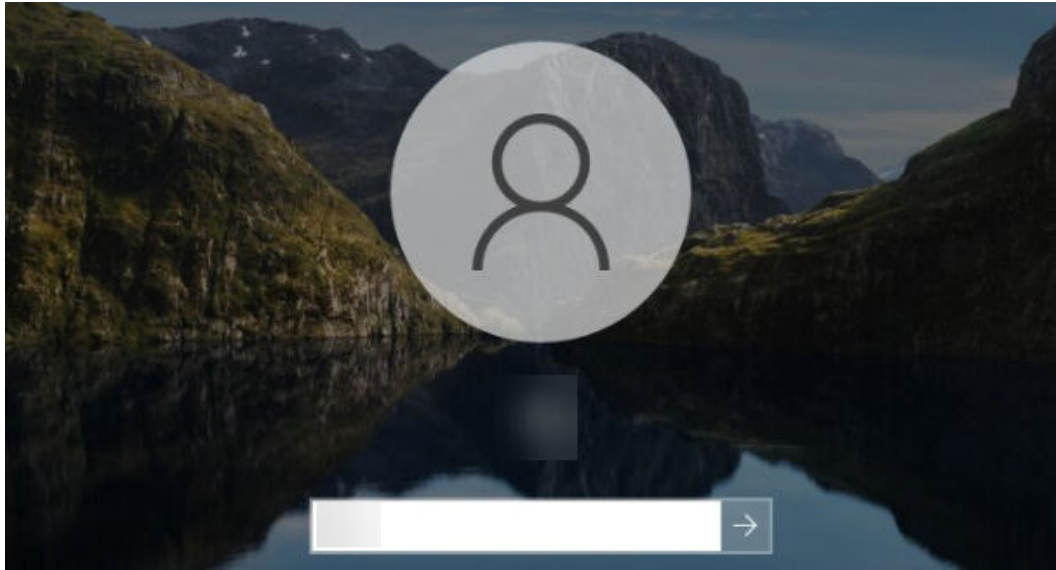
- After third-party authentication is enabled, the LDAP login mode is used.
- Enter the username and password of the LDAP platform for login.

NOTE

The entered LDAP user must be the same as the cloud desktop user. Otherwise, the verification fails.



- Click the target desktop. When the AD is connected, you need to enter the password again for login.



NOTE

- When the AD is connected:
 - The Windows cloud desktop uses the username and password of the AD.
 - The Linux cloud desktop uses the username and password of LDAP.
- When the AD is not connected:
 - The Windows and Linux cloud desktops use the username and password of LDAP.

Step 7 (Optional) Perform multi-factor authentication.

You need to perform authentication again only when the administrator has enabled **multi-factor authentication**.

- After multi-factor authentication is enabled, you need to bind a virtual MFA device to the desktop upon the first login.



- a. Download and install an application that supports TOTP on a smart device, such as a mobile phone.

- b. On the MFA tool page of the smart device, select the QR code scanning mode or manual input mode to bind the device.

NOTE

Your operation is subject to the application you use.

- If you choose to scan the QR code, scan the QR code in the **Scanning** area of the multi-factor authorization page of the Workspace client.
 - If you choose to manually input, on the MFA tool page of the smart device, enter the account and key in the **Manually** area of the multi-factor authorization page of the Workspace client.
- c. Enter the dynamic verification code generated by the virtual MFA device bound to the smart device in the verification code text box on the Workspace client.



