

Workspace

User Guide (End Users)

Issue: 01

Date: 2022-12-26



Copyright © Huawei Technologies Co., Ltd. 2022. 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



and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and registered trademarks mentioned in this document are the property of their respective holders.

Notice

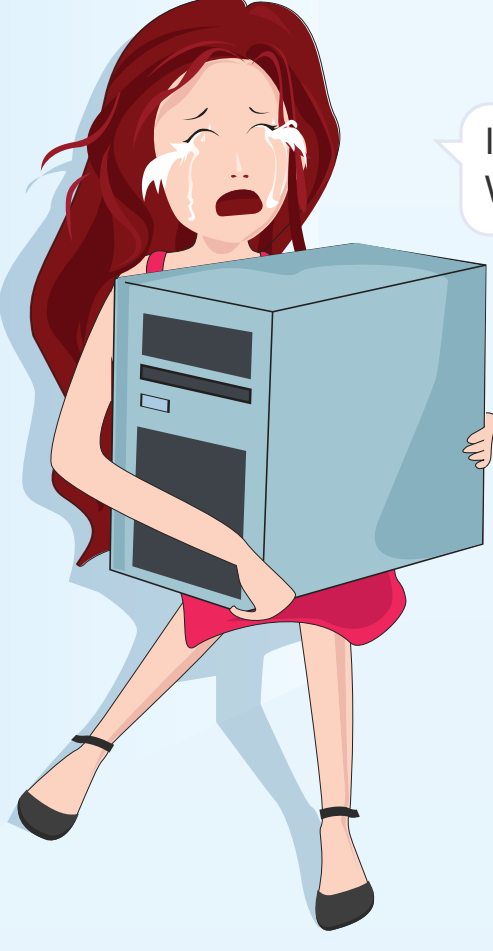
The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements,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

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

Contents

- 01 Getting to Know Workspace
- 02 Introduction to Terminals
- 03 Logging In to a Desktop Using a TC
- 04 Logging In to a Desktop Using a SC
- 05 Logging In to a Desktop Using a Mobile Terminal
- 06 Desktop Assistant
- 07 Changing the Login Password
- 08 Forbidden Operations
- 09 Configuring Dual-Screen Display
- 10 Common Function Configuration
- 11 Change History

Getting to Know Workspace



It's so heavy. Who can help me?

Thin clients can replace conventional PCs and are much smaller and much lighter.

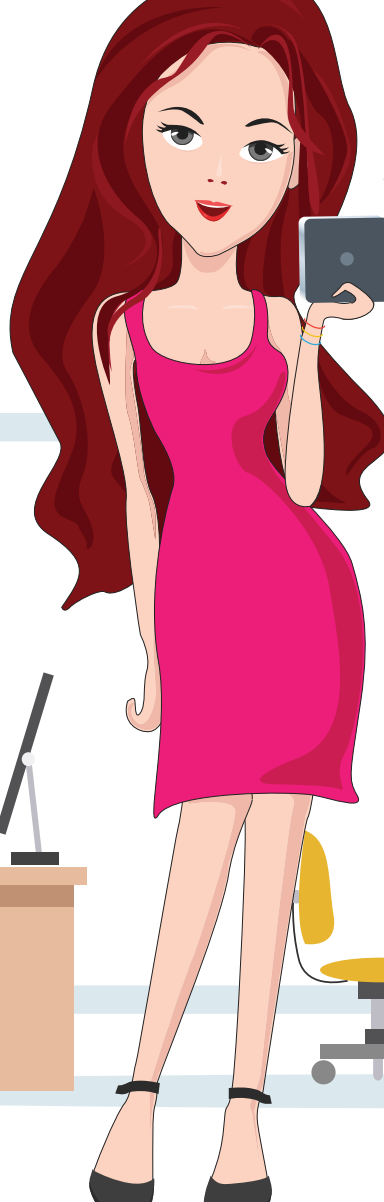


With TCs, I no longer need to worry about moving my workplace to another location.

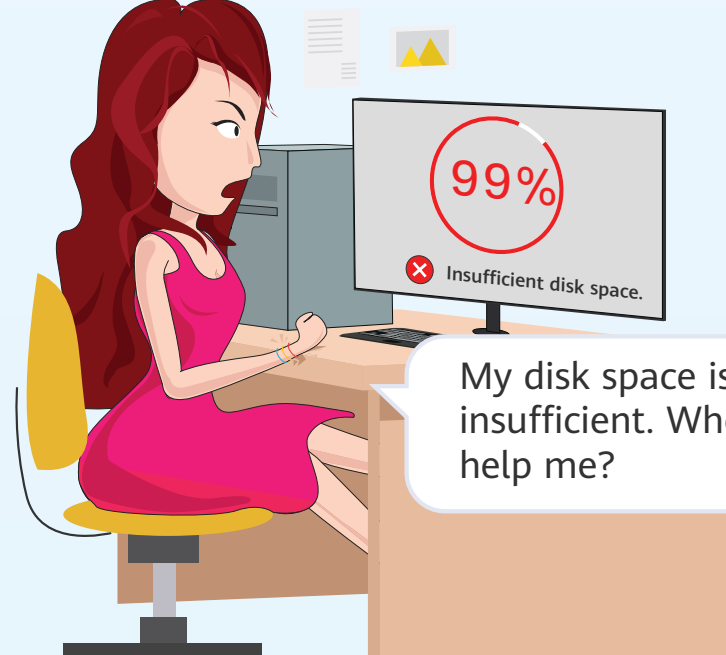


My data is lost due to power outage. Who can help me?

You can try to use Workspace, which offers high security and reliability by migrating data to the cloud.



With Workspace, my data is well protected in the cloud and will not be lost due to power outage.

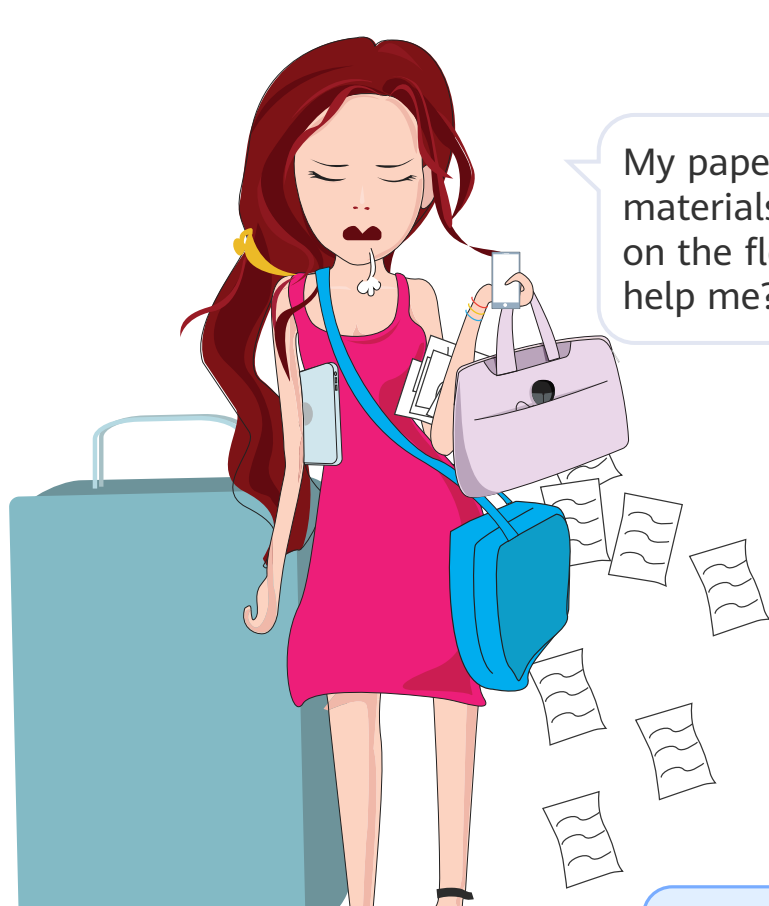


My disk space is insufficient. Who can help me?

You can try to use Workspace, which enables you to expand your virtual disks with one click.

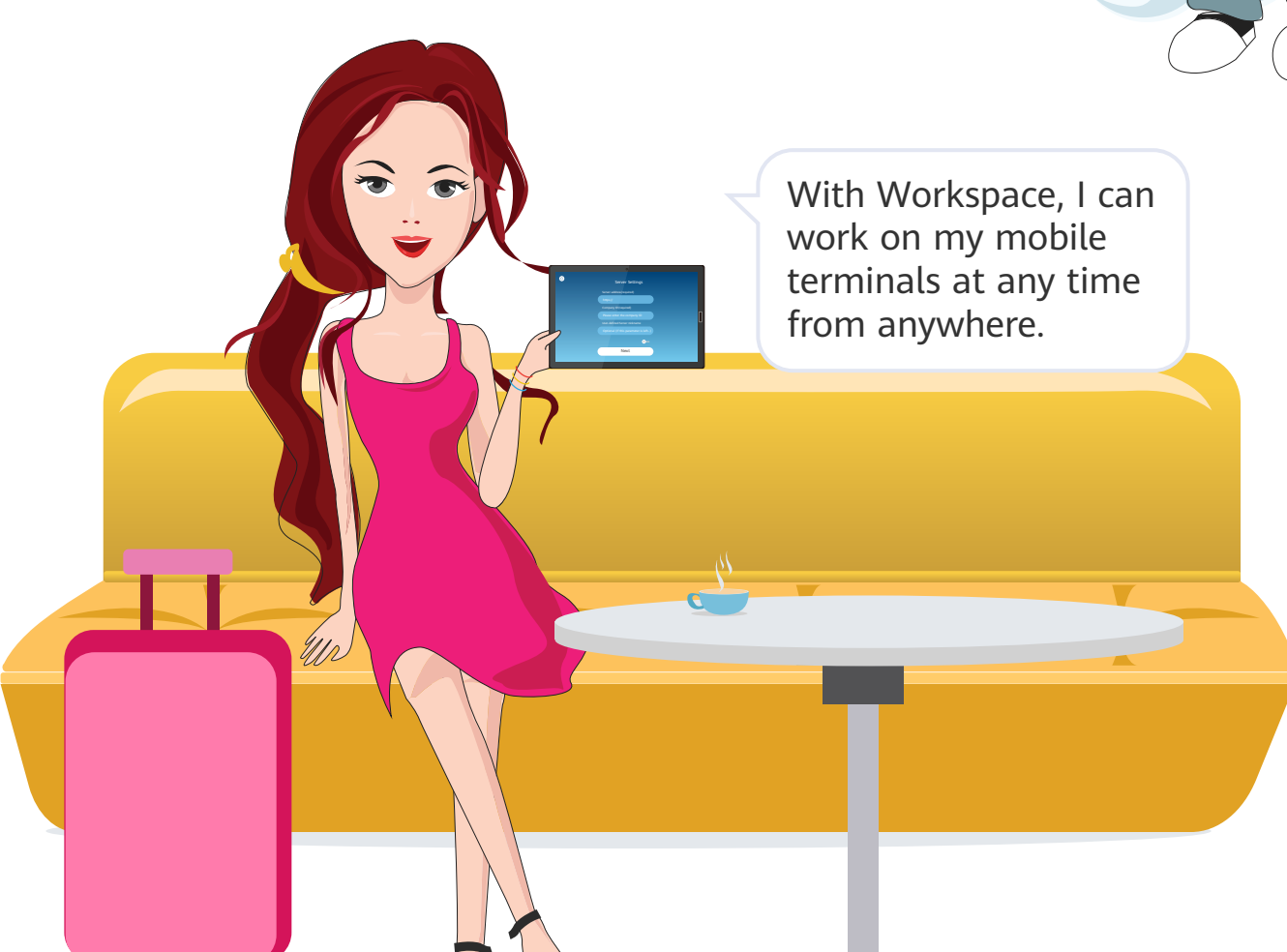


With Workspace, I can quickly and easily expand my virtual disks depending on changing needs.



My paper office materials are scattered on the floor. Who can help me?

You can try to use Workspace, which enables you to work at any time from anywhere.



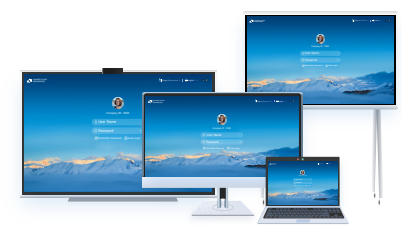
With Workspace, I can work on my mobile terminals at any time from anywhere.

Introduction to Terminals



Supported Terminals

Workspace is accessible to TCs, software clients (SCs), and mobile clients. Internet-connected terminals can access Workspace.



SCs (for PC reuse)

After installing an SC on your existing PC, you can access Workspace from your PC. In this way, your PC can be reused.



TCs

TCs are smaller in size and energy-saving, which can be used to access Workspace in multiple application scenarios.



Mobile Clients

Supports Android smart terminals, enabling mobile office anytime, anywhere.

About TCs

Take the HT3300 as an example.

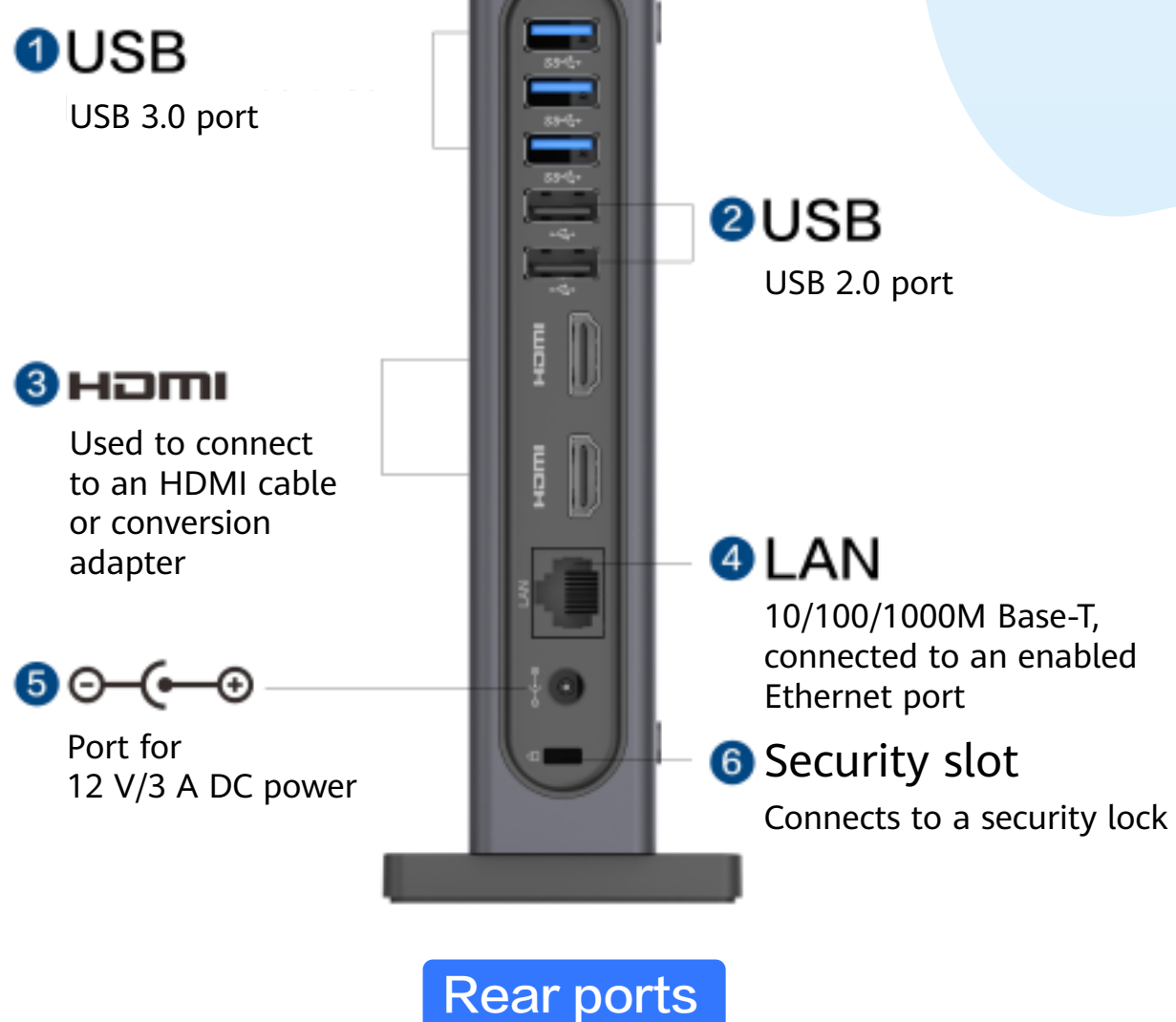
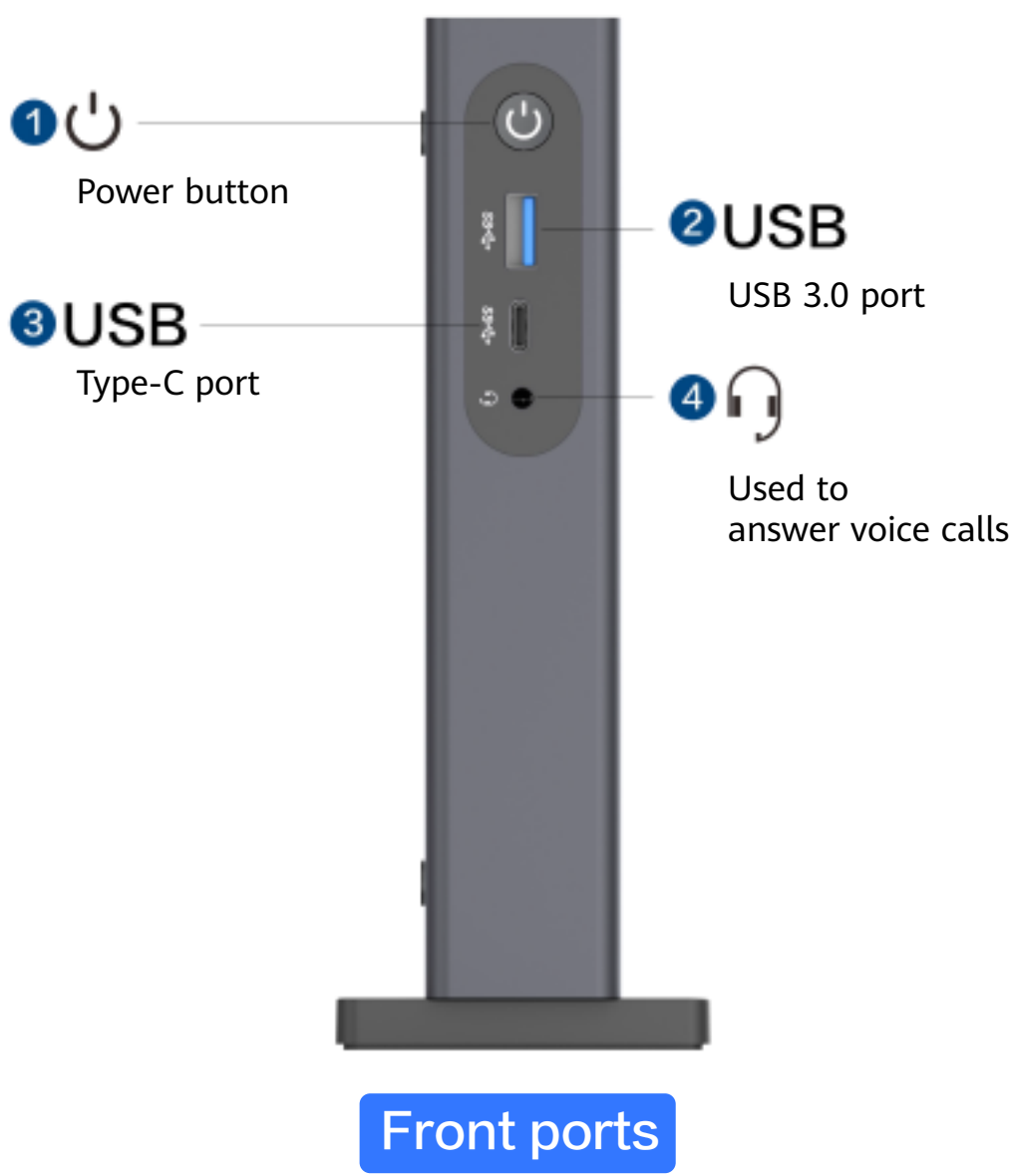


HT3300

Built on the 4-core Arm architecture, HT3300 runs UOS and features high performance and low power consumption. It is applicable to multimedia classrooms and OA.


