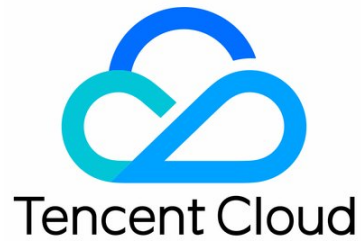


# Cloud Workload Protection Platform

## FAQs



## Copyright Notice

©2013–2025 Tencent Cloud. All rights reserved.

The complete copyright of this document, including all text, data, images, and other content, is solely and exclusively owned by Tencent Cloud Computing (Beijing) Co., Ltd. ("Tencent Cloud"); Without prior explicit written permission from Tencent Cloud, no entity shall reproduce, modify, use, plagiarize, or disseminate the entire or partial content of this document in any form. Such actions constitute an infringement of Tencent Cloud's copyright, and Tencent Cloud will take legal measures to pursue liability under the applicable laws.

## Trademark Notice

 Tencent Cloud

This trademark and its related service trademarks are owned by Tencent Cloud Computing (Beijing) Co., Ltd. and its affiliated companies ("Tencent Cloud"). The trademarks of third parties mentioned in this document are the property of their respective owners under the applicable laws. Without the written permission of Tencent Cloud and the relevant trademark rights owners, no entity shall use, reproduce, modify, disseminate, or copy the trademarks as mentioned above in any way. Any such actions will constitute an infringement of Tencent Cloud's and the relevant owners' trademark rights, and Tencent Cloud will take legal measures to pursue liability under the applicable laws.

## Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

## Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

# Contents

## FAQs

- Purchase

- Functionality

- Intrusion Related

# FAQs

## Purchase

Last updated: 2025-02-27 11:47:28

### How To Purchase the Host Security Professional Version and Flagship Edition?

You can upgrade on the [Host Security Purchase Page](#). For details, see the [Purchase Guide](#).

### How To Disable Host Security Professional Protection or Flagship Protection Service?

Go to the [Authorization Management Page](#) to view authorization details. You can perform the following operations on the authorized hosts:

- Professional Version – Pay-as-you-go: You can unbind or turn off the Professional Version. Unbind: Each host can only be unbound once per month; Turn off Professional Version: The number of licenses will decrease by 1 after turning off (if there is only one license, turning off the Professional Version will directly destroy the license order).

#### Note:

- Due to the adjustment in the billing mode, CWPP will discontinue the pay-as-you-go mode for the Professional Version starting from November 30, 2023. After the adjustment, new purchases of the Professional Version in pay-as-you-go mode will no longer be supported. Existing old pay-as-you-go orders can still be used and scaled out normally.
- If the related old pay-as-you-go orders are terminated, it will no longer be possible to scale out on the old orders in pay-as-you-go mode.

The screenshot shows the '授权详情' (Authorization Details) page for a '专业版-按量计费' (Professional Version - Pay-as-you-go) license. The page includes a '使用中' (In Use) status indicator and a '购买授权' (Purchase License) button. The license information section displays the resource ID, purchase time (2022-09-08 16:40:43), protection validity period (每天), and tags. The '已绑定主机 (1)' (1 Bound Host) section shows a table with columns for '绑定主机名称/IP', '主机标签', '主机状态', and '操作'. The table contains one entry with a checkbox, the host name '内...', '暂无标签', and a status of '已关机'. The '操作' column for this entry includes buttons for '更换授权', '解绑', and '关闭专业版'.

- Professional Version – Annual/Monthly Subscription and Ultimate Version – Annual/Monthly Subscription: You can perform the unbinding operation. Unbind: Each host can only be unbound once per month.

