

Product Bulletin

Product Bulletin

Issue 01
Date 2024-02-04



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.

Huawei Technologies Co., Ltd.

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

Website: <https://www.huawei.com>

Email: support@huawei.com

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 Workspace Client Version Support.....	1
2 Client Integrity Check.....	3
3 Restrictions on Sales Scenarios.....	5

1 Workspace Client Version Support

This document describes the client version support of Workspace.

NOTE

When a new Workspace client version is released, detailed version change description is provided.

Version Description

Version number: The format is $x.y.z.n$, where $x.y$ indicates the major version number, x indicates the last two digits of the current year, y indicates the current month, z indicates the minor version number, and n indicates the patch version number.

For example, in 23.2.0.0208, 23.2 indicates the major version released in February 2023, 0 indicates the minor version under the major version, and 0208 indicates the patch version under the major/minor version.

Version Support

NOTICE

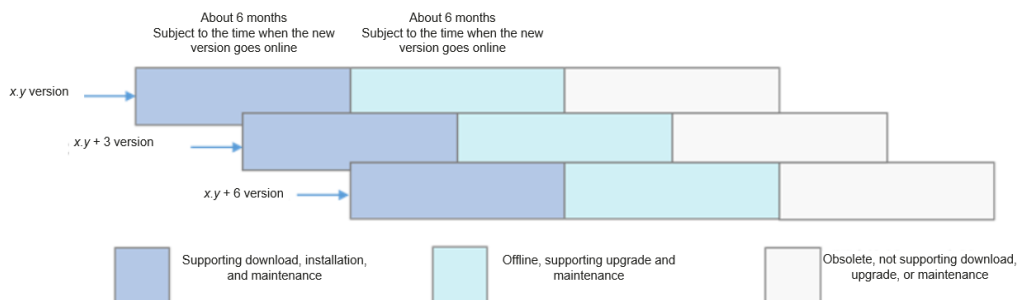
Offline: indicates that the download entry from the Workspace official website is no longer provided, and minor versions and new features of the client of this version are no longer released.

Obsolete: Workspace will no longer provide support for this version, including release of new functions, vulnerability fixes, and upgrade.

The Workspace version support policies are as follows:

Workspace client maintenance

Workspace supports the maintenance of a maximum of four major client versions, such as 22.2, 22.5, 22.8, and 22.11. For example, after 23.2 is put into commercial use, earlier versions (such as 22.2) will be obsolete.



Client upgrade

Workspace allows you to upgrade three major versions at the same time. Each version is maintained for one year. For example, after 23.2 is available, earlier versions (such as 22.5) cannot be upgraded. Therefore, you must upgrade your Workspace clients before the maintenance period ends.

- **Client version upgrade:** After the latest major version (such as 23.2) goes online, the client can be upgraded to the last stable version (such as 22.5) of the second latest major version.
- **Client patch upgrade:** For existing clients running on the live network, if there are major issues or vulnerabilities of the open source community, Workspace will perform the patch upgrade on these clients in the background. Users need just one click to complete the upgrade. If the patch upgrade has adverse impact on user services, Workspace will release a notice one week in advance.

Version Release Cycle

Generally, a major version of the Workspace client is released in about three months, and a minor version is released based on external requirements. A patch version is used to fix critical issues.

Version Constraints

After a client is upgraded to a new version, if you need to roll back the client to the old version, you need to uninstall the new version and then install the old version.

2 Client Integrity Check

Scenario

Check the software package integrity.

Prerequisites

- You have created a Workspace desktop.
- You have obtained the software package whose integrity needs to be verified.

Table 2-1 Verification code

Installation Package	Version	SHA256 value
Android	23.2.2	851c0058420a150c2dcc830f890c6db96a9f8950c57f52bef1245ddd6a95fc58
Kylin-AMD64	23.8.3	8eb55b35040a2fc234030a7e79d0f2f0437399690ae3e2f3b22c1f4d804ad2e7
Kylin-ARM64	23.8.3	835031b355acb86b587747ef16c576eff400b54cca72cb87802dac840fb35e99
UOS-AMD64	23.8.3	8eb55b35040a2fc234030a7e79d0f2f0437399690ae3e2f3b22c1f4d804ad2e7
UOS-ARM64	23.8.3	835031b355acb86b587747ef16c576eff400b54cca72cb87802dac840fb35e99
Ubuntu-AMD64	23.8.3	8eb55b35040a2fc234030a7e79d0f2f0437399690ae3e2f3b22c1f4d804ad2e7

Verifying Software Package Integrity

Step 1 Log in to the Windows cloud desktop as a user.

Step 2 On the cloud desktop, press **Win + r** and enter **cmd**. The command line interface (CLI) is displayed.

Step 3 Run the following command to obtain the hash value of the software:

```
certutil -hashfile {Software package directory}/{Software package name}  
sha256
```

Replace *Software package directory* with the actual download directory, for example, C:\Users.