About ports

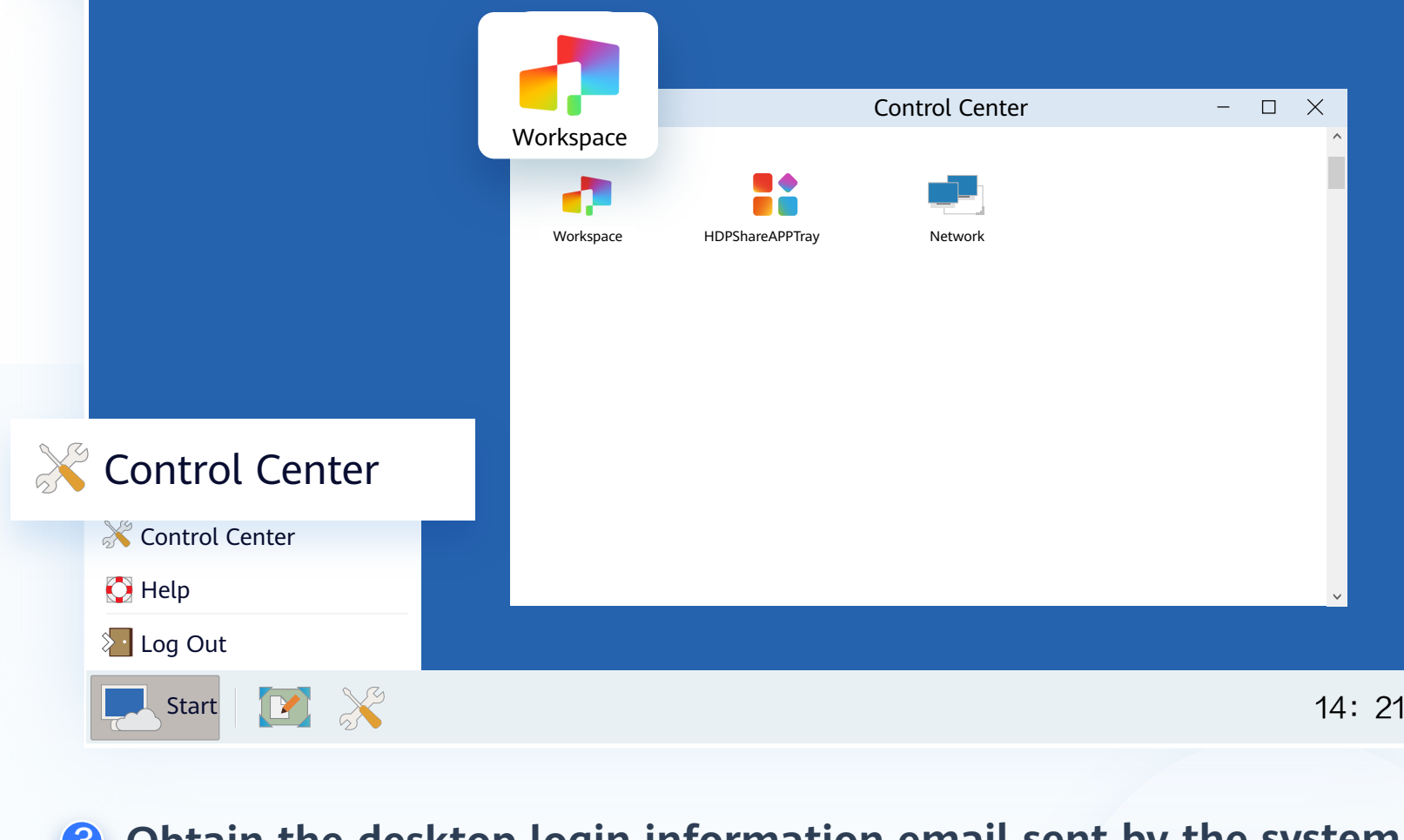
Take the HT3300 as an example to describe the TC port diagram.



Logging In to a Desktop Using an TC

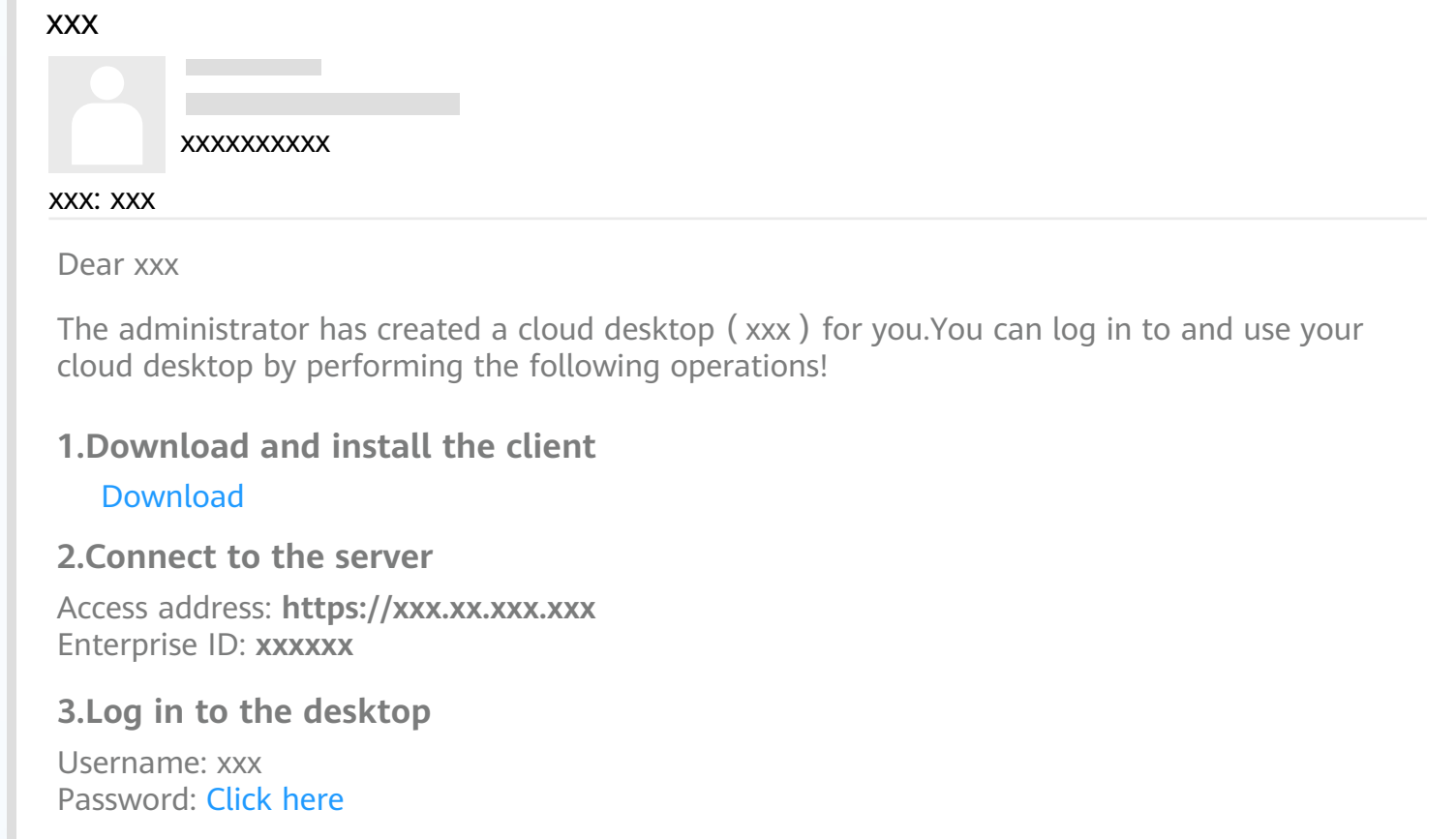
- 1 Connect the cables and power on the TC.
- 2 For the first login, choose **Start > Control Center** on the TC desktop and open the cloud client.

Note: When some TCs are powered on, the software list page including the cloud desktop client is displayed. You can click  to access the cloud desktop server configuration page. The actual TC information prevails.

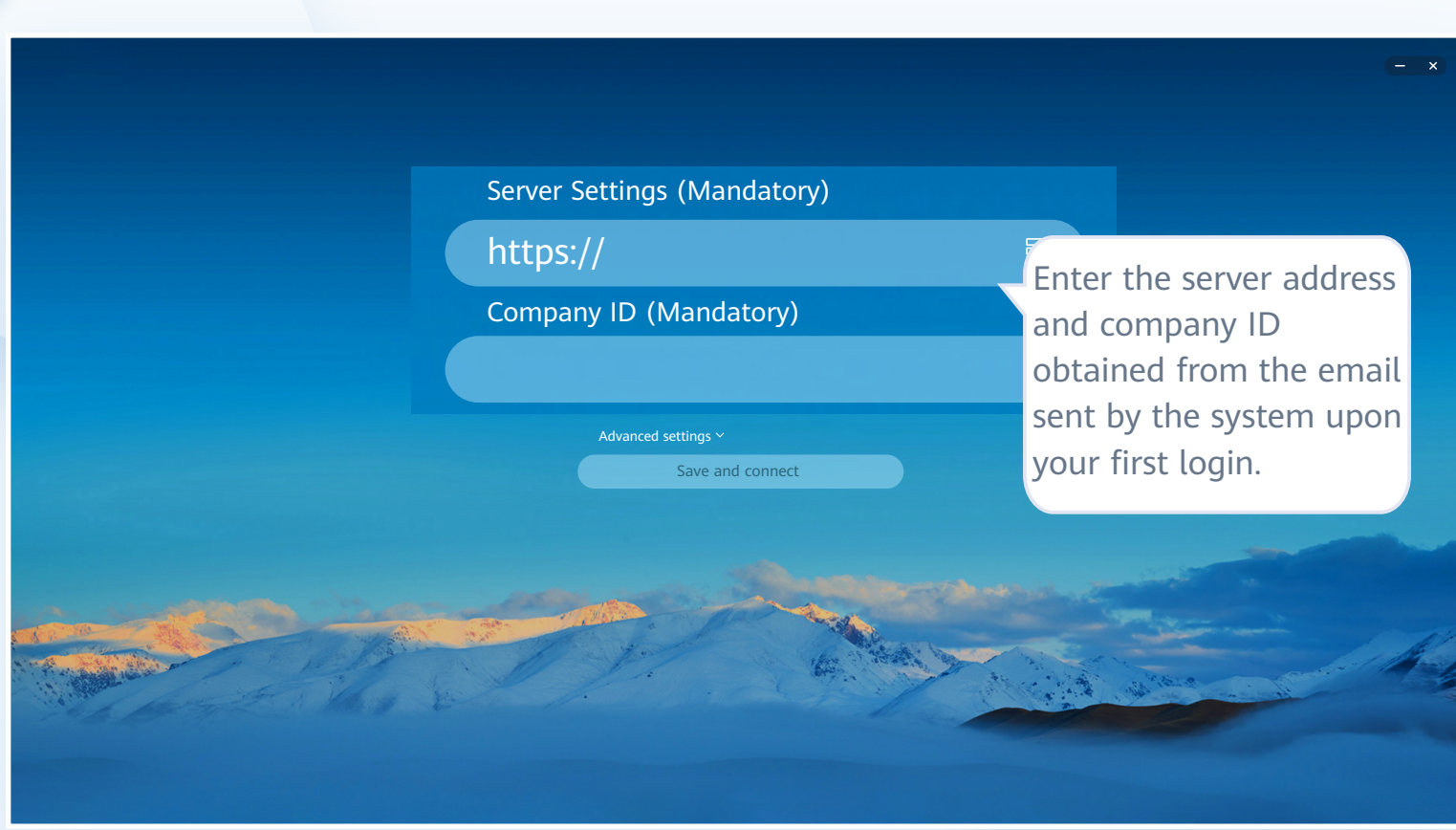


- 3 Obtain the desktop login information email sent by the system.

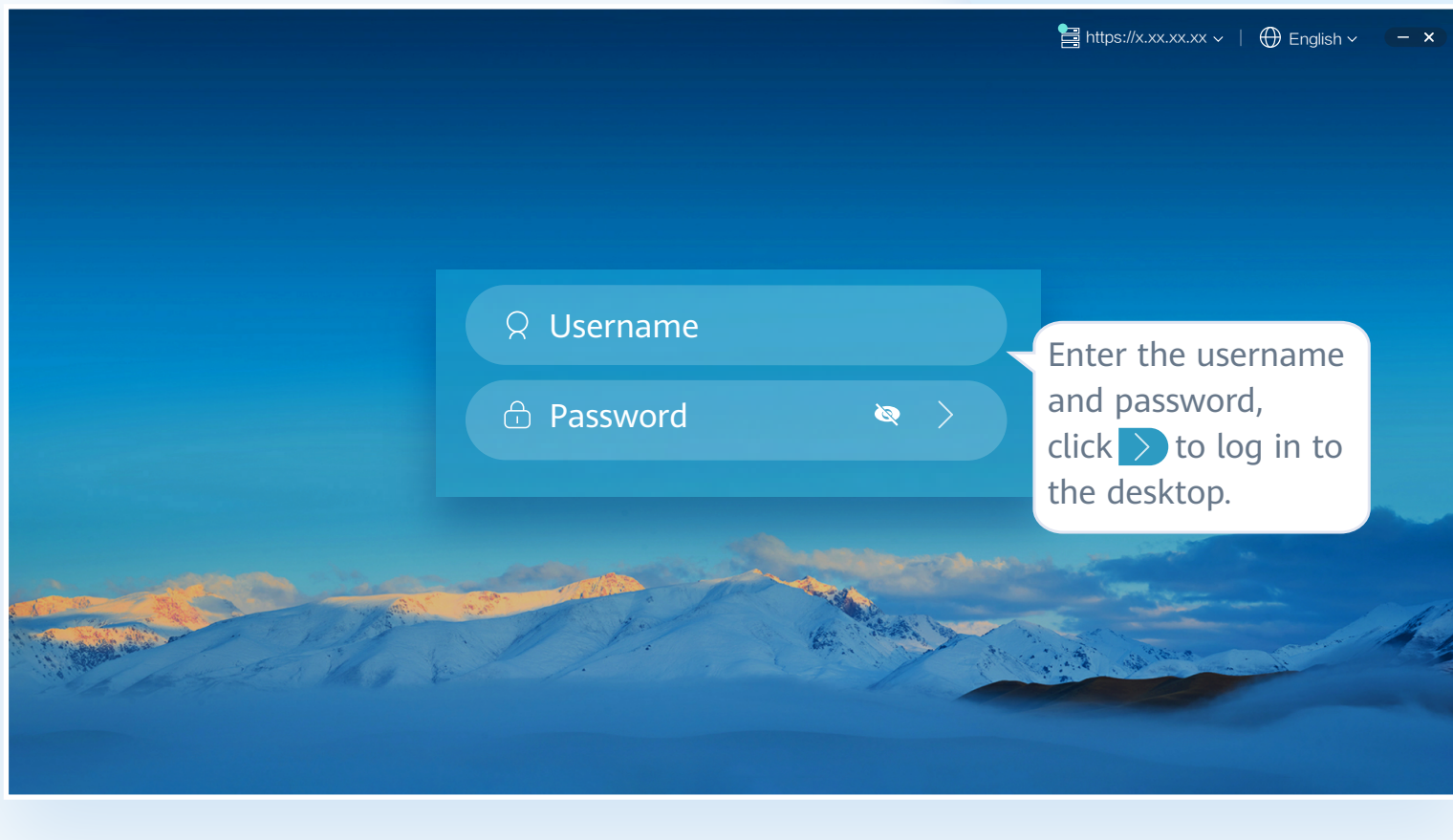
Note: The notification email for connecting to the AD is slightly different from that when the AD is not connected. Refer to the email you receive.




- 4 Configure server information.



- 5 Log in to the desktop.



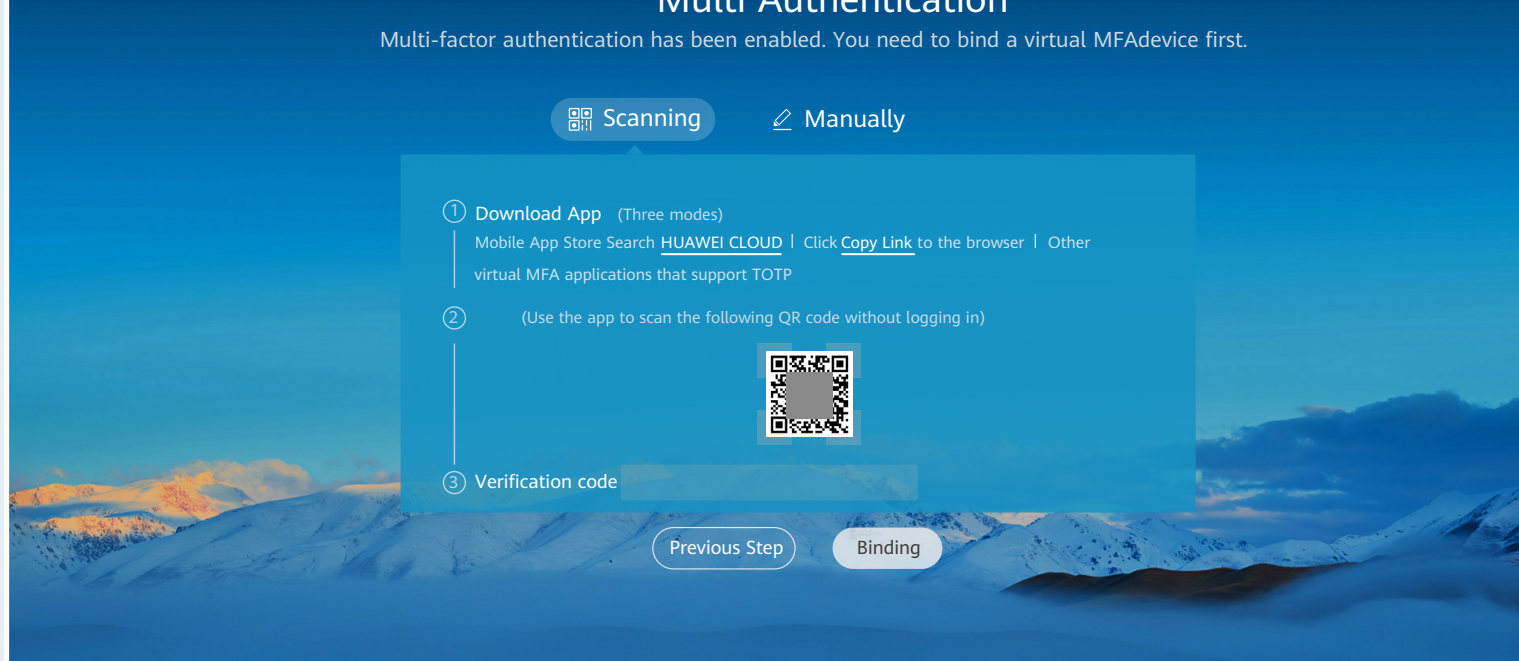
Note: If the user has multiple desktops, enter the user name and password, and click . The desktop list page is displayed. You need to click the target desktop to access the corresponding desktop.