### 授权详情 使用中 购买授权 ×

[续费](#) [扩容](#) [升级旗舰版](#)  自动续费 ①

---

#### 授权信息

资源ID: [REDACTED] 📄

购买时间: 2022-09-15 16:17:47

防护有效期: 2022-09-15 16:17:47 至 2022-10-15 16:17:47

标签: 无 ✎

备注: ✎

已用授权 / 总授权数  
**1 / 1**

---

#### 已绑定主机 (1)

[批量解绑](#) [批量更换授权](#)  🔍 🔄 📄

<input type="checkbox"/>	绑定主机名称/IP	主机标签	主机状态	操作
<input type="checkbox"/>	[REDACTED] 内 [REDACTED] 公	暂无标签	防护中	<a href="#">更换授权</a> <a href="#">解绑</a>

#### ⚠️ Note

- After the Cloud Virtual Machine (CVM) expires or is manually terminated, the CWPP Professional/Ultimate protection licenses will be automatically unbound. The freed licenses can be bound to other servers.
- After disabling the CWPP Professional and Ultimate protection services, high-risk vulnerability monitoring and warning services for the server will no longer be provided.
- The fee for CWPP is deducted based on the actual number of licenses purchased, regardless of whether the license is bound to a host or whether the host is powered on.

## Will Purchasing the Security Protection License Automatically Bind It To the Host?

According to the actual situation, it is divided into the following three types:

- If the user chooses to bind the host when purchasing the protection license, the host will be automatically bound after the purchase.

The screenshot shows the 'Host Security Protection' interface. At the top, there's a 'Host Security Protection' title and a 'Large Region' dropdown. Below that, there are tabs for 'Security Protection' and 'Value-added Services'. A 'Protection License' section shows '2' licenses. A red box highlights the 'Immediately bind host (1 selected)' checkbox. Below this, there are dropdowns for 'Direct Selection', 'All Server Zones', and 'All Regions'. The 'Select Hosts' section has a search bar and a table of hosts. The first host is selected with a red box. The 'Already Selected Hosts' section shows one host. At the bottom, there are sections for 'Automatic Purchase' and 'Tags', and a summary bar showing 'Basic Protection' and 'Value-added Services' for 0.00 yuan.

- If the user does not choose to bind the host when purchasing the protection license, they need to go to the [Authorization Management page](#) to bind after the purchase.
- If the user has enabled the auto-binding switch, the host will be automatically bound if there are remaining licenses.

The screenshot shows the 'Authorization Management' page. It has a 'Go to Order Center' link. The 'Protection License Overview' section shows 'Remaining Available Licenses' with a 'Purchase Protection License' button. Below this, there are sections for 'Automatic Renewal' (turned on), 'Automatic Binding' (turned on and highlighted with a red box), and 'Automatic Purchase' (turned off).

## Why Does a New Purchase Of CVM Automatically Generate a Sub-Order For CWPP Professional Protection?

If you turn on the Automatic Upgrade Protection switch in the [Authorization Management](#) of the Host Security console, newly added cloud servers will automatically upgrade to the professional protection edition, and a sub-order for purchasing Host Security professional protection will be automatically generated in the order.

## How To Handle Issues With Tencent Cloud Account Real-Name Authentication?

If you encounter any Tencent Cloud account issues while using Host Security, please refer to the [Account Document](#) for details.

## Does the Host Security Product Conflict With Other Security Products?

CWPP does not conflict with other security products and belongs to different protection dimensions, providing security capabilities at different levels to ensure user safety.

## How To Uninstall the Tencent Cloud CVM CWPP Client?

Log in to the [CWPP Console](#), select **Asset Management > Host List** in the left navigation bar, find the CVM to be uninstalled in the server list, and click **Uninstall**, or open the installation directory and use the uninstallation program in the directory to uninstall.

## Will Adding a New Protection Directory Consume the Web Tamper Protection License?

Authorization is calculated based on the machine dimension, meaning 2 machines consume 2 authorizations. Users can configure multiple protection directories on one machine, with a total file number limit of 10,000.

On the add protection directory page of [Webpage Tamper-proofing](#), when selecting the server where the directory is located, you can view the authorization status on the right side of the server. If it is an authorized server, it does not consume authorization. If you select an unauthorized server, it will prompt that authorization will be consumed.