NOTE

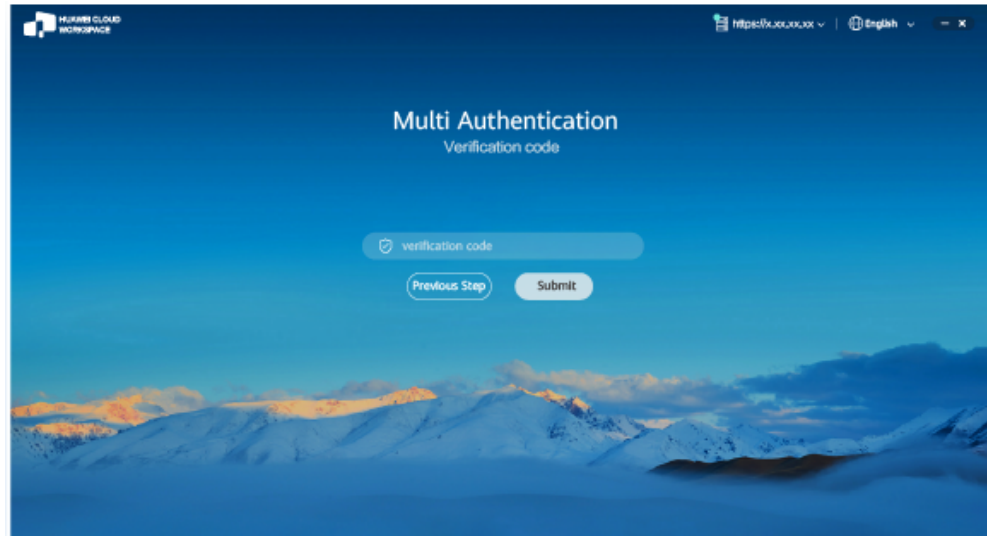
The preceding verification code page is only an example. The actual page varies depending on the application in use.

- d. On the multi-factor authorization page of the Workspace client, click **Binding**.

NOTE

If the account has multiple desktops, the desktop list page will be displayed after you click **Binding**. You need to click the target desktop to access it.

- After multi-factor authentication is enabled, use the proprietary authentication system of Huawei Cloud. If this is not the first time of login to the desktop, use the proprietary authentication system of the enterprise and directly enter the verification code for authentication.



- a. Open an application that supports TOTP on a smart device, such as a mobile phone, and access the MFA tool page.
- b. Enter the dynamic verification code generated by the virtual MFA device bound to the smart device in the verification code text box on the Workspace client.



NOTE

The preceding verification code page is only an example. The actual page varies depending on the application in use.

- c. On the multi-factor authorization page of the Workspace client, click **Submit**.

 NOTE

If the account has multiple desktops, the desktop list page will be displayed after you click **Submit**. You need to click the target desktop to access it.

----End

5.3 Using a Mobile Terminal

Scenarios

This section provides instructions for end users to log in to their computers using mobile terminals.

Mobile terminals running Android 6.0 or later are supported. You can use the stylus to perform operations.

 NOTE

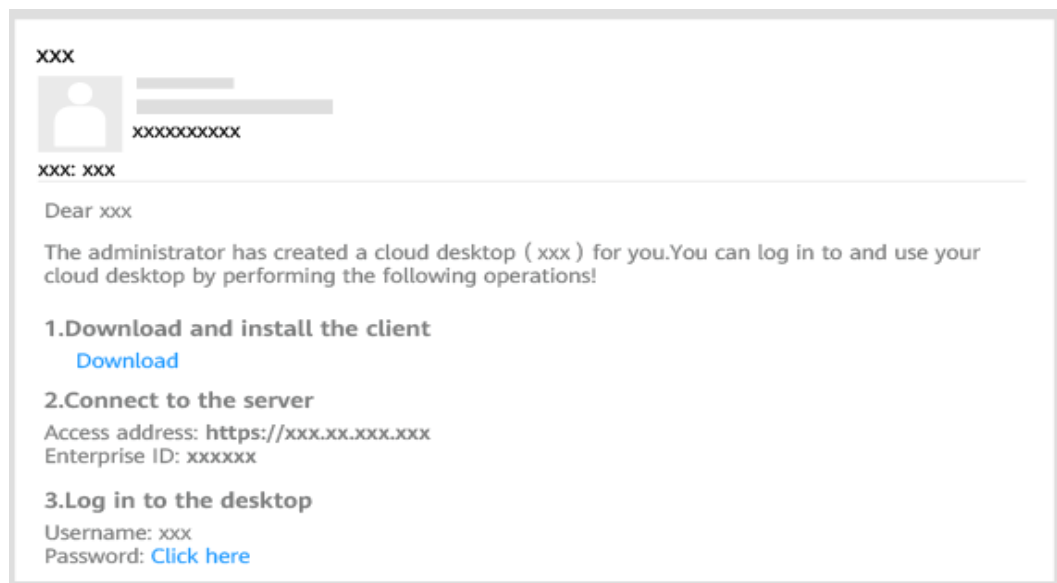
The operations on different mobile terminals are similar. The following uses the operations on a mobile phone as an example.