After multi-factor authentication is enabled, you need to pass the dynamic verification code again to log in to the cloud desktop.

- 6 (Optional) Perform multi-factor authentication.

Note: 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.

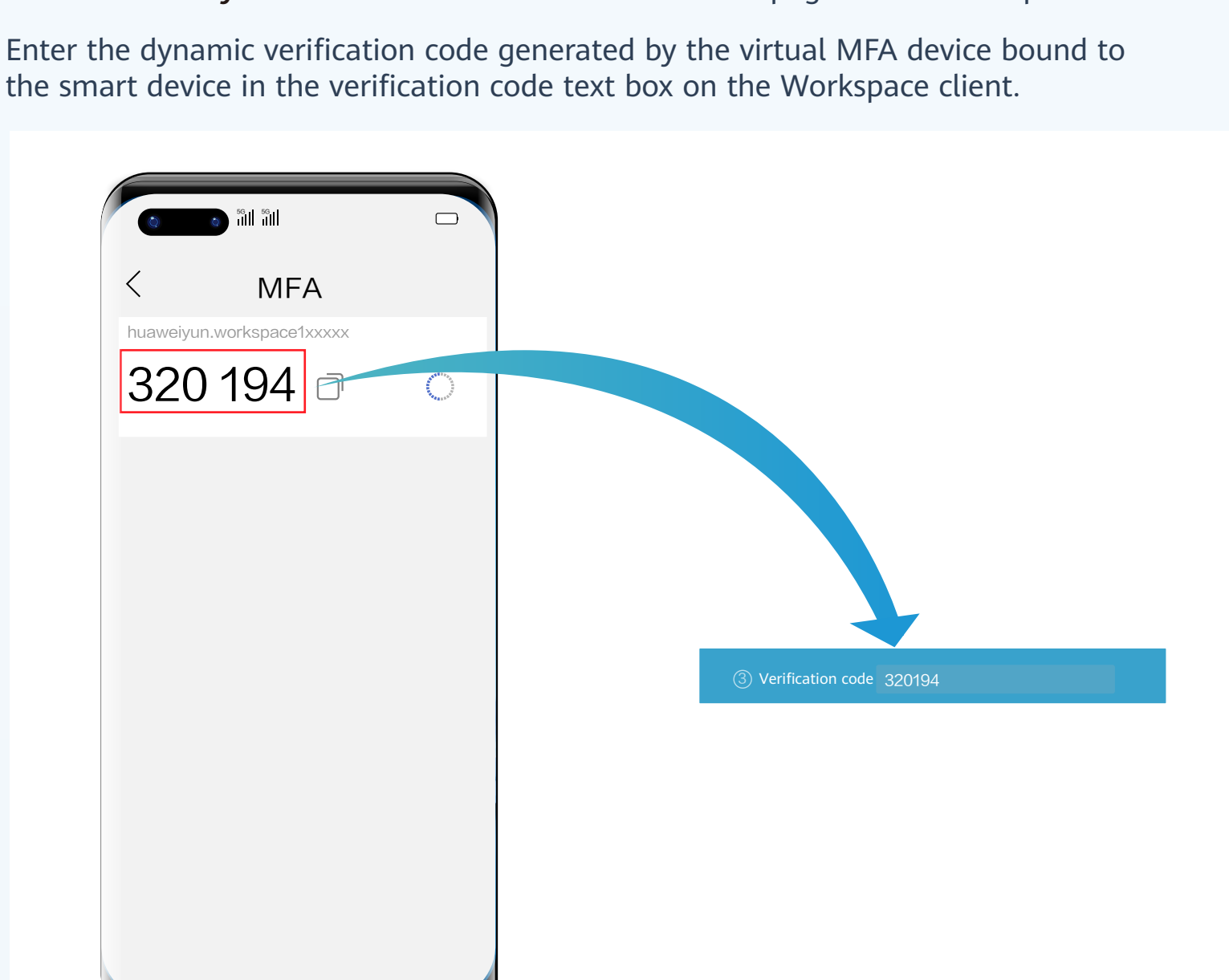


- 1 Download and install an application that supports TOTP on a smart device, such as a mobile phone, and access the MFA tool page.
- 2 On the MFA tool page of the smart device, select the QR code scanning mode or manual input mode to bind the device.

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.

- 3 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.

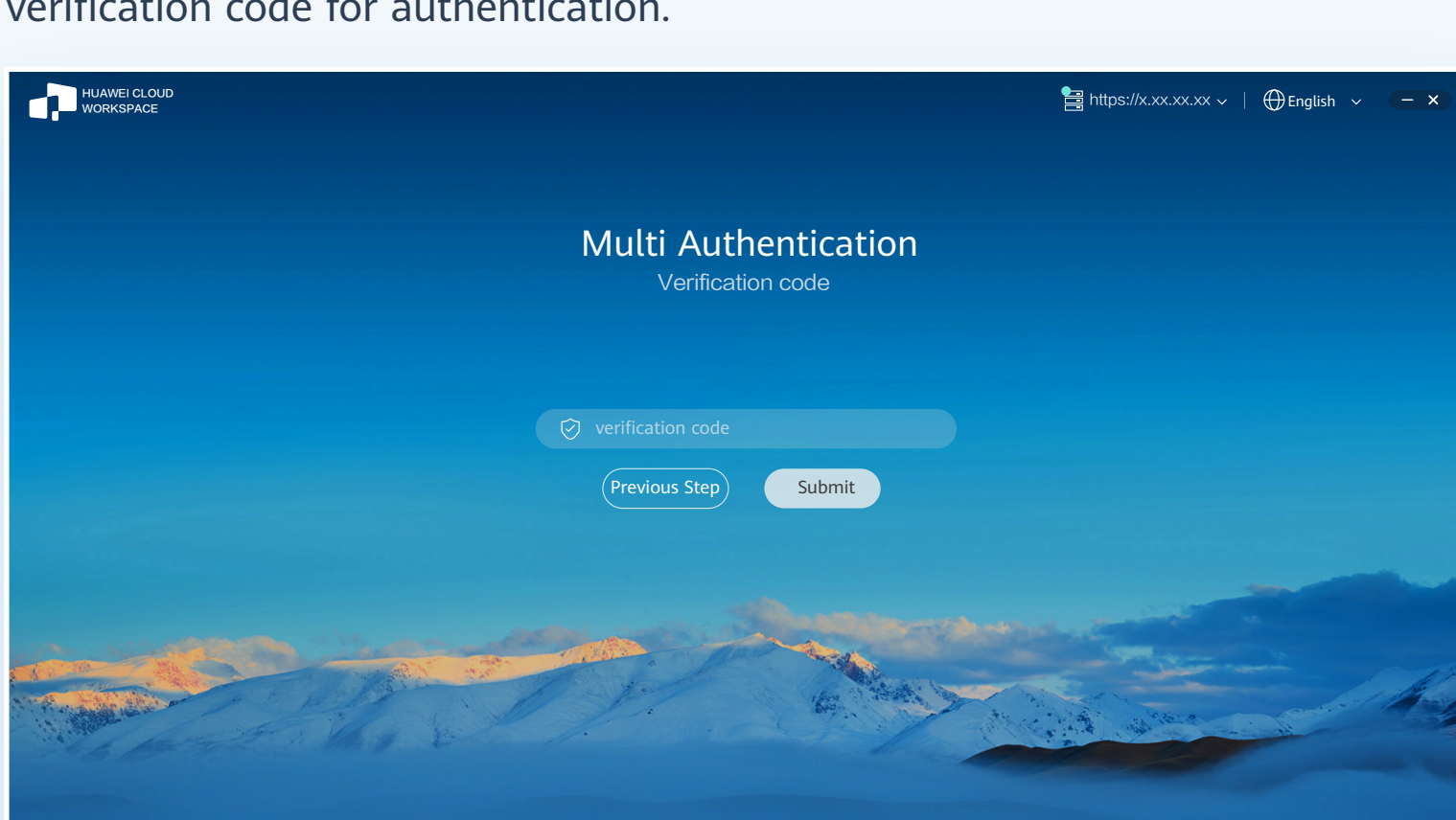


Note: The preceding verification code page is only an example. The actual page varies depending on the application in use.

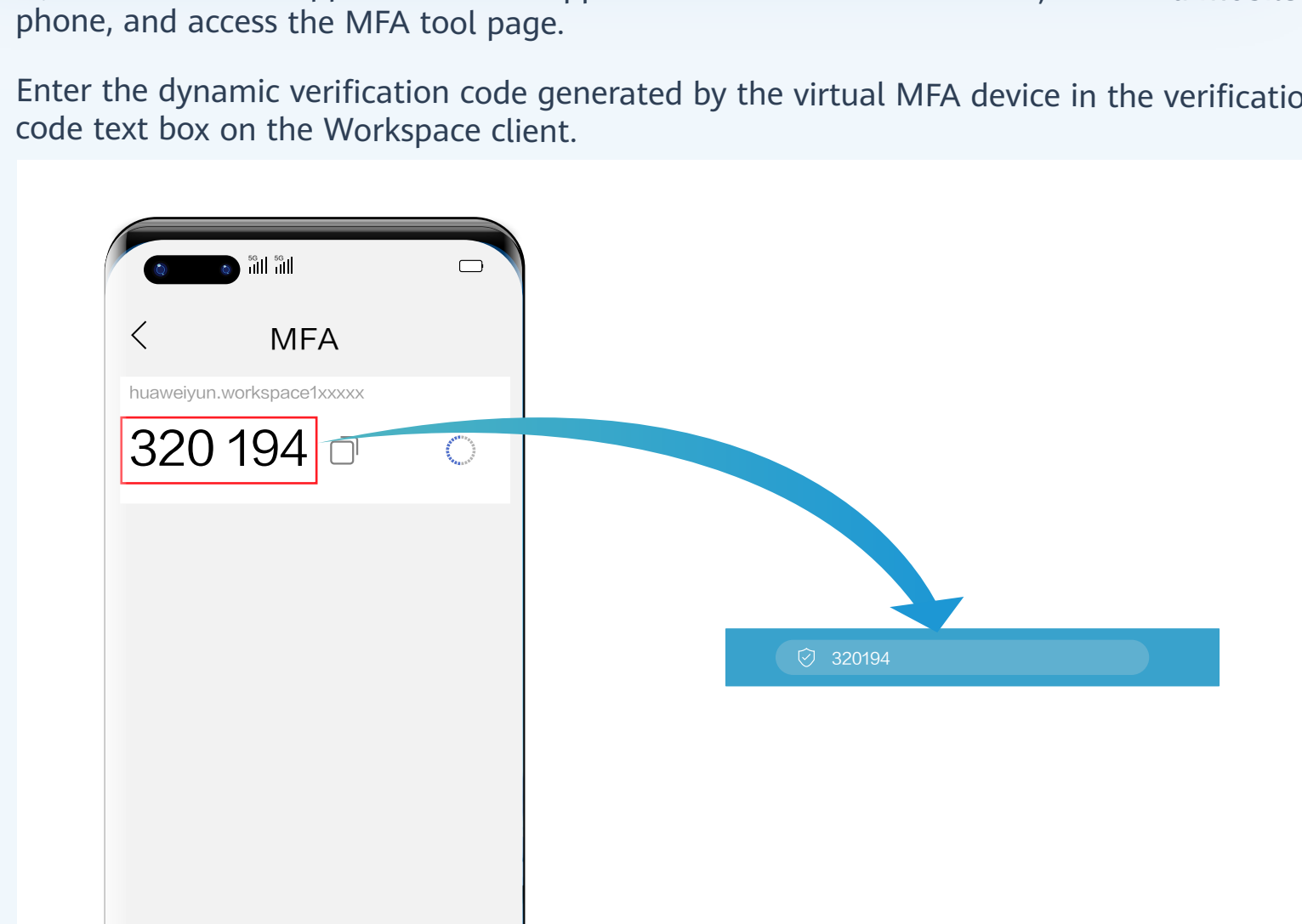
- 4 On the multi-factor authorization page of the Workspace client, click **Binding**.

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.



- 1 Open the installed application that supports TOTP on the smart device, such as a mobile phone, and access the MFA tool page.
- 2 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.

- 3 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.

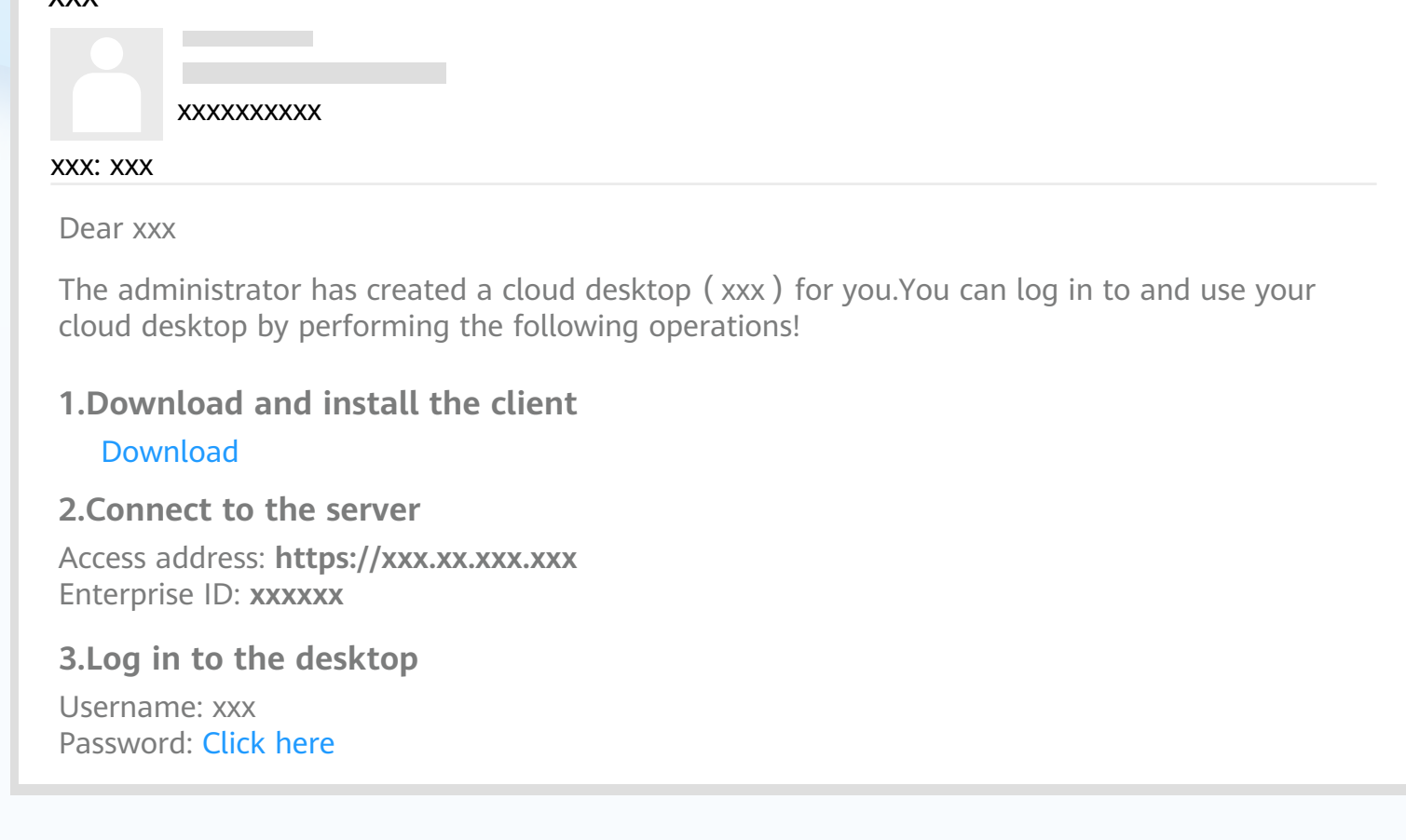
Logging In to a Desktop Using an SC

Note:

- ★ You can log in to a PC running Windows 10 or macOS 10.14-12.4.
- ★ Installation is allowed when the security software displays a dialog box.

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

Note: The notification email for connecting to the AD is slightly different from that when the AD is not connected. Refer to the email you receive.