添加防护

添加防护目录

防护目录①

名称①

防护文件类型①

选择目录所在服务器 可使用授权服务器数: 1 个

服务器标签

选择区域

选择云服务器

请输入服务器名称/IP/ID进行搜索

服务器名称/IP	标签	授权状态
<input checked="" type="checkbox"/> 镜像 119.1...		已授权
<input type="checkbox"/> 未命名 10.1...		未授权

已选择 1 台服务器, 消耗授权数 0

服务器名称/IP	授权状态	防护开关	自动恢复开关 ①
镜像 119.1...	已授权	<input checked="" type="checkbox"/>	<input type="checkbox"/>

# Functionality

Last updated: 2025-02-27 11:53:07

## How Often Are the Virus and Vulnerability Libraries Updated?

Virus library: updated at 00:00 every day.

Vulnerability library: updated from time to time.

## Why May the Detection Results Be Different Between Multiple Scans Of the Vulnerabilities Of Jar Packages?


The detection of Jar package vulnerabilities, for example, Struts2 vulnerability highly dependent on whether the Jar package is loaded. The vulnerability cannot be detected when the package is not loaded. When the service is running, the Webserver loads the Jar package in two modes — dynamic loading and static loading. In the dynamic loading mode, the Struts2 vulnerability can only be detected when the Jar package is running, so the check results are different between periods. It is recommended to scan for high-risk Jar package vulnerabilities multiple times to improve the accuracy of the check results.

## What Is the Scan Frequency Of the Host Security?

- Host Security Basic Version: Provides one-time detection.
- CWPP Professional Version: Supports Customized Cycle.
- Host Security Flagship Version: Supports Customized Cycle.

## How To Handle a Trojan File?

On the [Malicious File Scan](#) page, you can handle Trojan files as follows:

- Delete: Click  to copy the trojan file path, locate the trojan, and manually delete the file.

<input type="checkbox"/>	服务器IP名称	路径	病毒名	首次发现时间 ↑	最近检测时间 ↓	处理状态	操作
<input type="checkbox"/>		c:\[redacted]	Win	2021-09-14 16:24:01	2021-09-14 16:24:01	待处理	<a href="#">详情</a> <a href="#">信任</a> <a href="#">隔离</a> <a href="#">删除记录</a>
<input type="checkbox"/>		c:\[redacted]	Win	2021-09-14 16:24:00	2021-09-14 16:24:00	待处理	<a href="#">详情</a> <a href="#">信任</a> <a href="#">隔离</a> <a href="#">删除记录</a>

- Trust: You can perform a trust operation, and Host Security will no longer detect this file on the machine.
- Isolation: Currently, intercepting Trojans is not supported. Only real-time or post-event detection and alarms are available. However, you can perform an isolation operation on the file to prevent it from being launched again.

## What Is the Security Scoring Mechanism On the Overview Page?

For more information on the security scoring mechanism on the overview page, see the [Security Overview](#) document.

## How To Back Up Data Automatically Using Snapshots?

Snapshot is a data backup method provided by Tencent Cloud. It can create a fully-available duplicate of the specified cloud disk, whose lifecycle is independent of the lifecycle of the original cloud disk. You can create snapshots regularly to quickly recover data in case of accidental data loss.

You can create a snapshot in the console as instructed below:

1. Log in to the [CBS console](#).
2. On the Cloud Disk page, find the row of the instance for which you need to create a snapshot, and click **Create Snapshot**.

快照总大小	计费模式	随实例释放	操作
未创建快照	按量计费 2020-02-10 10:39:12 创建	随实例释放	<a href="#">续费</a> <b>创建快照</b> <a href="#">更多</a>

3. On the create snapshot page, confirm the information, enter the snapshot name, click **Submit**, and wait for the snapshot to be created.

For more information, see the [Snapshot Overview](#) and [Creating Snapshots](#) documents.