Software package name: Replace it with the name of the downloaded software package, for example, **Workspace_xxx.apk**.

Example: certutil -hashfile Workspace_android.apk sha256

Step 4 Compare the SHA256 hash value obtained in [Table 2-1](#) with the hash value obtained in [Step 3](#).

- If they are the same, the verification is successful.
- If they are different, download the software of the corresponding version and repeat [Step 3](#) to [Step 4](#) to verify the software.

----End

3 Restrictions on Sales Scenarios

Table 3-1 describes the sales scenarios of Workspace.

 **NOTE**

- **Sales allowed:** Workspace can meet the requirements of most common scenarios. However, as user experience is closely related to network QoS and cloud desktop configurations, PoC, performance, and compatibility tests should be performed after customers sign for approval.
- **Sales restricted:** Workspace may not be able to meet requirements in these scenarios. A PoC test must be performed to evaluate desktop performance and compatibility. Sales is allowed only when the performance and compatibility meet customer requirements.
- **Sales prohibited:** Workspace cannot be sold because it does not meet customer requirements.

Table 3-1 Sales scenarios of Workspace

Category	Sales Scenario	Network Access of End Users	Description
Sales allowed NOTE PoC tests must be performed. The performance and compatibility result must be approved with the customer signature.	Office automation (OA)	Internet and Direct Connect access	OA of government organizations and enterprises. Typical applications include Microsoft Office, WPS, Chrome, and audio and video players. The typical scenarios are as follows: <ul style="list-style-type: none">• Secure intranet OA• Work from home/Remote OA• Upstream and downstream secure OA such as suppliers• Customer service and O&M• Multi-branch office access in retail stores/enterprises

Category	Sales Scenario	Network Access of End Users	Description
	Development and testing	Internet and Direct Connect access	Code development and testing of small and medium-sized enterprises. Typical applications include Eclipse, Visual Studio, IDE, XShell, and PuTTY. The typical scenarios are as follows: <ul style="list-style-type: none"> • Software development, testing, and outsourcing • Big data development and testing • Chip design and R&D • Web development
	GPU design	Internet and Direct Connect access	3D design and rendering in the design and manufacturing industries. Typical applications include AutoCAD, CATIA, Creo, NX, Maya, 3ds Max, UE4, Premiere, and BIM. The typical scenarios are as follows: <ul style="list-style-type: none"> • Industrial design (automobiles, integrated circuits, and home appliances, etc.) • Media production (movies, broadcasting, and television) • Architectural design (buildings, real estate, and interior design) • Rendering/Animation (gaming/virtual humans)
Sales restricted NOTE PoC tests must be performed. The performance and compatibility result must be approved with the customer signature.	Concurrent peripherals	Internet and Direct Connect access	Although end users use Direct Connect for access, they still need latency-sensitive peripheral functions, such as handwriting tablet, camera, high-speed document scanner, scanner, and printer. In addition, multiple peripherals may be used for access at the same time. The bandwidth and latency requirements of peripherals are subject to the PoC test.
	Non-linear video editing	Internet and Direct Connect access	Non-linear editing (NLE) requires hardware resources of high-performance graphics cloud workstations. More editing tracks require higher configuration. The compatibility of NLE software also depends on partners' application software. The PoC test result shall prevail and the sales are restricted.

Category	Sales Scenario	Network Access of End Users	Description
	Video conferencing	Internet and Direct Connect access	<p>Video conferencing:</p> <p>Video conferencing requires concurrent video codec. CPU/GPU codec is resource- and bandwidth-consuming. Video conferencing software based on the existing VDI network architecture cannot ensure good user experience if the VDI is not optimized.</p> <p>Solution:</p> <p>Use a PC as the client and hold a video conference on the PC. That is, install the video conferencing software on the PC rather than on Workspace. Perform PoC tests and the test result must be approved with the customer signature.</p>
	Call centers	Internet and Direct Connect access	There is a mature solution based on Huawei AICC. Perform PoC tests to check whether the performance and latency meet customer requirements.
<p>Sales prohibited</p> <p>NOTE Scenarios and solution capabilities do not match.</p>	Embedded development and hardware burning	N/A	Embedded development involves hardware burning, which is sensitive to network latency and jitter. The cross-network technical architecture adopted by the Workspace solution cannot meet the requirements on latency and jitter.
	Simulation (such as Android development)		Emulator simulation involves nested virtualization. Huawei Cloud platform does not support the nested virtualization function.
	Nested desktop login		In nested desktop login scenarios, user experience cannot be guaranteed. For example, a computer slowly responds to keyboard and mouse device operations due to the delay in multi-layer nesting, compression artifact occurs, and even other functions are affected.

Category	Sales Scenario	Network Access of End Users	Description
	Video surveillance		The performance of video surveillance depends on the decoding mechanism of video software, GPU decoding, and number of concurrent video channels. Currently, Workspace cannot provide proprietary GPU desktops to meet these requirements.