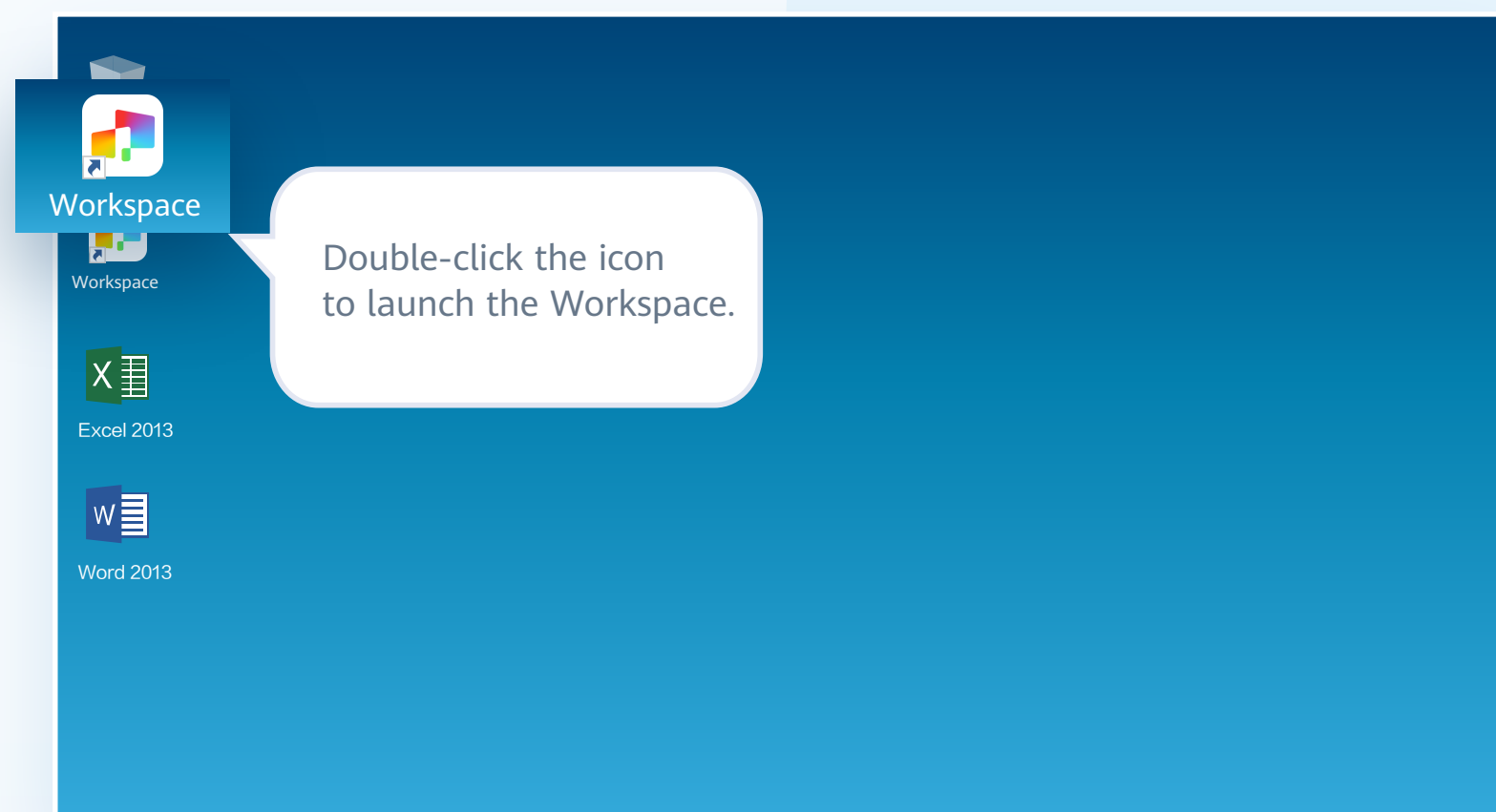


2 Download and install the client software.

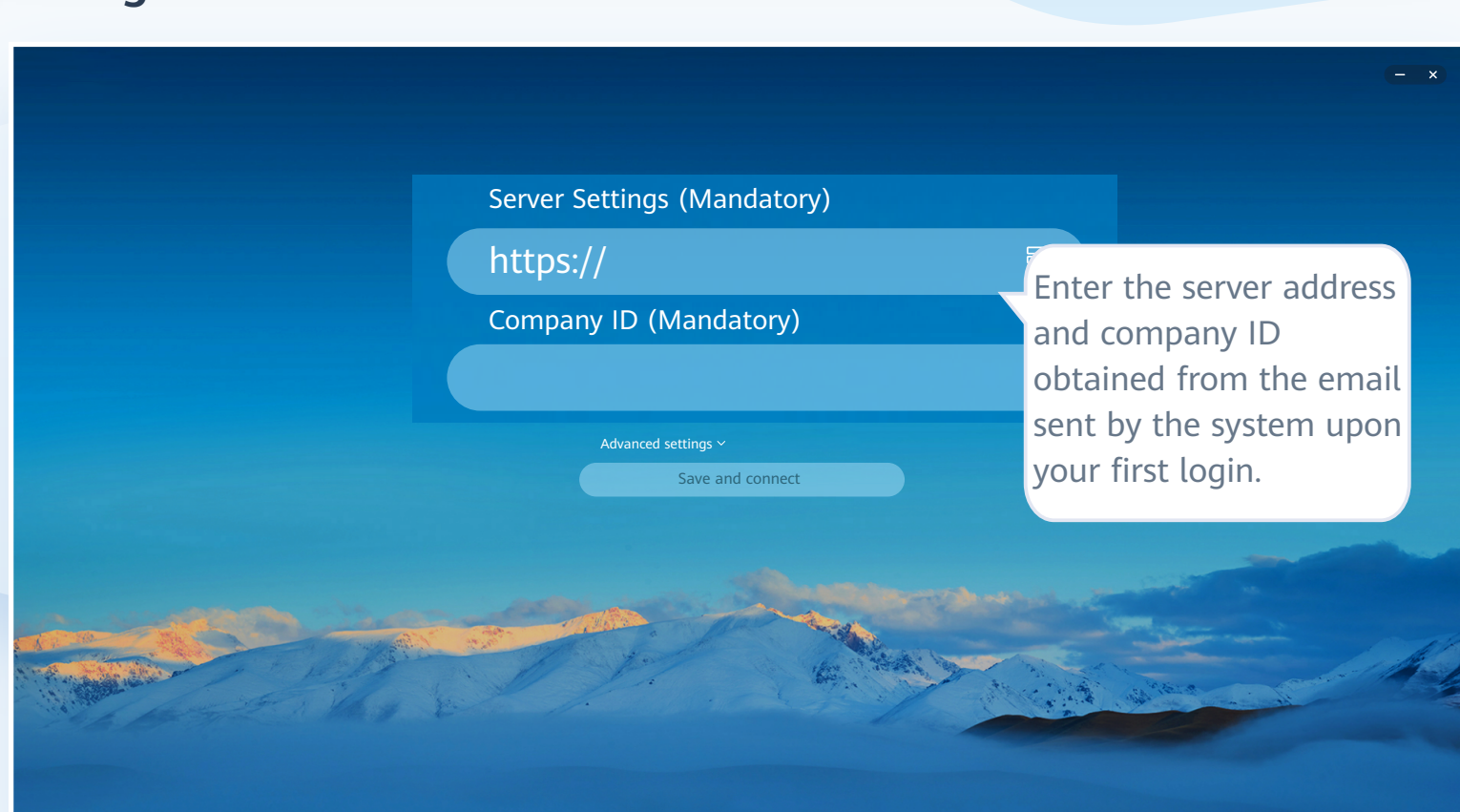
Click [Download](#) in the notification email to obtain the client installation package.

3 Double-click the icon to start the client.

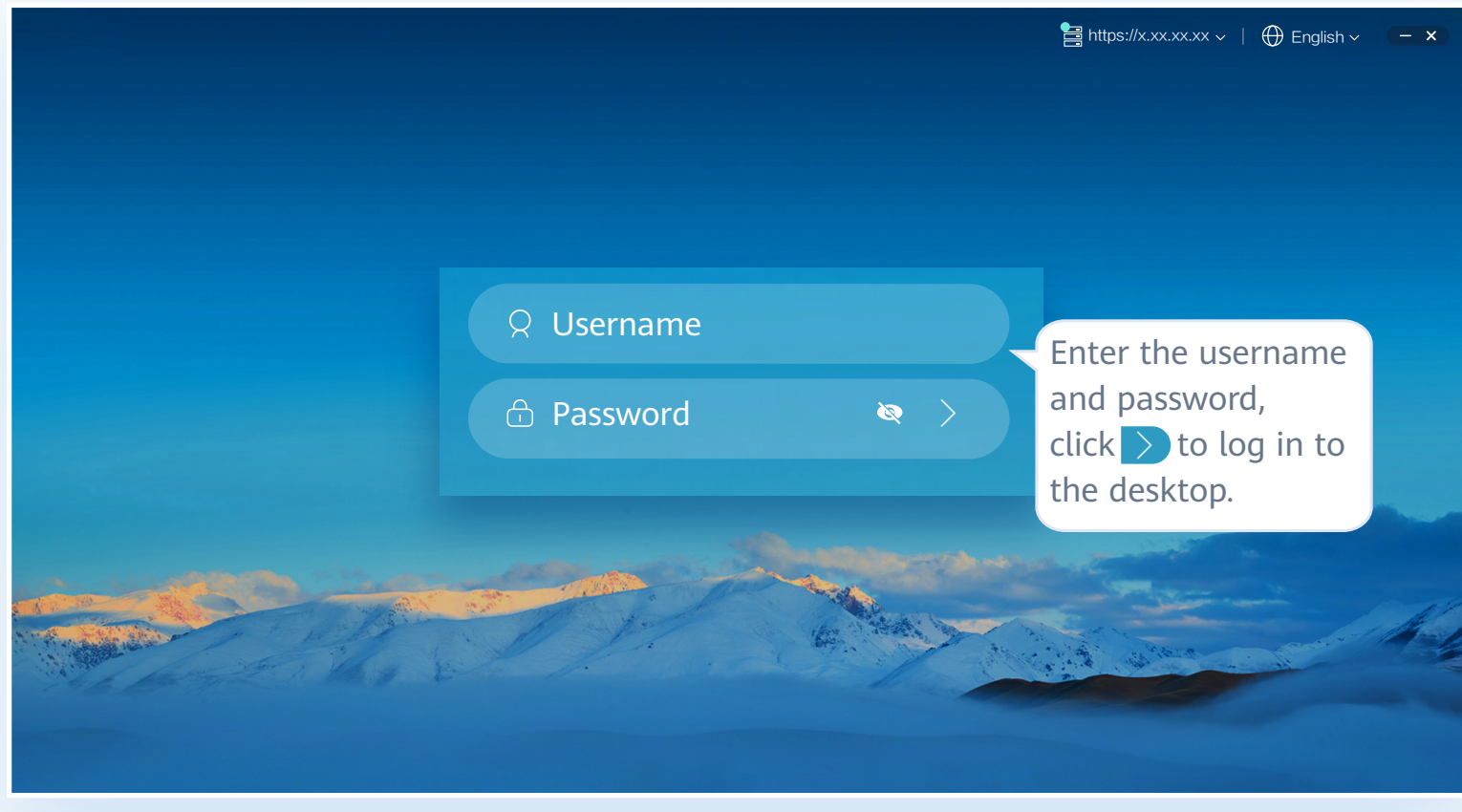
Note: If a macOS PC is used, you need to set system preferences before starting the client for the first time. Otherwise, security cannot enter characters on the cloud desktop. Choose **System Preferences > Security & Privacy > Input Monitoring**, select **HDPViewer**, and switch the input mode to **English**.



4 Configure server information.



5 Log in to the desktop.



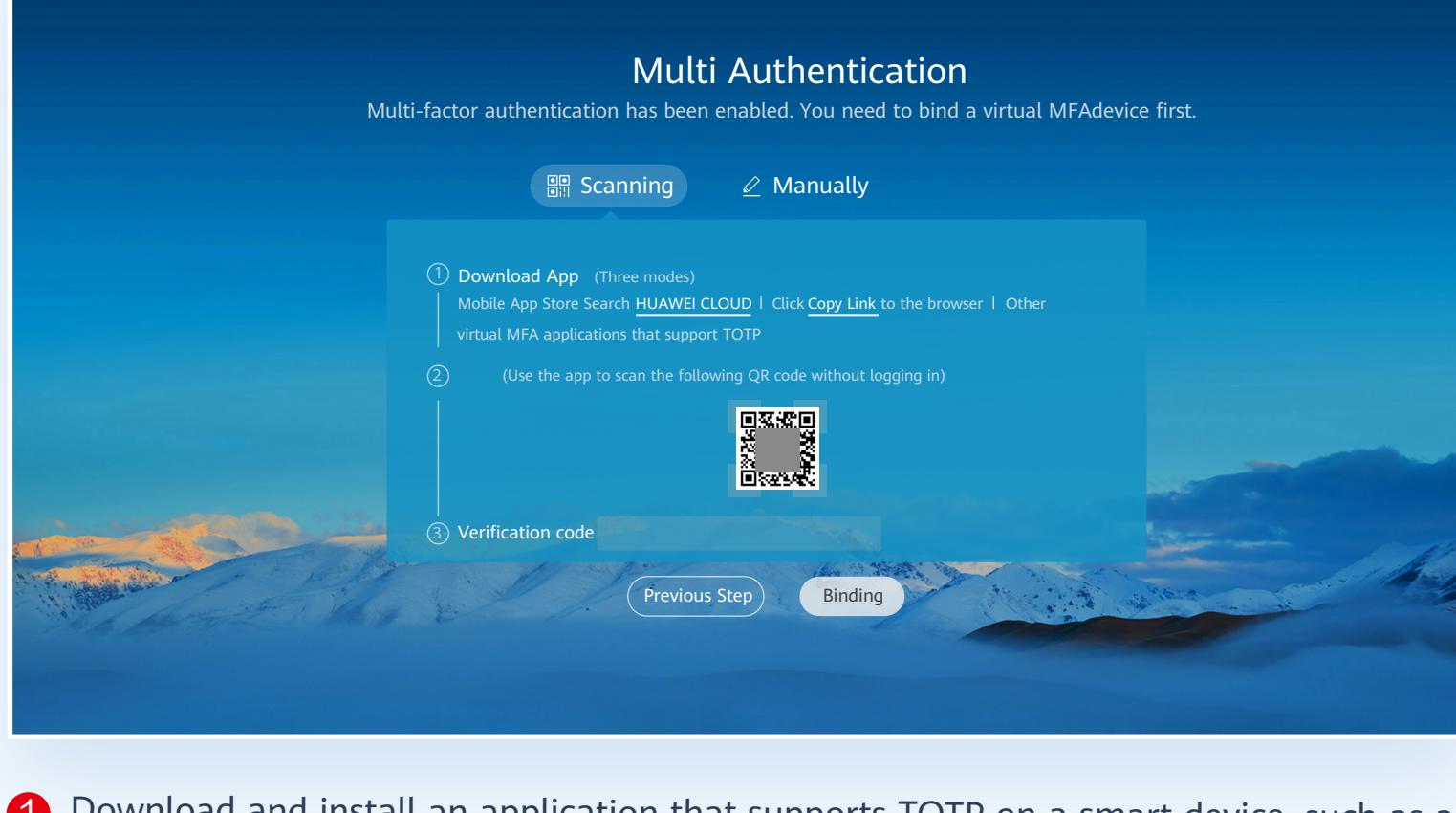
Note: If the user has multiple desktops, enter the user name and password, and click **>**. The desktop list page is displayed. You need to click the target desktop to access the corresponding desktop.

After multi-factor authentication is enabled, you need to pass the dynamic verification code again to log in to the cloud desktop.

6 (Optional) Perform multi-factor authentication.

Note: 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.



- 1 Download and install an application that supports TOTP on a smart device, such as a mobile phone, and access the MFA tool page.
- 2 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.

- 3 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.

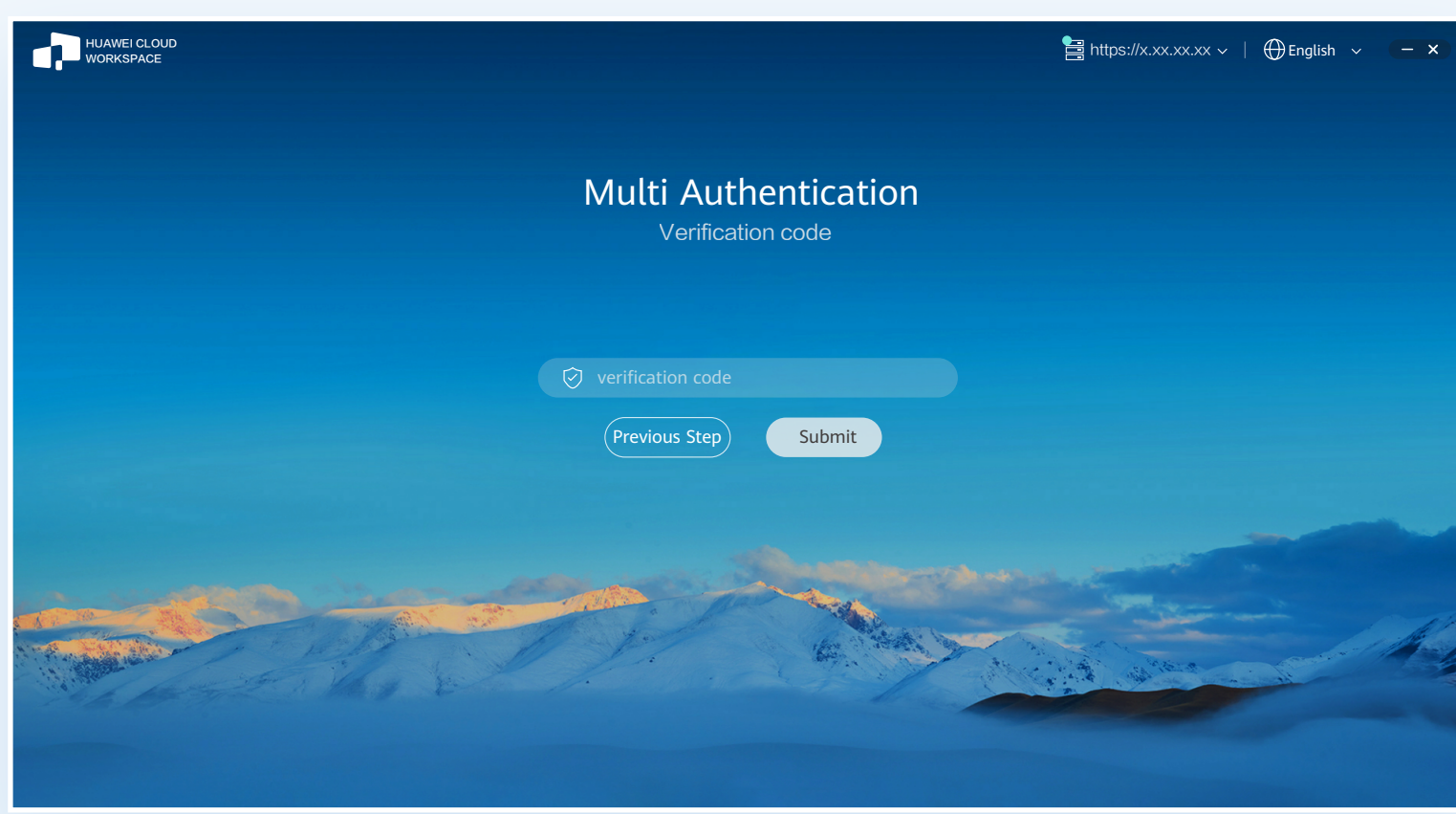


Note: The preceding verification code page is only an example. The actual page varies depending on the application in use.

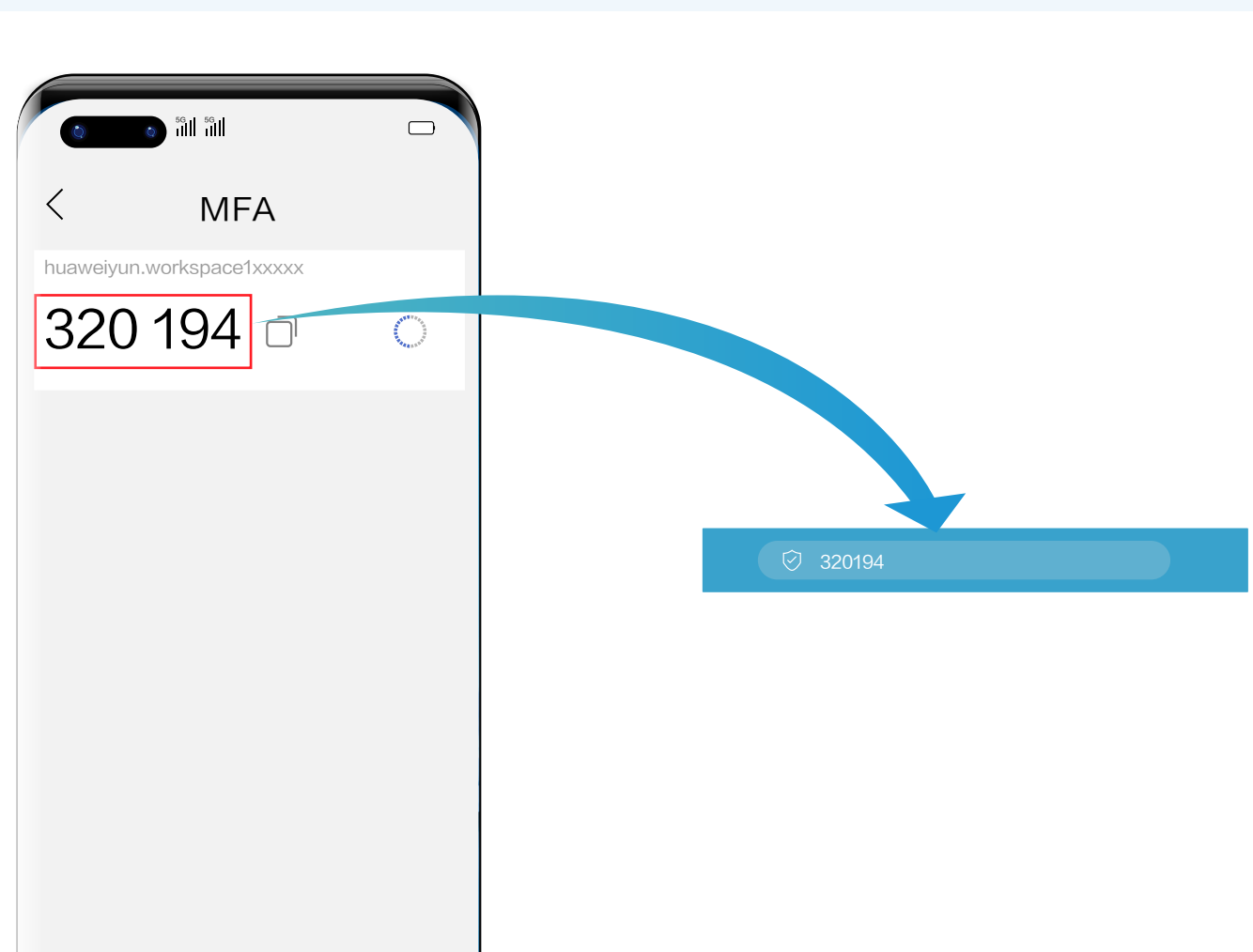
- 4 On the multi-factor authorization page of the Workspace client, click **Binding**.