## How Long Does It Take For Security Baselines To Take Effect Once They Are Configured In the Product?

The security baselines take effect immediately after the product is configured.

## What Should Be Done If the Result Of a Security Baseline Check Item Is "Failed"?

1. Go to the [Security Baseline](#) page, select the failed detection item, click **View Details** in the action column to enter the details page of the detection item.

基线名称	基线检测项	影响服务器数	最后检测时间	处理状态	操作
	1	1	2021-06-03 19:31:24	未通过	<a href="#">查看详情</a> <a href="#">重新检测</a>

2. On the details page, select the required server IP, and click **Details** to enter the Detection Detail Page.

服务器IP/名称	检测通过项	风险项	首次检测时间	最后检测时间	状态	操作
1 公	0	1	2021-06-03 19:31:25	2021-06-03 19:31:24	未通过	<a href="#">重新检测</a> <a href="#">详情</a>

3. On the Detection Detail Page, hover the mouse over  to view the processing suggestion for the baseline.

**MySQL 弱口令检测**

描述  
MySQL 存在弱口令: [redacted]

**处理建议 (处理时请先做备份)**

1. 改用更复杂的密码, 推荐字母、数字、特殊符号组合, 长度高于 10 位;
2. 选择使用腾讯云 CDB。
3. 如果直接删除账户, 需执行 OPTIMIZE TABLE mysql.user; 命令进行优化。

说明	威胁等级	状态	最后检测时间	操作
MySQL 存在弱口令...	高危	未通过	2021-06-03 19:31:24	<a href="#">重新检测</a> <a href="#">忽略</a>

10 条 / 页

## Will I Be Notified If the Host Security Detects Attacks Such As Vulnerabilities and Trojans?

Yes. You will get alarms if CWP detects attacks such as Trojans, emergency vulnerabilities, or other attacks, and will be notified via internal messages, SMS, email, or WeCom. You can set your notification channel in the [Message Center](#).

# Intrusion Related

Last updated: 2025-02-27 11:48:07

The following video will introduce the significance of protecting host security, preventive measures, and solutions to common issues:

[Watch video](#)

- **Intrusion FAQs**

- [What are the damages of a Cloud Virtual Machine \(CVM\) intrusion?](#)
- [How to reduce the probability of a Cloud Virtual Machine \(CVM\) intrusion?](#)
- [How to protect a Cloud Virtual Machine \(CVM\) after an intrusion?](#)
- [How to implement preventive measures for a Cloud Virtual Machine \(CVM\)?](#)

- **Trojan Related Issues**

- [Will I be notified if the host security detects attacks such as vulnerabilities and Trojans?](#)
- [How to resolve false negatives in Trojan detection?](#)
- [How to handle Trojan and virus files?](#)

- **Abnormal Log-in Issues**

- [How to resolve the log-in exception displayed by the CVM?](#)
- [How to handle abnormal log-in alarms?](#)
- [How to eliminate false alarms when normal log-in behavior is reported as abnormal?](#)
- [Can abnormal log-in detection be disabled?](#)

- **Password Leakage Issues**

- [How to handle brute force cracking of a Cloud Virtual Machine \(CVM\)?](#)
- [Note: How to resolve after the password is successfully brute force cracked?](#)

- **Offline Protection Status Issues**

- [How to solve the problem when the protection status of a Cloud Virtual Machine \(CVM\) shows offline?](#)

## What are the damages of a CVM intrusion?

- Business interruption: Databases and files are tampered with or deleted, resulting in inaccessible services and system paralysis.
- Data theft: Hackers steal corporate data and sell it publicly, leading to customer privacy leaks, which causes damage to the corporate brand and user loss.
- Being encrypted and ransomed: Hackers intrude into cloud servers and implant irreversible ransomware to encrypt data, extorting money from enterprises.
- Service instability: Hackers run mining programs and DDoS Trojan programs on the CVM, consuming a large amount of system resources, causing the CVM to fail to provide services.