Procedure

Step 1 Obtain the desktop login information email sent by the system.

 NOTE

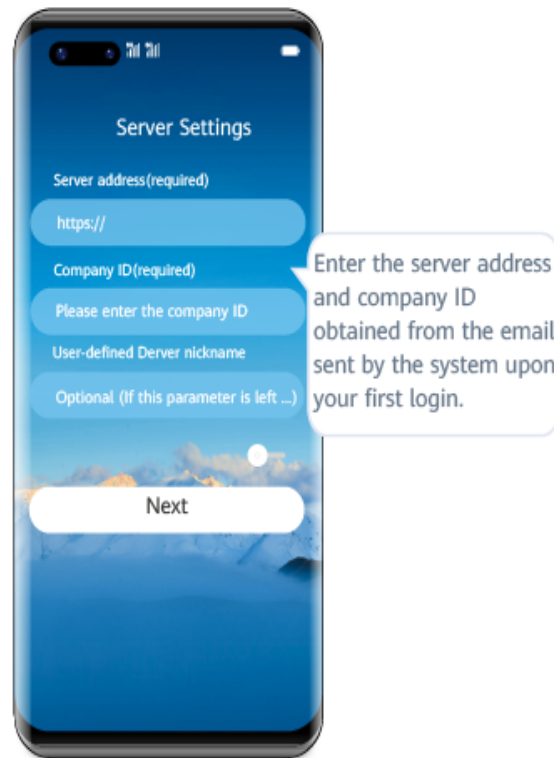
The notification email for AD connection is slightly different from that when the AD is not connected. Refer to the actual notification email.



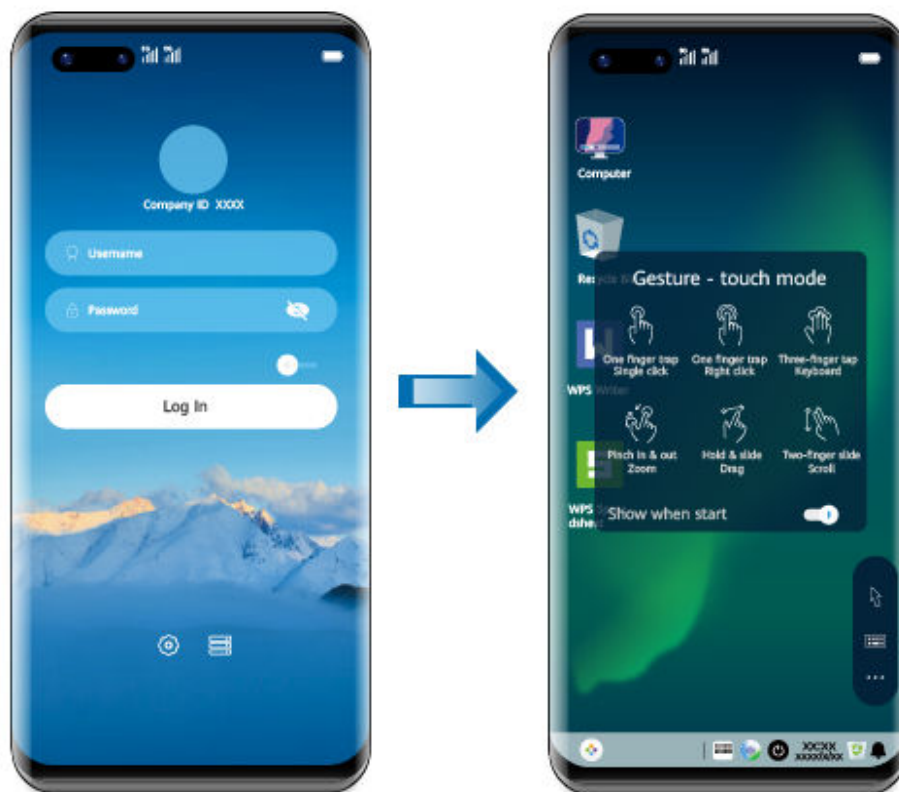
Step 2 Obtain the client as prompted in the system email.