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.



- 1 Open the installed application that supports TOTP on the smart device, such as a mobile phone, and access the MFA tool page.
- 2 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.

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

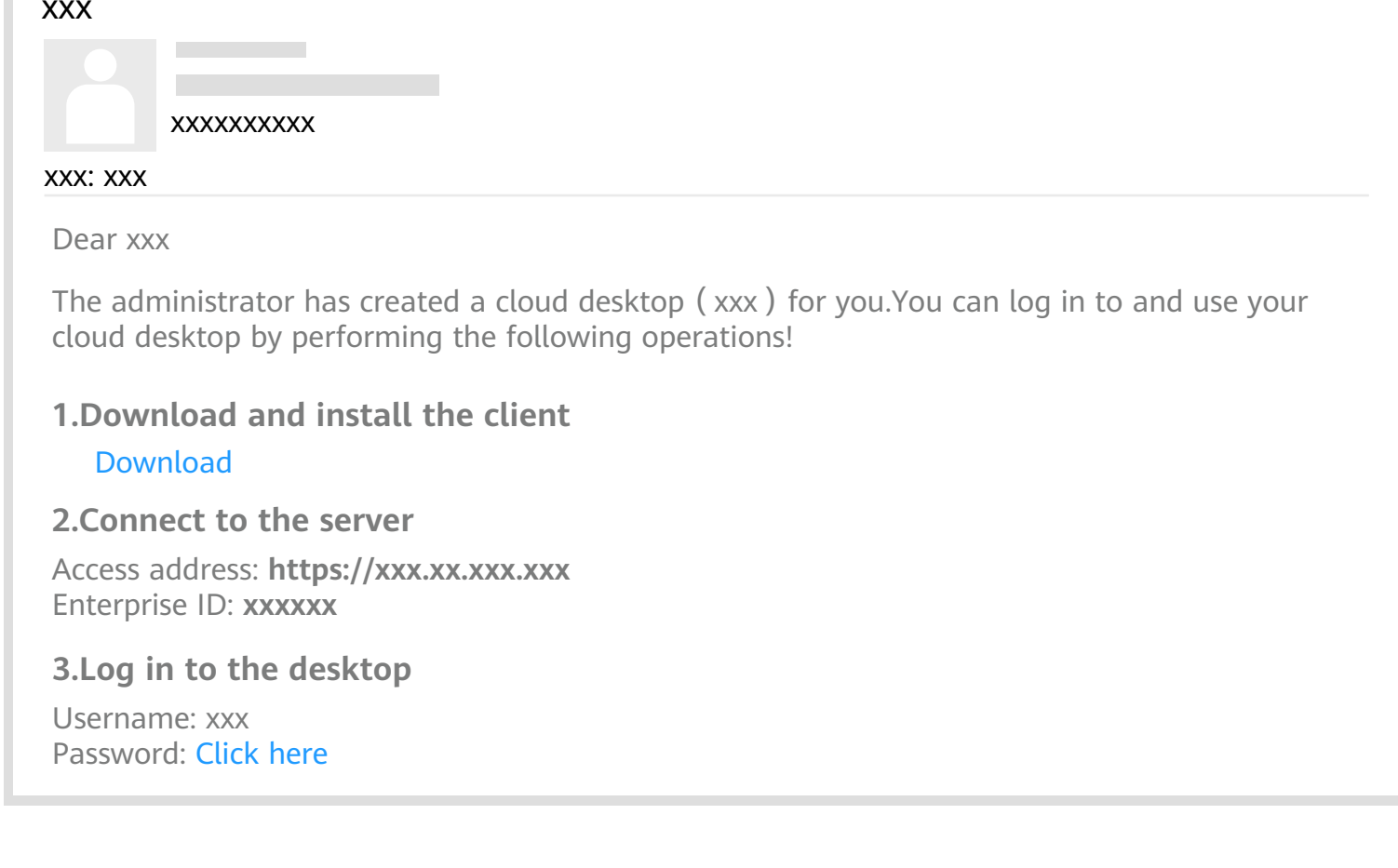
Note: If the account has multiple desktops, the desktop list page will be displayed after you click **Submit**. You need to click the target desktop to access it.

Logging In to a Desktop Using a Mobile Terminal

Note: Mobile terminals running Android 6.0 or later are supported. You can use the stylus to perform operations. The operations on different mobile terminals are similar. The following uses the operations on a mobile phone as an example.

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

Note: The notification email for connecting to the AD is slightly different from that when the AD is not connected. Refer to the email you receive.

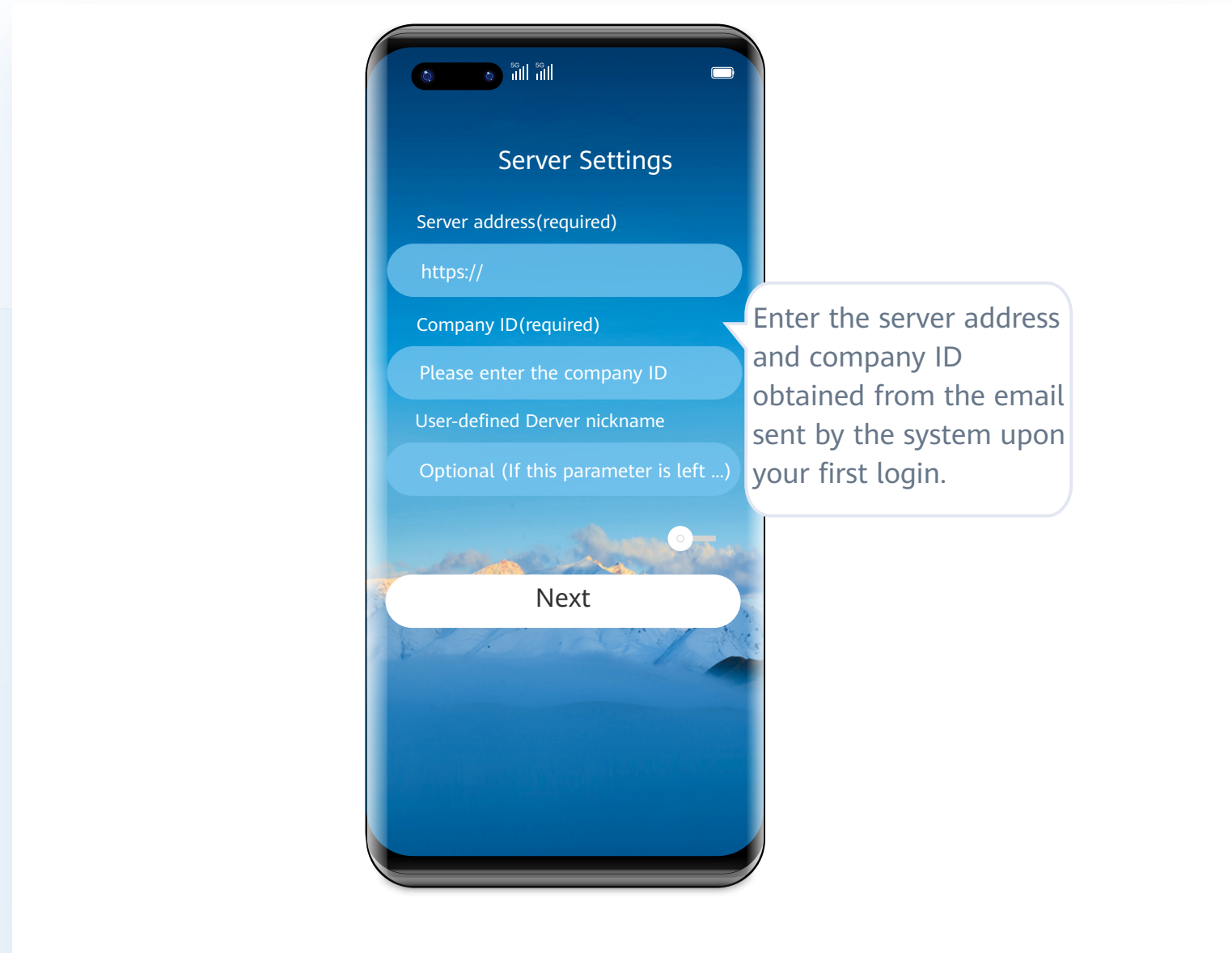


2 Download and install the client software.

Click [Download](#) in the notification email to obtain the client installation package.

Note: Please use a browser to scan the QR code.

3 Start the client, and configure server information.



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.



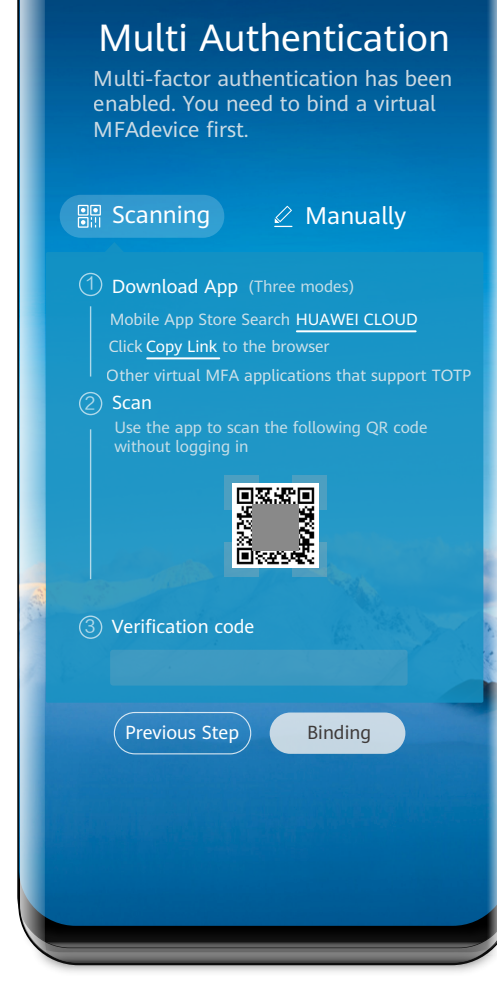
Note: If the user has multiple desktops, enter the user name and password, and click **Log In**. The desktop list page is displayed. You need to click the target desktop to access the corresponding desktop.

After multi-factor authentication is enabled, you need to pass the dynamic verification code again to log in to the cloud desktop.

5 (Optional) Perform multi-factor authentication.

Note: 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.



- Download and install an application that supports TOTP on a smart device, such as a mobile phone, and access the MFA tool page.

- 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.

- 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.

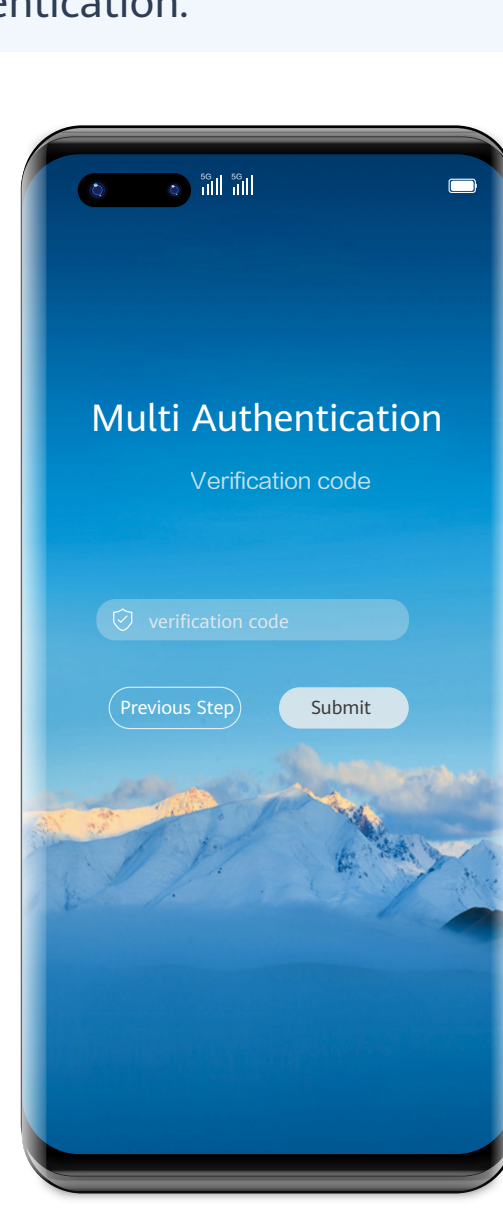


Note: The preceding verification code page is only an example. The actual page varies depending on the application in use.

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

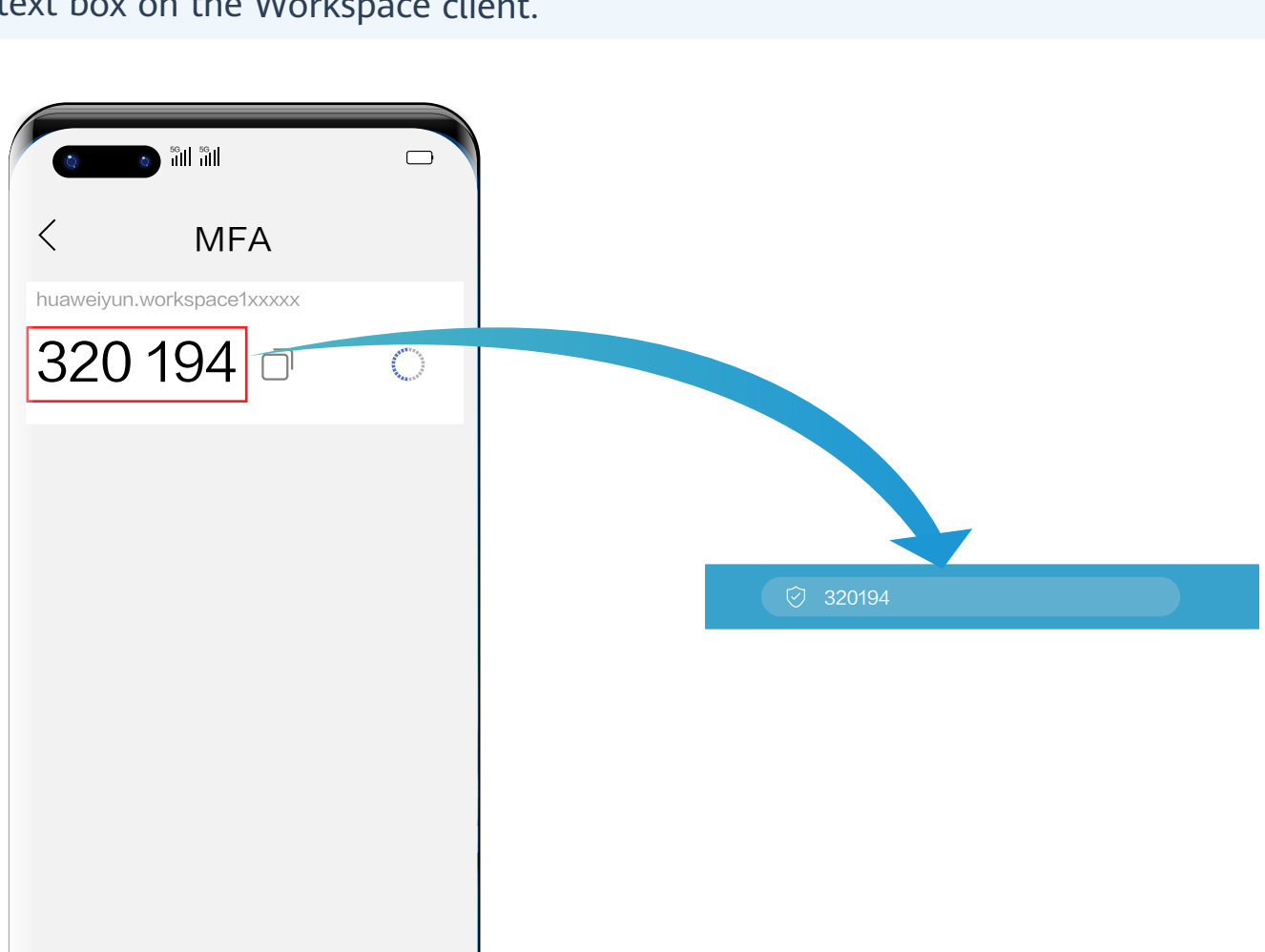
Note: If the account has multiple desktops, the desktop list page will be displayed after you click **Binding**. You need to click the target desktop to access it.

- 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.



- Open the installed application that supports TOTP on the smart device, such as a mobile phone, and access the MFA tool page.

- Enter the 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.

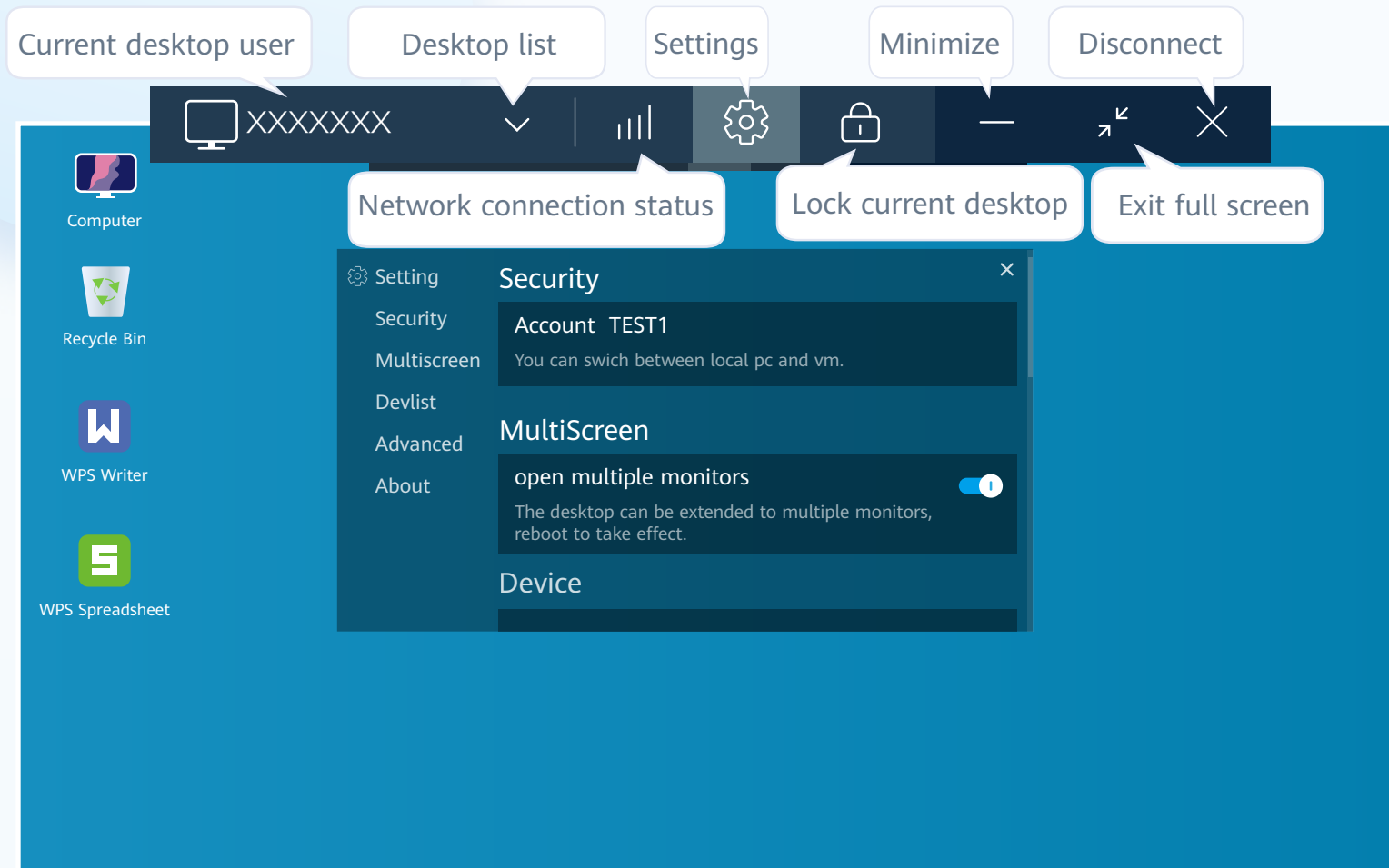
- On the multi-factor authorization page of the Workspace client, click **Submit**.