## How to reduce the probability of CVM intrusion?

- Timely fix high-risk vulnerabilities and baseline issues.
- Set a strong password to avoid brute force attacks.
- Periodically inspect accounts, permissions, and ports, and promptly handle Alarm information in the [CWPP Console](#).
- Regularly create snapshot backups. For details, see [Creating Snapshots](#).

## How To Protect a CVM After Being Intruded?

The preventive measures are recommended as follows:

- Set the CVM password to a complex password containing 12–16 characters, including uppercase letters, lowercase letters, special characters, and numbers. You can also use a password generator to automatically generate a complex password.
- Delete unnecessary users set on the CVM, and for users who do not need to log in, set their permissions to prohibit login.
- Change the default port number of the remote login service and prohibit super administrator users from logging in. For Windows remote port modification, refer to [How to Modify the 3389 Server Remote Port](#), and for Linux remote port modification, refer to [Modify SSH Port + Prohibit ROOT Login](#).

- A more secure method for Linux systems is to use key-based login only and prohibit password login.
- Tencent Cloud platform provides [Security Group Features](#). It is recommended to open only business protocols and ports, and not to open all protocols and ports.
- It is not recommended to open core application service ports such as MySQL and Redis to the public network. You can change to local access or prohibit external network access.
- If your local external IP is fixed, it is recommended to use a security group or system firewall settings to prohibit login requests from all IPs except the local external IP.

**Note:**

Regular security protection of the CVM system can effectively enhance its security but cannot guarantee absolute safety. It is recommended to conduct regular security inspections and data backups of the CVM system to prevent data loss or business unavailability due to unexpected situations.

## How to implement preventive measures for CVM?

It is recommended to [upgrade to CWPP Professional Edition](#) and handle security events of medium risk and above.

## Will I be notified if Host Security detects attacks such as vulnerabilities and Trojans?

Yes. If CWPP detects Trojans, emergency vulnerabilities, or other attacks, you will be notified via internal message, SMS, email, or WeCom. You can set your notification channel in the [Message Center](#).

## How To Resolve a False Negative In Trojan Detection?

If undetected Trojan files are found, you can contact and submit them to the Tencent Cloud security team through a [ticket](#) for quick identification by the Tencent Cloud security team.

## How to handle Trojan and virus files?

- If viruses and Trojan files are found, isolate or delete the malicious files promptly.
- Some stubborn Trojans and viruses may repeatedly write themselves. It is necessary to check for weak passwords, vulnerabilities, and other anomalies on the machine and fix them, while also deleting the malicious files.
- Some infected malware trojans are extremely difficult to clean. It is recommended to regularly take snapshot backups of the machine.
- For more operations, refer to [Operational Processing of Trojan Files](#).

## How to resolve login exceptions on the CVM?

Abnormal login is determined based on the admin's usual login locations. Please carefully check the login records. If it is not the admin logging in, the password may have been compromised, and a detailed security check on the CVM is required.

## How to handle abnormal login alarms?

1. First, confirm whether the abnormal login was performed by relevant business personnel. If not, check the console for Trojans, vulnerabilities, or abnormal resource usage. If any exceptions are found, handle them promptly.
2. Confirm whether the login account has a weak password and modify it promptly.
3. Troubleshoot the machine for abnormal login accounts or accounts with excessive permissions, and disable the accounts or adjust the permissions promptly.

## How To Eliminate a False Alarm For Abnormal Login In Normal Login Behavior?

You can log in to the [Host Security Console](#), select **Intrusion Detection** > **Unusual Login** from the left navigation, find the record defined as an unusual login on the Unusual Login page, and click **Add to Allowlist** in the right action column to eliminate the false alarm by custom adding the login to the allowlist.