Step 3 Enable the client and configure the server address and enterprise ID as prompted.

- Configure the server address and enterprise ID on the server setting page.



Step 4 Enter the username and password to log in to the desktop. Upon the first login, you can use gestures to adapt to the desktop.



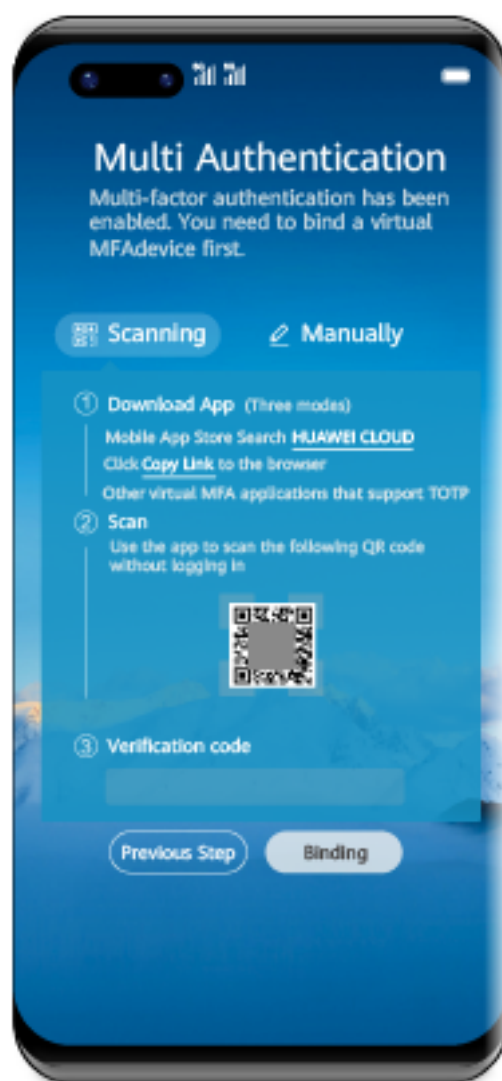
NOTE

- If the account has multiple desktops, enter the username and password and click **Log In**. The desktop list page is displayed. You need to click the target desktop to access it.
- If multi-factor authentication has been enabled, you need to pass the multi-factor authentication again before accessing the cloud desktop.

Step 5 (Optional) Perform multi-factor authentication.

You need to perform authentication again only when the administrator has enabled **multi-factor authentication**.

- After multi-factor authentication is enabled, you need to bind a virtual MFA device to the desktop upon the first login.



- a. Download and install an application that supports TOTP on a smart device, such as a mobile phone, and access the MFA tool page.
- b. On the MFA tool page of the smart device, select the QR code scanning mode or manual input mode to bind the device.

 NOTE

Your operation is subject to the application you use.

- If you choose to scan the QR code, scan the QR code in the **Scanning** area of the multi-factor authorization page of the Workspace client.
 - If you choose to manually input, on the MFA tool page, enter the account and key in the **Manually** area of the multi-factor authorization page of the Workspace client.
- c. Enter the dynamic verification code generated by the virtual MFA device bound to the smart device in the verification code text box on the Workspace client.