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.

Desktop Assistant

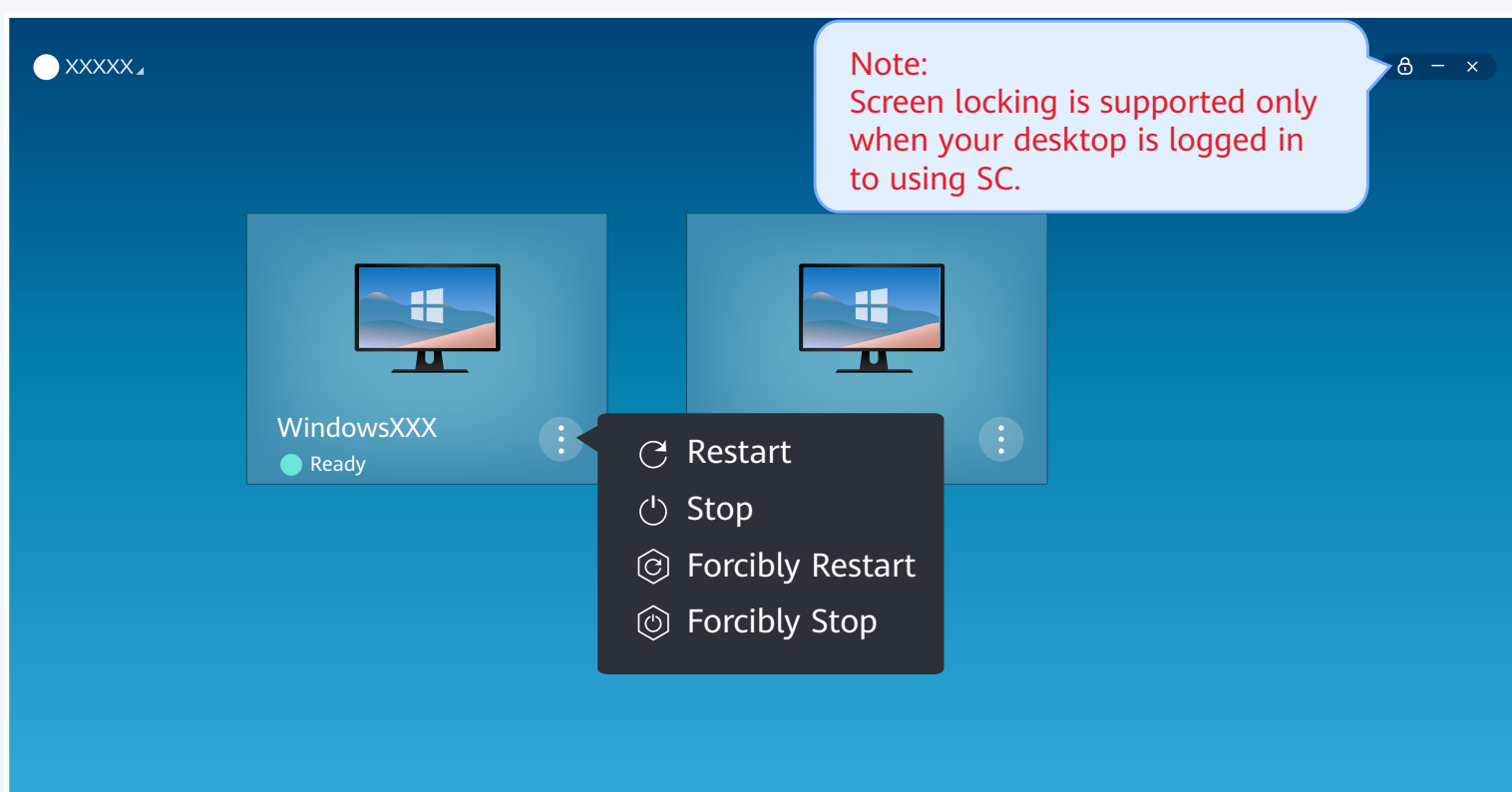
Desktop Floating Bar

The desktop floating bar offers multiple tools for you to set or view parameters as needed.



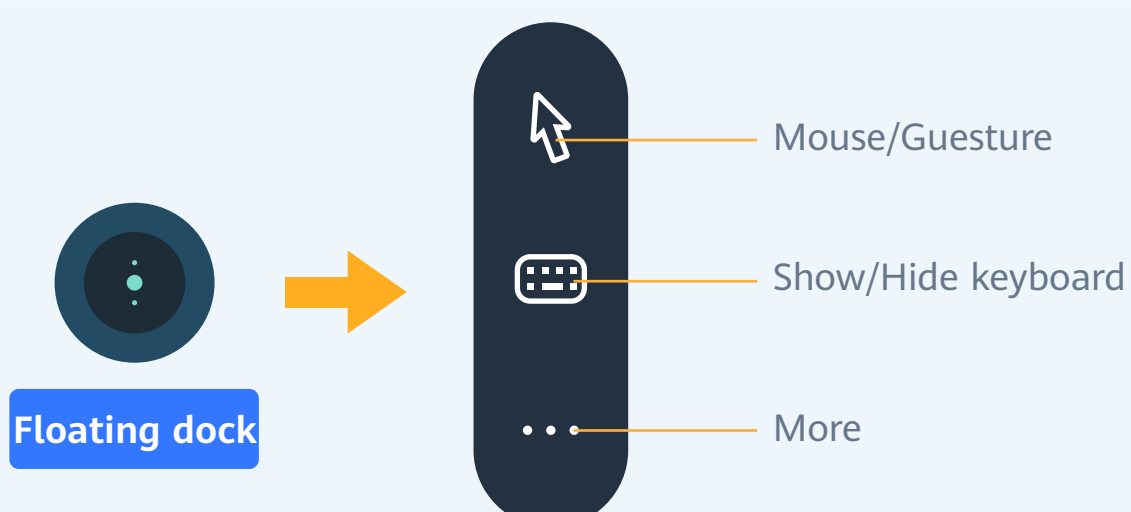
Desktop Tools

In the window where you can choose a desktop that you want to use, click to restart, stop, forcibly restart, forcibly stop, or click to lock the screen.



Mobile Terminal Floating Dock

The floating dock is a hidden button on the toolbar of your mobile FusionAccess. You can click it to perform settings.

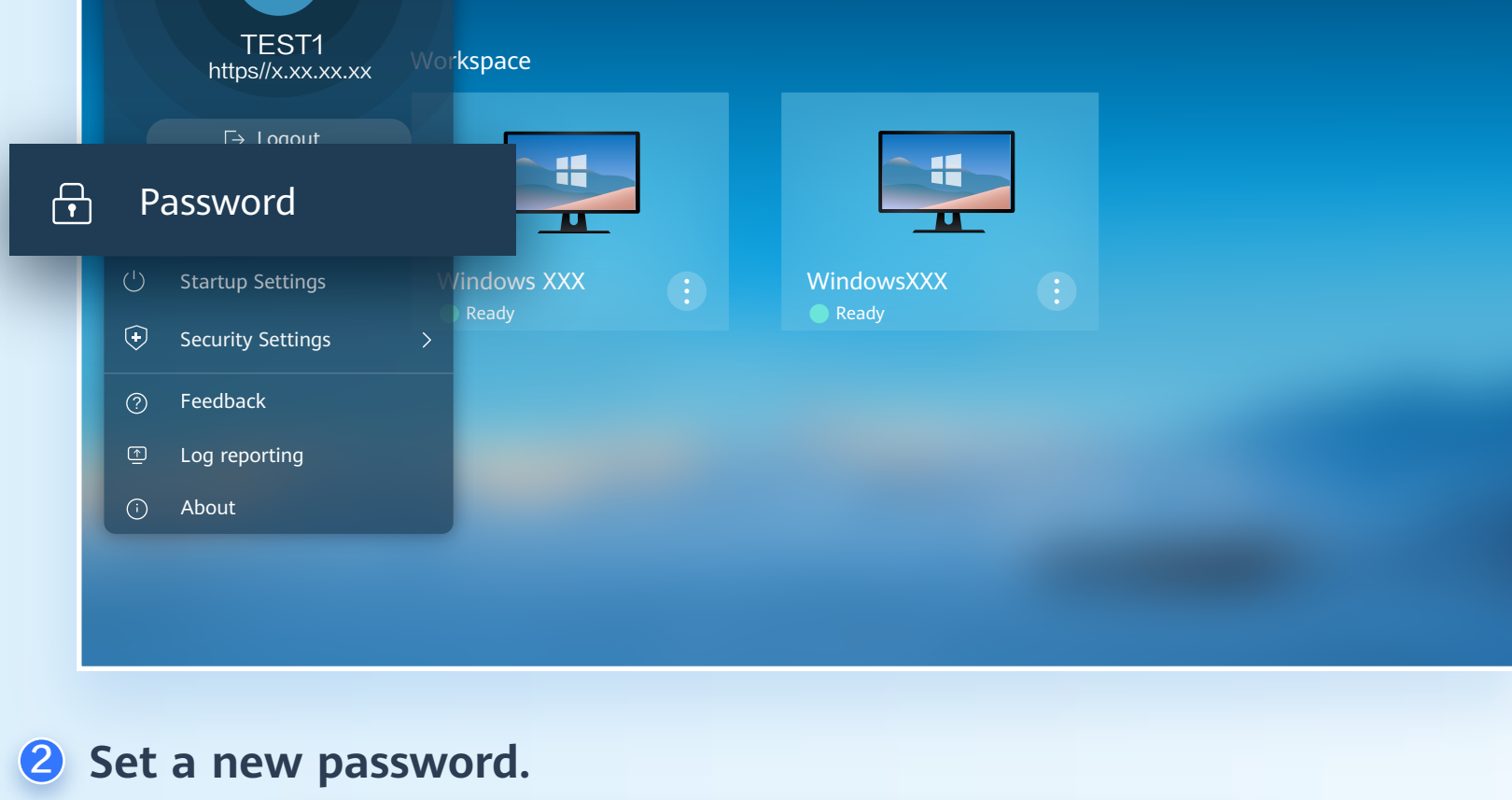


Changing the Login Password

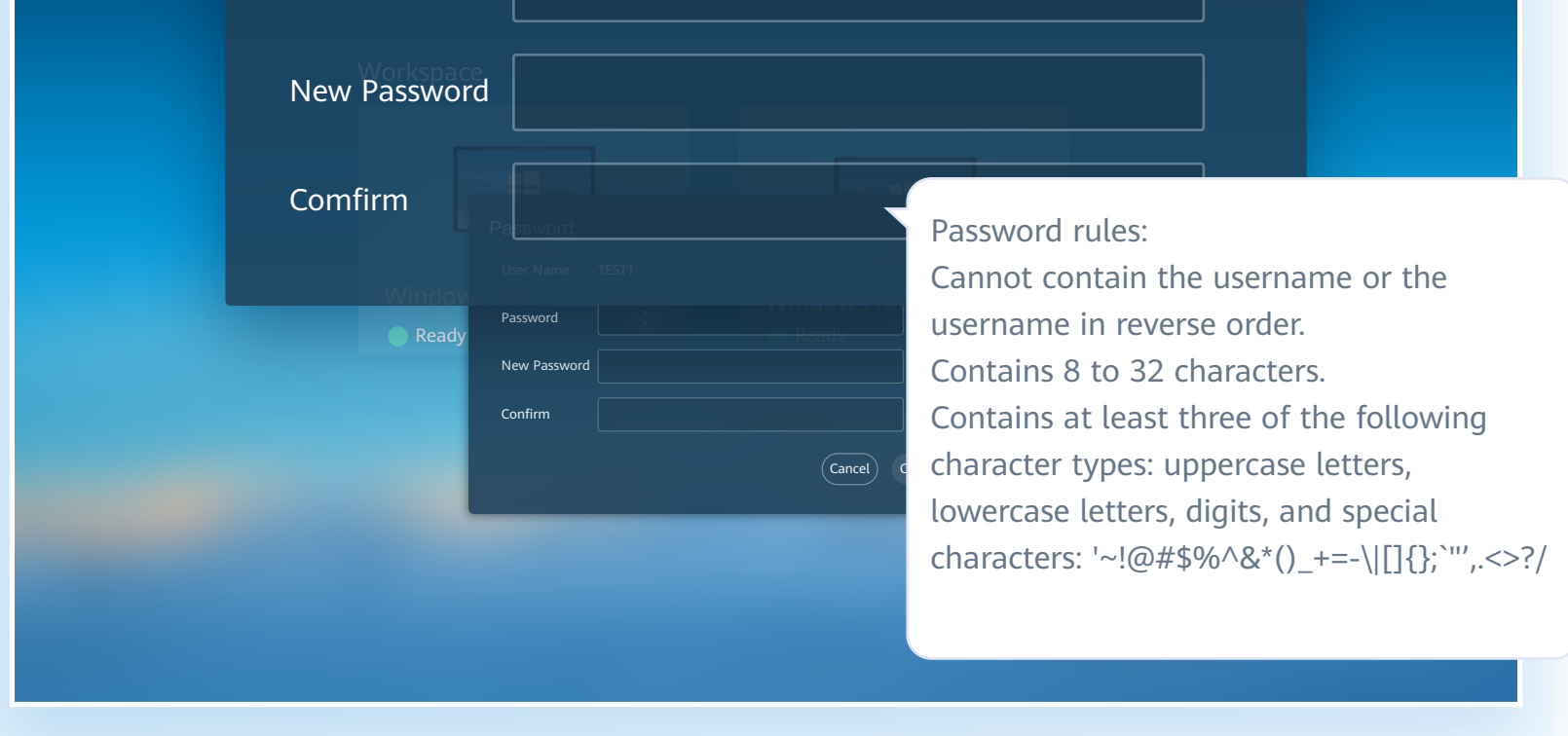
Changing the Login Password on the Client

Changing the Login Password on the Client After Login

- 1 On the desktop page, click the profile in the upper left corner and choose Password.

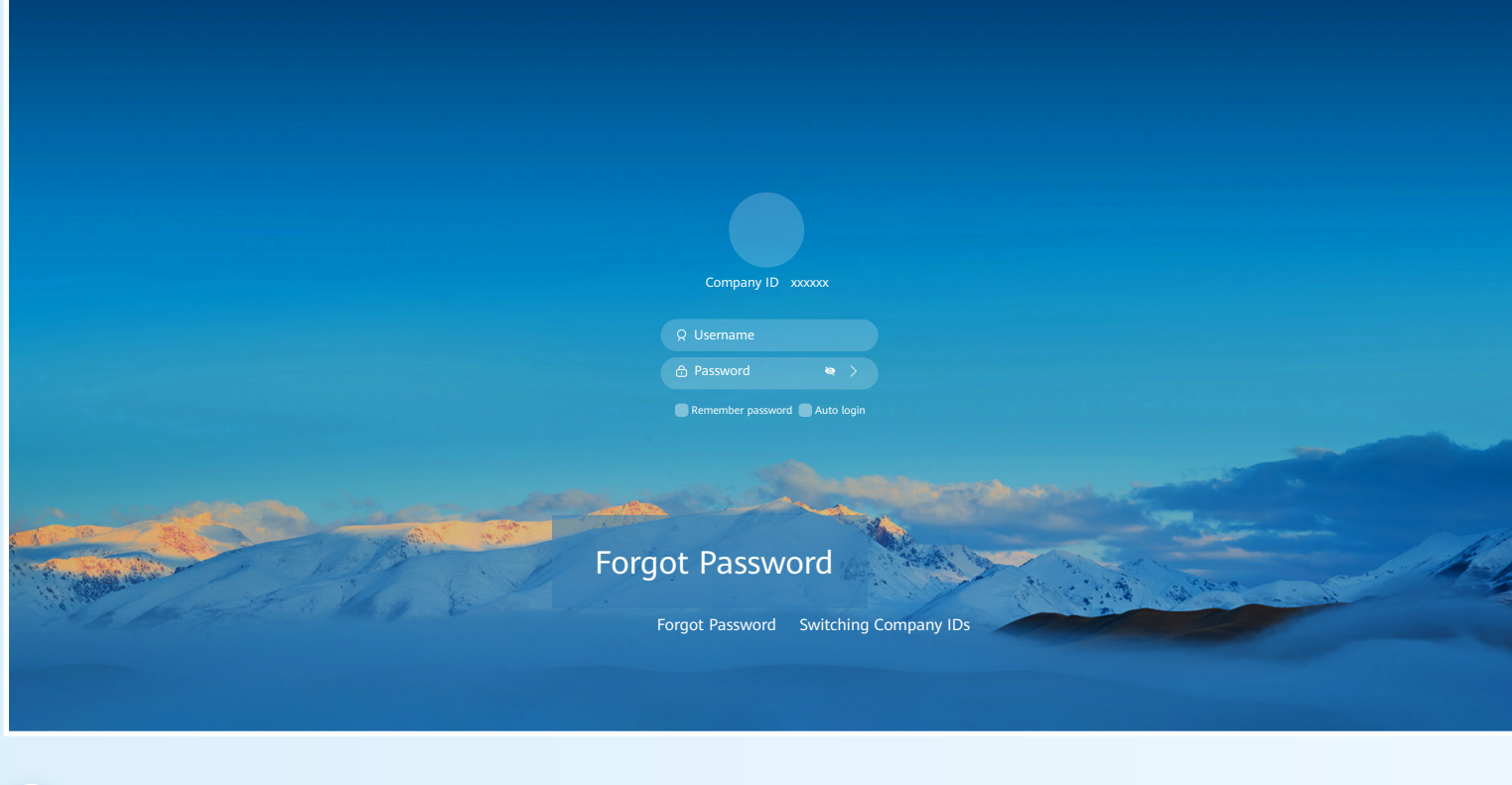


- 2 Set a new password.