## Can abnormal login detection be disabled?

Abnormal login detection cannot be disabled. If you do not want to receive abnormal login alarm notifications, you can add the login source to the allowlist or uncheck the alarm notification. The steps are as follows:

- **Method 1:** On the [Unusual Login page](#), select **Allowlist Management > Adding to the allowlist**, and add the login source to the allowlist.

**异常登录**

异常登录 **白名单管理**

**重要提示:**

1. 白名单用于用户设置允许的登录来源，规则采用“非白即黑”策略，仅允许白名单范围内登录，若有非白名单来源登录将会发出异常告警，请您谨慎设置白名单。 [告警设置](#)
2. 若机器未设置登录白名单（包括单机、全局规则），主机安全默认以用户首次登录该机器的来源地为可信源。若机器有设置白名单列表，则以白名单列表为准。建议用户根据实际情况设置完善的白名单。
3. 单条规则的四个维度“登录源IP、登录用户名、登录时间、常用登录地”设定为“and”逻辑，即一个登录事件必须同时满足四个条件才会匹配此规则。单个条件设置为空，则代表不限制。
4. 白名单设置后，5分钟内生效。若日常出现异常登录告警，经用户确认为正常登录，可在白名单管理列表对相应规则进行编辑、删除操作。

删除 **添加白名单** 选择日期 多个关键字用竖线“|”分隔，多个过滤标志用回车键分隔

服务器名称	来源IP	常用登录地	登录用户名	登录时间	创建时间	修改时间	备注	操作
<input type="checkbox"/> 全部服务器		广东-深圳市	root	--	2021-02-07 09:54:00	2021-02-07 09:54:00		<a href="#">编辑</a> <a href="#">删除</a>

- **Method 2:** On the **Settings Center > Alarm Settings** page, uncheck the alarm items "high-risk abnormality" or "suspicious abnormality" for unusual logins.

#### Note:

If you uncheck this option, you will not receive real-time alarm notifications for remote logins. Please proceed with caution.

**入侵检测**

事件类型	告警状态	告警时间	告警项
文件查杀	<input type="checkbox"/>	<input type="radio"/> 全天 <input type="radio"/> 09:00 ~ 18:00	
异常登录	<input checked="" type="checkbox"/>	<input type="radio"/> 全天 <input checked="" type="radio"/> 09:00 ~ 18:00	<input checked="" type="checkbox"/> 高危异常 <input checked="" type="checkbox"/> 可疑异常
密码破解	<input checked="" type="checkbox"/>	<input type="radio"/> 全天 <input checked="" type="radio"/> 09:00 ~ 18:00	<input checked="" type="checkbox"/> 暴破成功

## How to handle brute force cracking of a CVM?

If the CVM is successfully cracked by brute force, promptly troubleshoot and handle any anomalies on the machine:

- Check if there are any accounts with weak passwords on the machine, modify weak passwords or use keys for login. Additionally, you can reduce the risk of brute force cracking by setting up security groups or other methods.
- CWPP has launched a brute force cracking block feature for effective interception in Host Security.

## How To Resolve After a Password Is Successfully Cracked By Brute Force?

After the password is successfully cracked, the CVM may have been compromised by hackers and backdoor programs may have been left.

- Check the CVM security status for any unknown accounts and Trojan files. If found, delete and fix them immediately, and change the CVM login password. For more information, see [Linux Intrusion Troubleshooting](#) or [Windows Intrusion Troubleshooting](#).
- Decide whether to reset the CVM based on the actual situation, and set a complex password, preferably a combination of letters, numbers, and special characters, with a length of 15 characters or more.

## How to resolve the offline protection status of a CVM?

The Tencent Cloud CWPP client is not connected to the server-side, causing the backend to display offline. It is recommended to re-download and install the CWPP client. Possible reasons for being offline are as follows:

- The CVM has enabled firewall rules.
- The CVM has installed third-party malware, causing the security protection program to be compromised.

#### Note:

For fault troubleshooting methods, see [Offline Agent on Linux](#) or [Offline Agent on Windows](#).