 NOTE

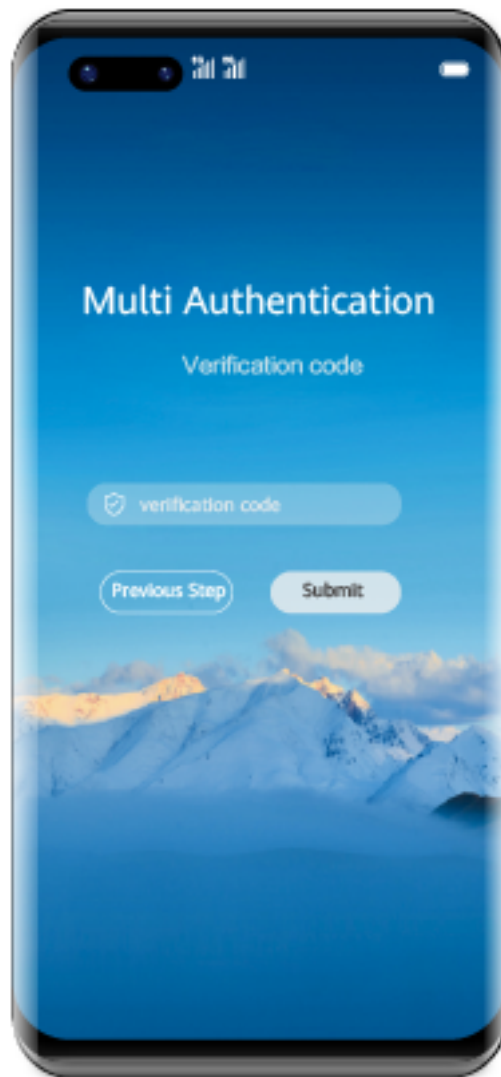
The preceding verification code page is only an example. The actual page varies depending on the application in use.

- d. On the multi-factor authorization page of the Workspace client, click **Binding**.

 NOTE

If the account has multiple desktops, the desktop list page will be displayed after you click **Binding**. You need to click the target desktop to access it.

- After multi-factor authentication is enabled, use the proprietary authentication system of Huawei Cloud. If this is not the first time of login to the desktop, use the proprietary authentication system of the enterprise and directly enter the verification code for authentication.



- a. Open the installed application that supports TOTP on the smart device, such as a mobile phone, and access the MFA tool page.
- b. Enter the dynamic verification code generated by the virtual MFA device in the verification code text box on the Workspace client.

**NOTE**

The preceding verification code page is only an example. The actual page varies depending on the application in use.

- c. On the multi-factor authorization page of the Workspace client, click **Submit**.

NOTE

If the account has multiple desktops, the desktop list page will be displayed after you click **Submit**. You need to click the target desktop to access it.

----End

5.4 Logging In to a Desktop Using a Browser

Scenarios

Log in to a user desktop using a browser.

NOTE

- Use Chrome 64bit(75), Edge 64bit(108), or a later version to log in to the desktop.
- The following procedure uses a Windows PC as an example. The detailed procedure varies depending on the operating system.

Procedure

- Step 1** Obtain the desktop login information email sent by the system.

NOTE

The notification email for AD connection is slightly different from that when the AD is not connected. Refer to the actual notification email.



Step 2 Open the browser and configure the access address.



Step 3 Enter the enterprise ID, user name, password, and other login information, select I have read and agree to the User Privacy Policy, and click Log In.

Step 4 The Workspace page is displayed. Click the workspace to be logged in to.

NOTE

- When you log in to the browser for the first time, an interception window is displayed. You need to manually configure the browser to allow the window to pop up, as shown in.
- When you log in to the system for the first time, a certificate verification dialog box is displayed. You need to manually set the certificate. Click Advanced to continue, as shown in.

Figure 5-5 Browser pop-up window



Figure 5-6 Certificate verification



----End

A Change History

Released On	Description
2023-12-01	This issue is the fourth official release. Added: Logging In to a Desktop Using a Browser
2023-09-20	This issue is the third official release. Added: <ul style="list-style-type: none">• Purchasing Yearly/Monthly-billed Desktop Pools• Purchasing Pay-per-Use Desktop Pools
2023-07-03	This issue is the second official release. Added: "Third-Party SSO" in Using a Soft Client .
2022-12-26	This issue is the first official release.