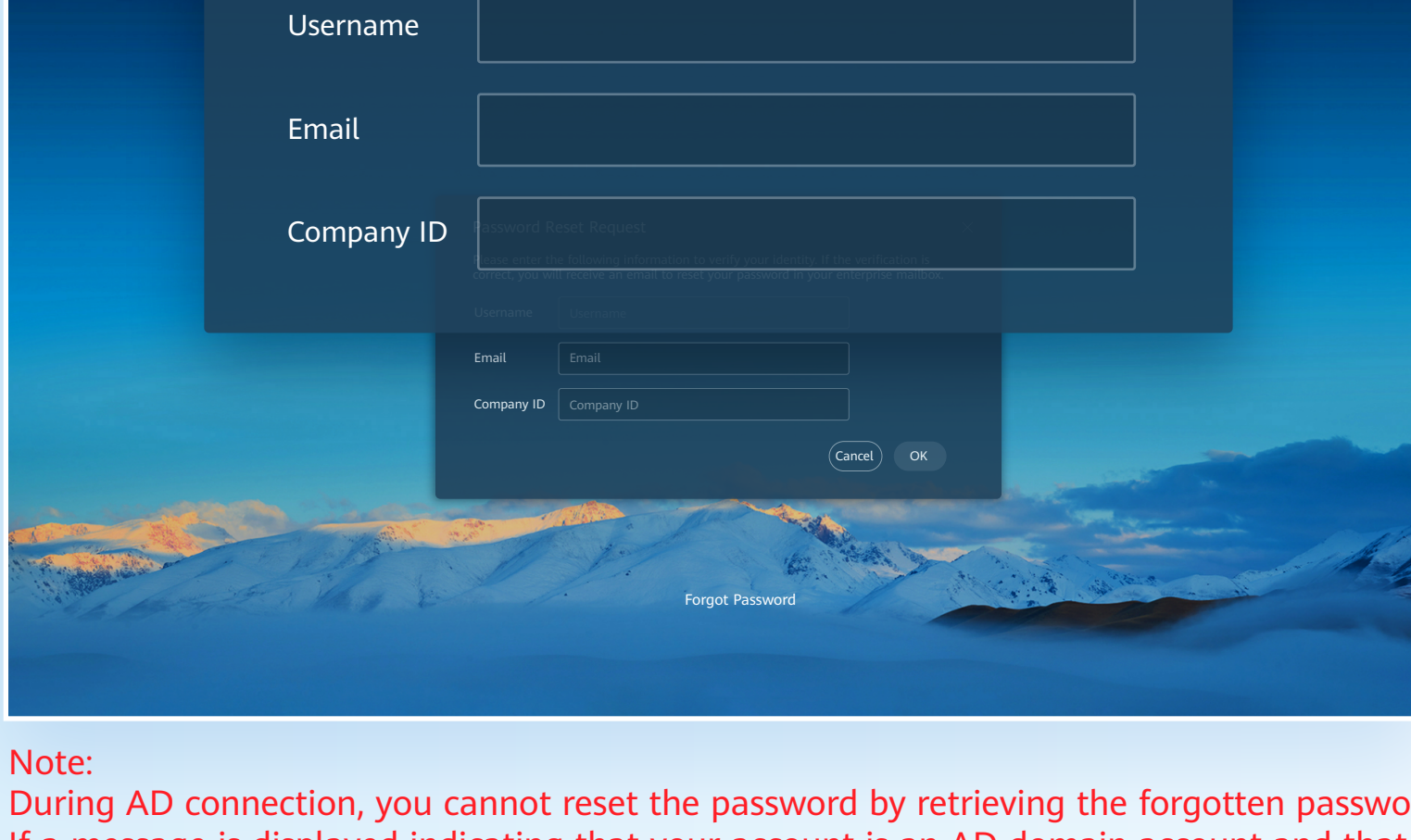


Changing the Login Password on the Client Before Login

- 1 Click Forgot Password on the login page.

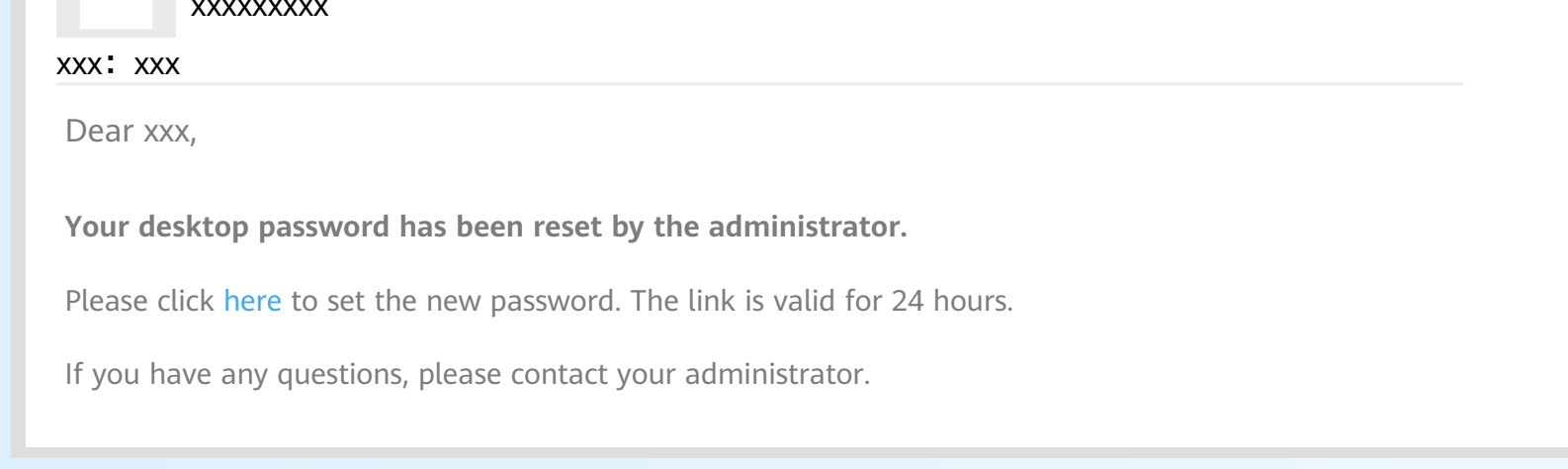


- 2 Enter information of the user whose password needs resetting and click OK.

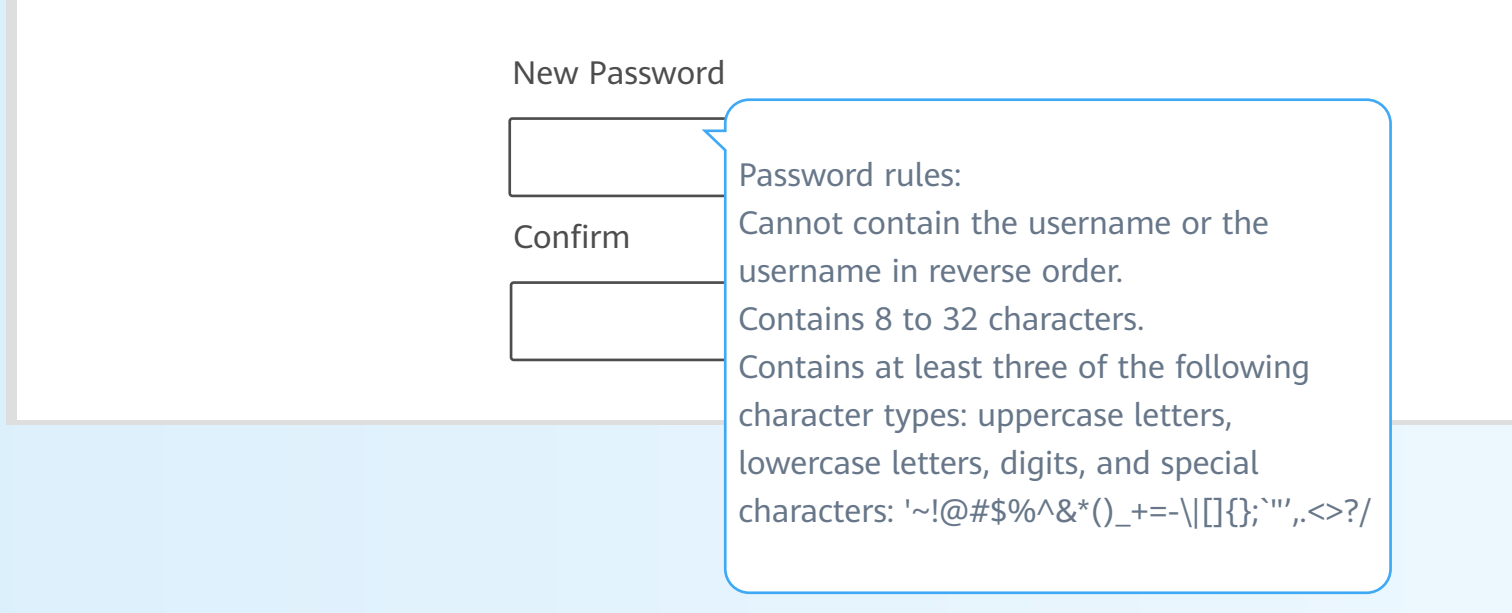


Note: During AD connection, you cannot reset the password by retrieving the forgotten password. If a message is displayed indicating that your account is an AD domain account and that you need to contact the administrator to reset the password, contact the administrator as prompted.

- 3 In the password reset email, click the link for resetting the password.



- 4 On the page for resetting passwords, set a new password and click OK.





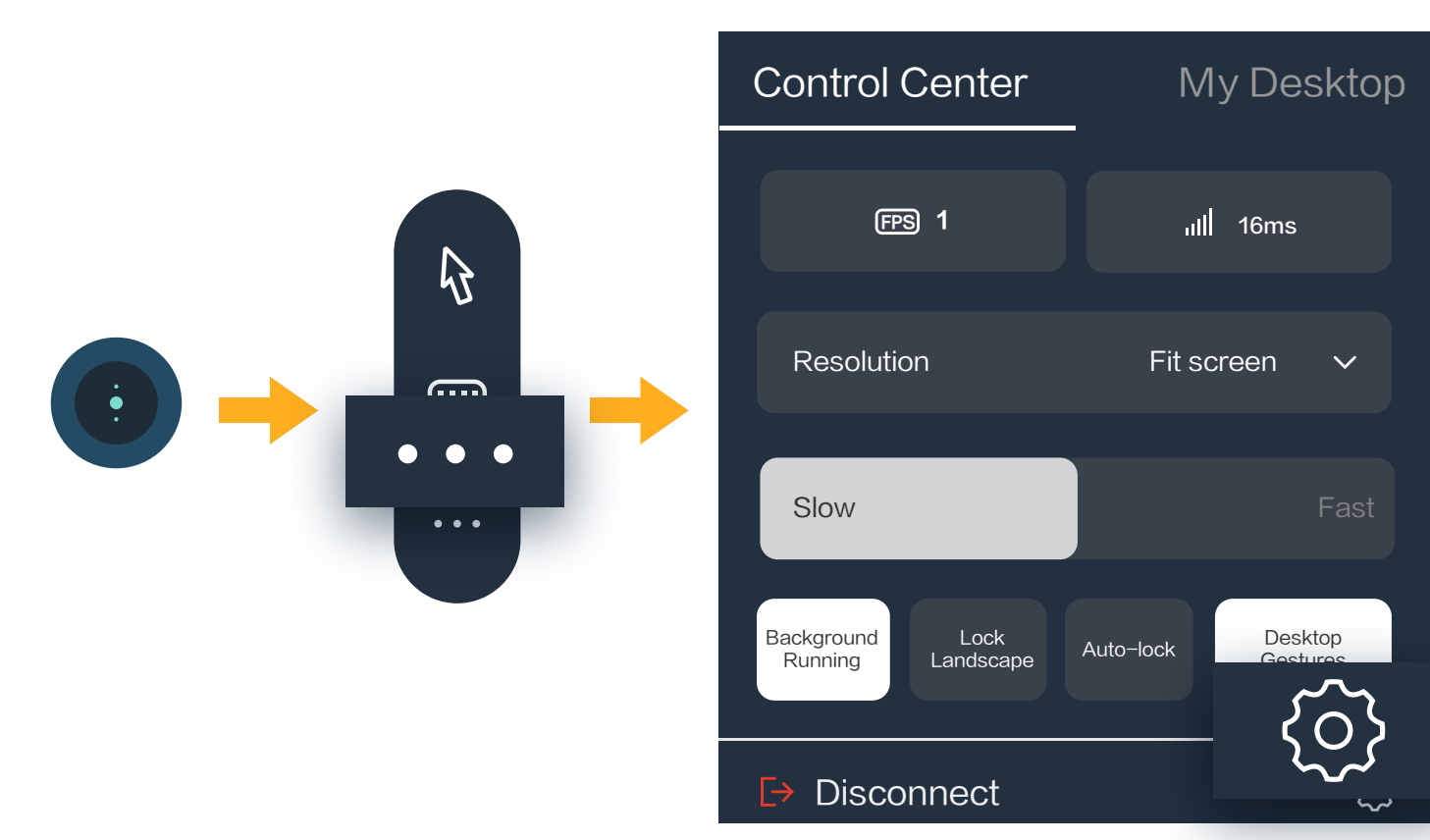
Changing the Login Password on the Mobile Client

Changing the Login Password on the Client After Login

Method 1: On the Home page, click the user avatar and choose Reset Password to change the password.

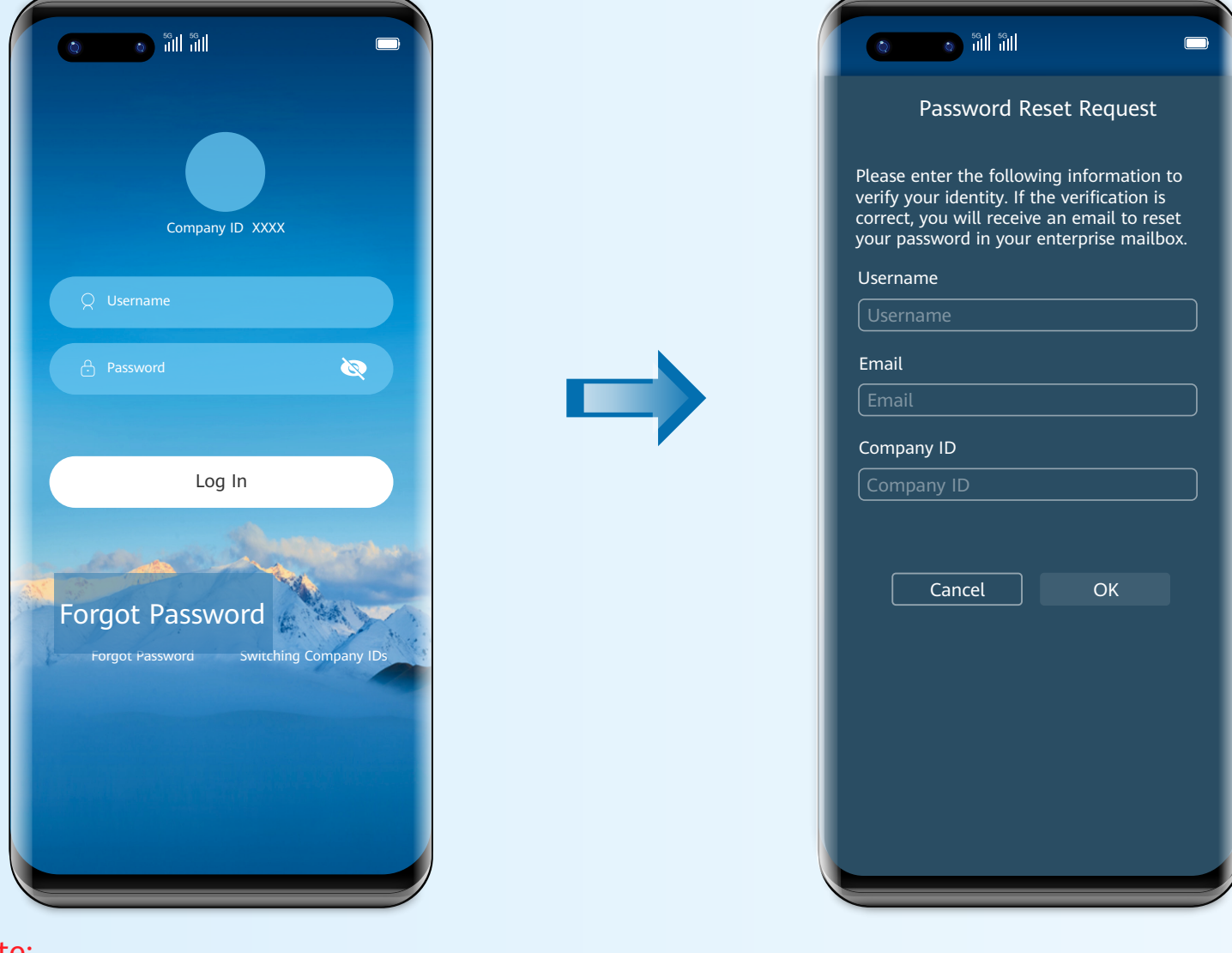


Method 1: On the desktop window, click the floating dock, choose , and click  to change the password.



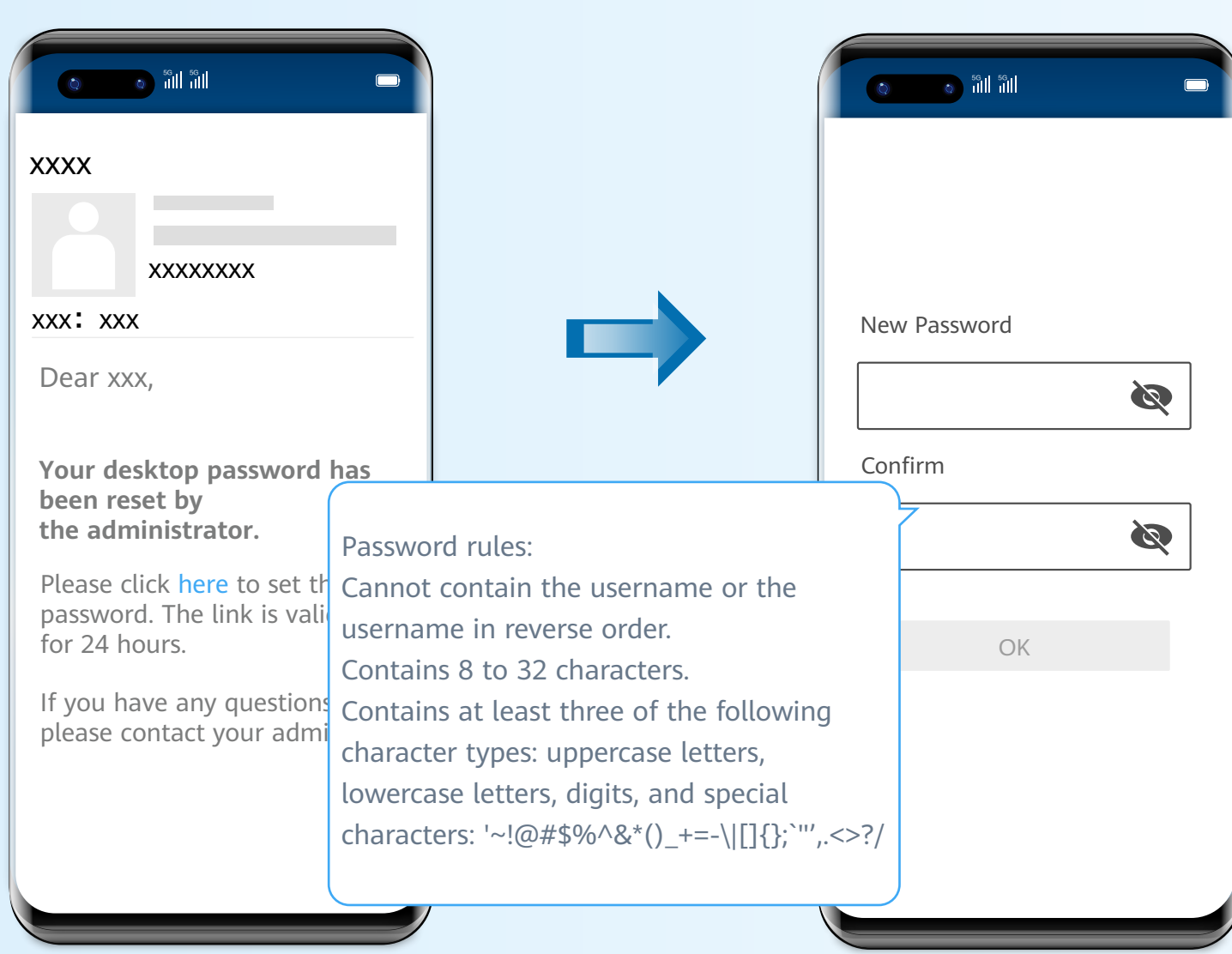
Changing the Login Password on the Client Before Login

- 1 Click Forgot Password on the login page.



Note: During AD connection, you cannot reset the password by retrieving the forgotten password. If a message is displayed indicating that your account is an AD domain account and that you need to contact the administrator to reset the password, contact the administrator as prompted.

- 2 In the password reset email, click the link for resetting the password.



Forbidden Operations

1 Risky Operations (Processes and Services)

- ◆ Change the default service and startup options in the system configuration.
- ◆ End the LOCAL SERVICE, NETWORK SERVICE, and SYSTEM processes in Task Manager.
- ◆ Disable HDP services.
- ◆ Uninstall the following programs.
 - ◆ Access Agent
 - ◆ Microsoft .NET Framework x Client Profile
 - ◆ Microsoft .NET Framework x Extended
 - ◆ Microsoft Visual C++ xxx Redistributable - xxx

2 Risky Operations (Network)

- ◆ Disable NICs, and disable or modify network configurations.
- ◆ Run the script or command for modifying a route, such as route DELETE *.
- ◆ Delete ports 28511, 28512, 28521, and 28522 from Windows firewall exception options.
- ◆ Enable software or tools, such as the IPsec, that can restrict network traffic.

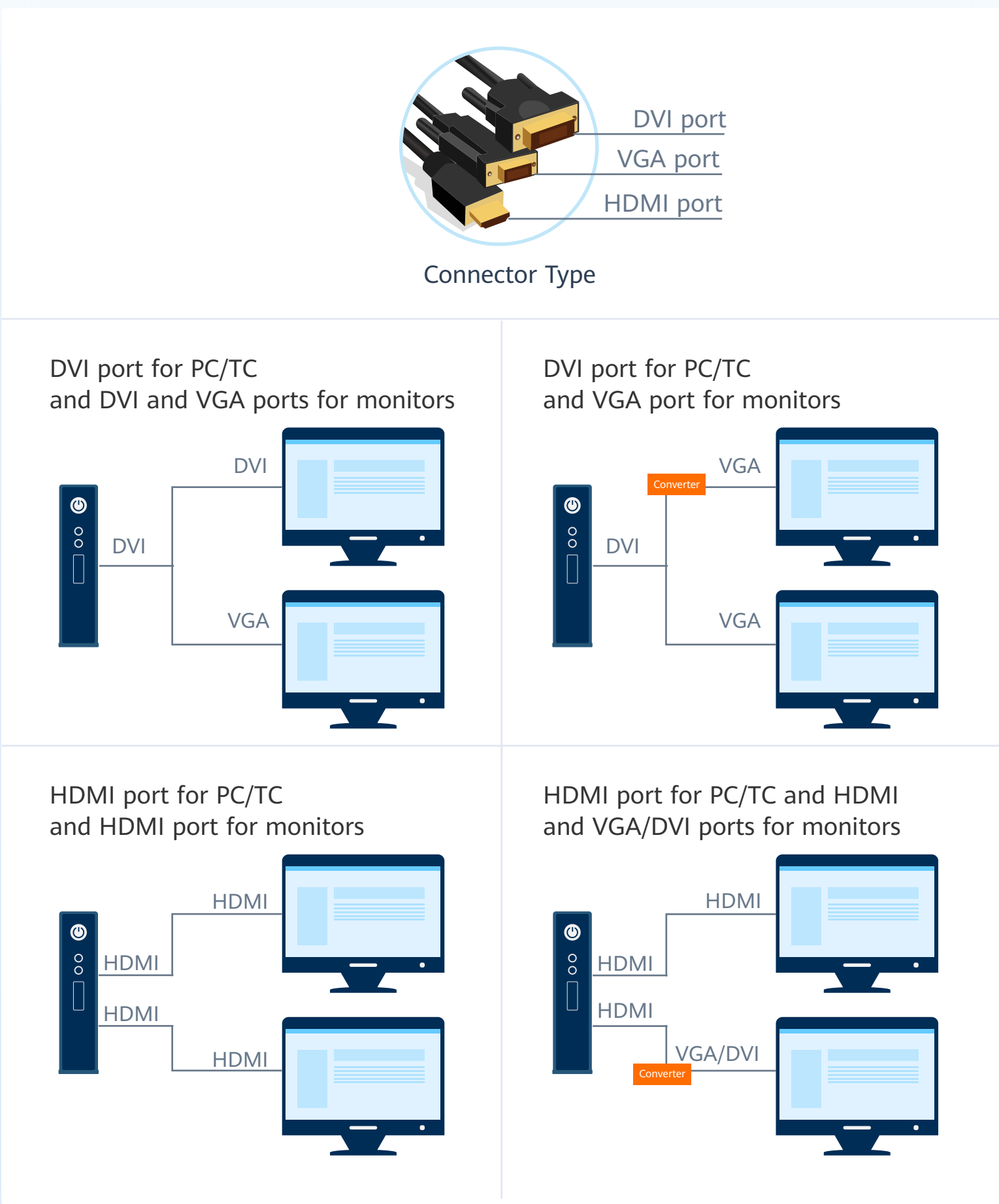
3 Risky Operations (Others)

- ◆ Delete files or folders in **C:\Program Files\Huawei**.
- ◆ Do not hibernate desktops, which disable hibernation by default.
- ◆ Modify the configuration file of the HDP client (AccessAgent).
- ◆ Run Rabbit Magic or Wopti Utilities to clean or optimize the registry.
- ◆ Install a customized screensaver with complex transformation functions, which consumes system resources and causes a delay in desktop access.

Configuring Dual-Screen Display

Note:
Windows PCs and HT3300 can be configured with dual screens.

1 Dual-screen cable: Connect the PC/TC to the monitor based on the connector type.



Note:
Ensure that the desktop configuration item MultiScreen is enabled. You can expand the client floating window and click to check the configuration.

2 PC/TC Settings

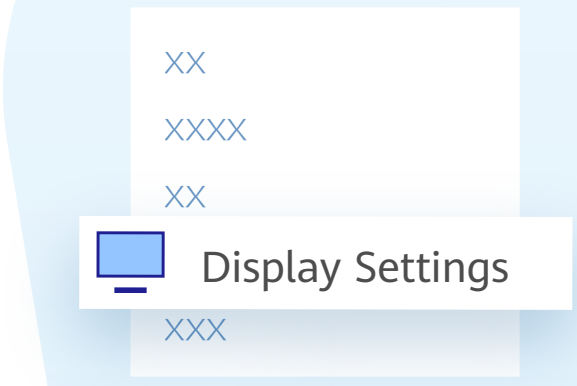
Windows PC

01

Start the PC.

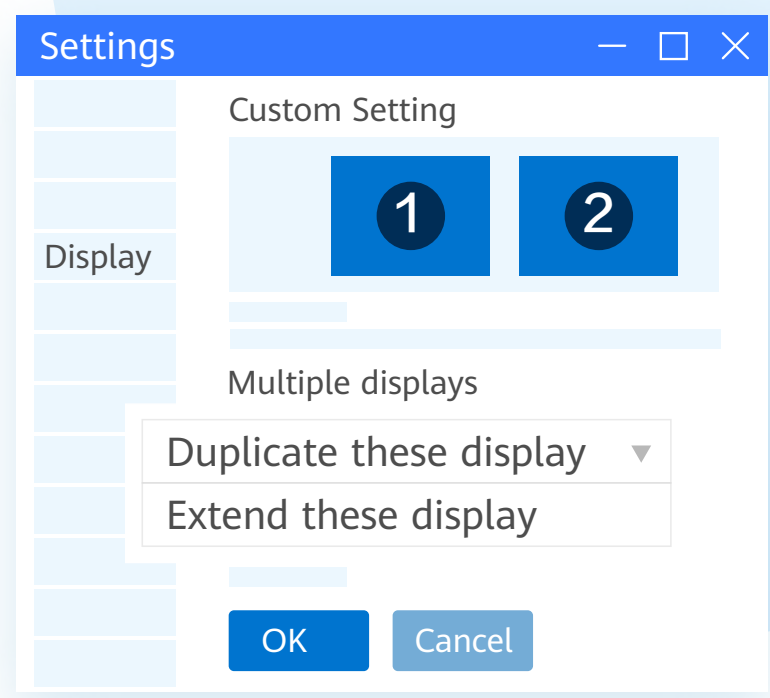
02

Right-click on the desktop and select **Display Settings**.



03

Set the display mode of multiple displays based on the site requirements. Click **OK** to save the settings.



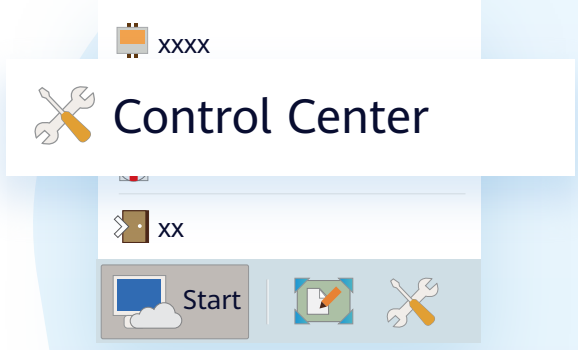
Linux TC

01

Start the TC.

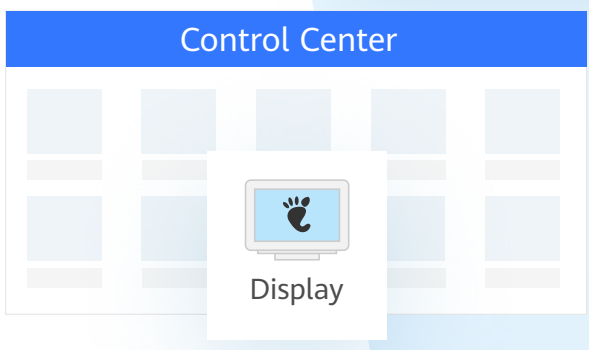
02

Click **Start**. Select **Control Center**.



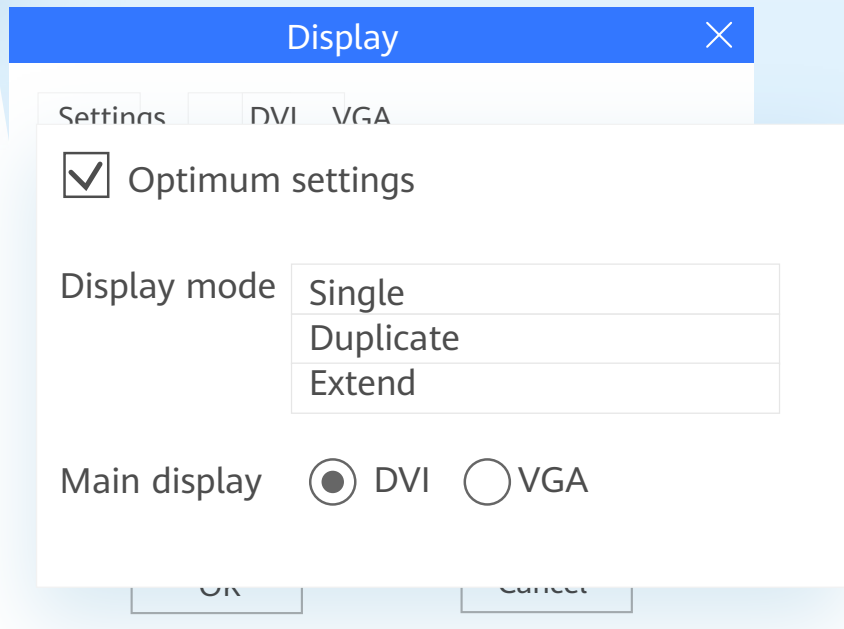
03

Double-click **Display**.



04

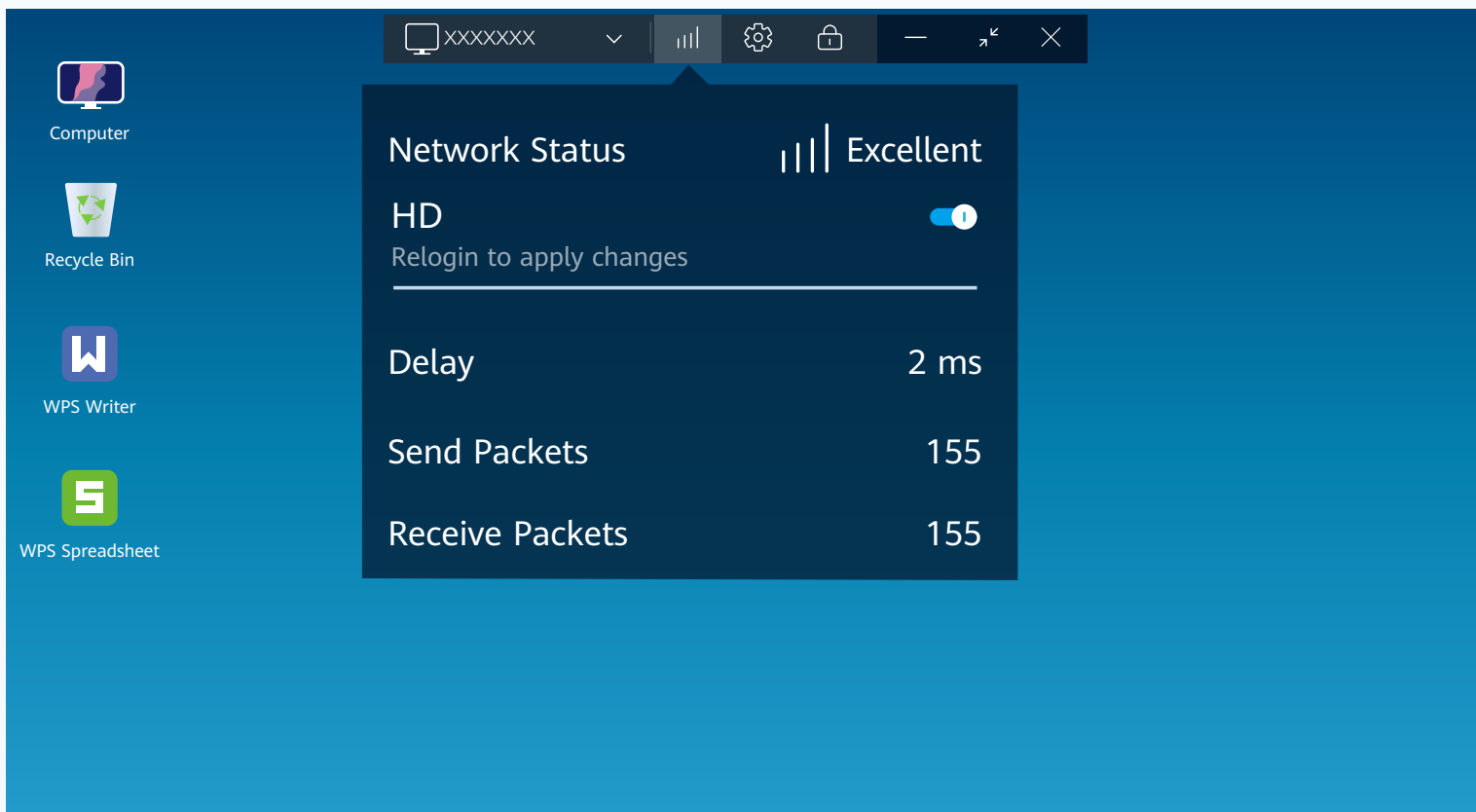
Select **Optimum settings**. Select a display mode and the main display as required, and click **OK**. The setting is complete.



Common function configuration

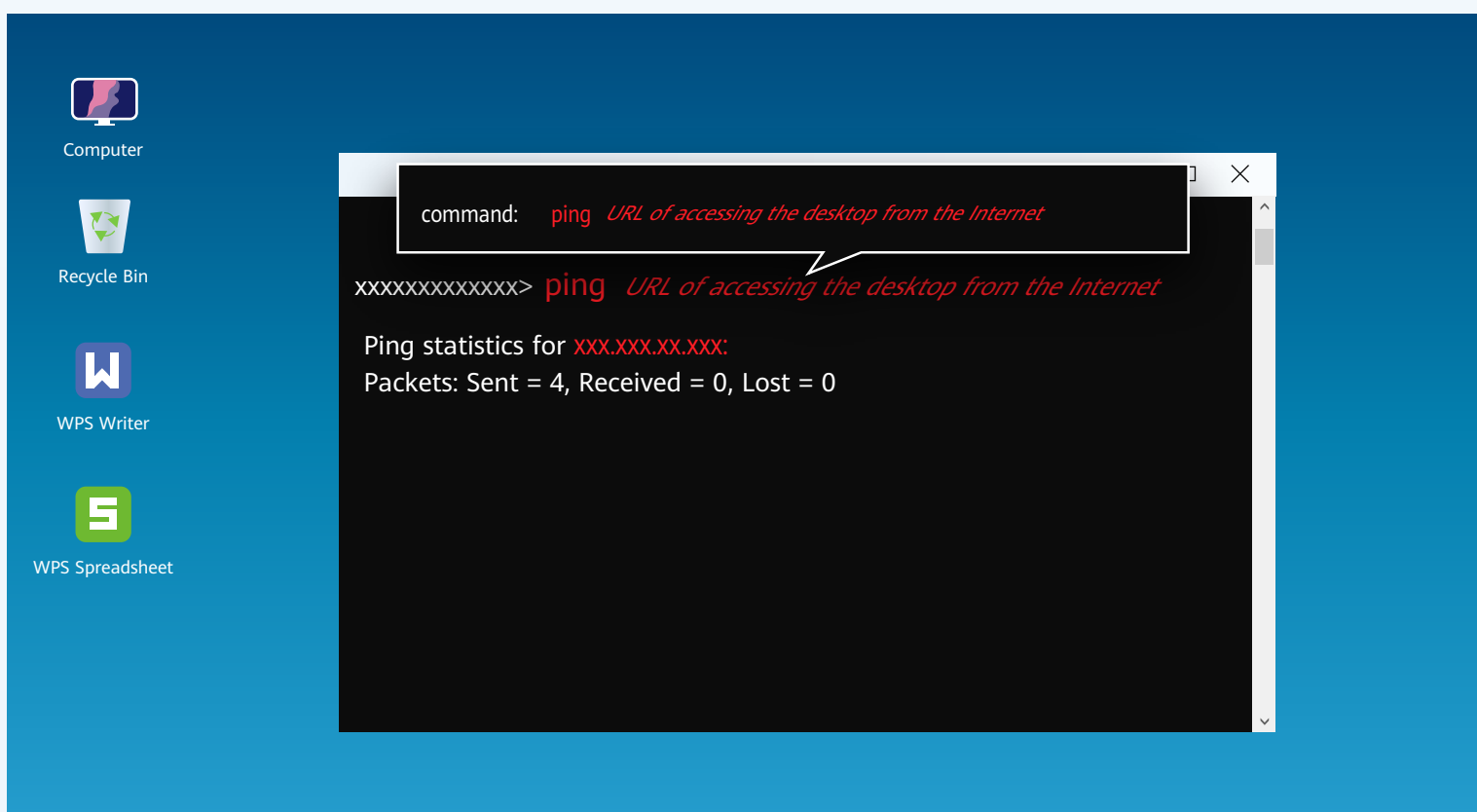
Check the network status

- 1 Click  and check the latency in Network Status.



- 2 Run the following command in the CLI to check the network connection between the terminal and the desktop:

`ping URL of accessing the desktop from the Internet`



To enter the Windows desktop CLI, perform the following steps:

- ◆ On the **Start** menu, enter **cmd** in the **Search** application to open the CLI.

Installing Applications

Note: Before performing the following operations, contact the administrator to enable related policies or configurations.



File copy: The terminal user copies the applications to be installed from the local PC to the desktop for installation.



USB copy: The terminal user copies the applications to be installed to the desktop using the USB flash drive for installation.



Internet: The terminal user downloads and installs applications from the Internet.



App store: The terminal user downloads and installs applications from the general app store.

A Change History

Release Date	Description
2022-12-26	This issue is the first official release.