Cloud Workload Protection Platform

FAQs

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

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.

- 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.

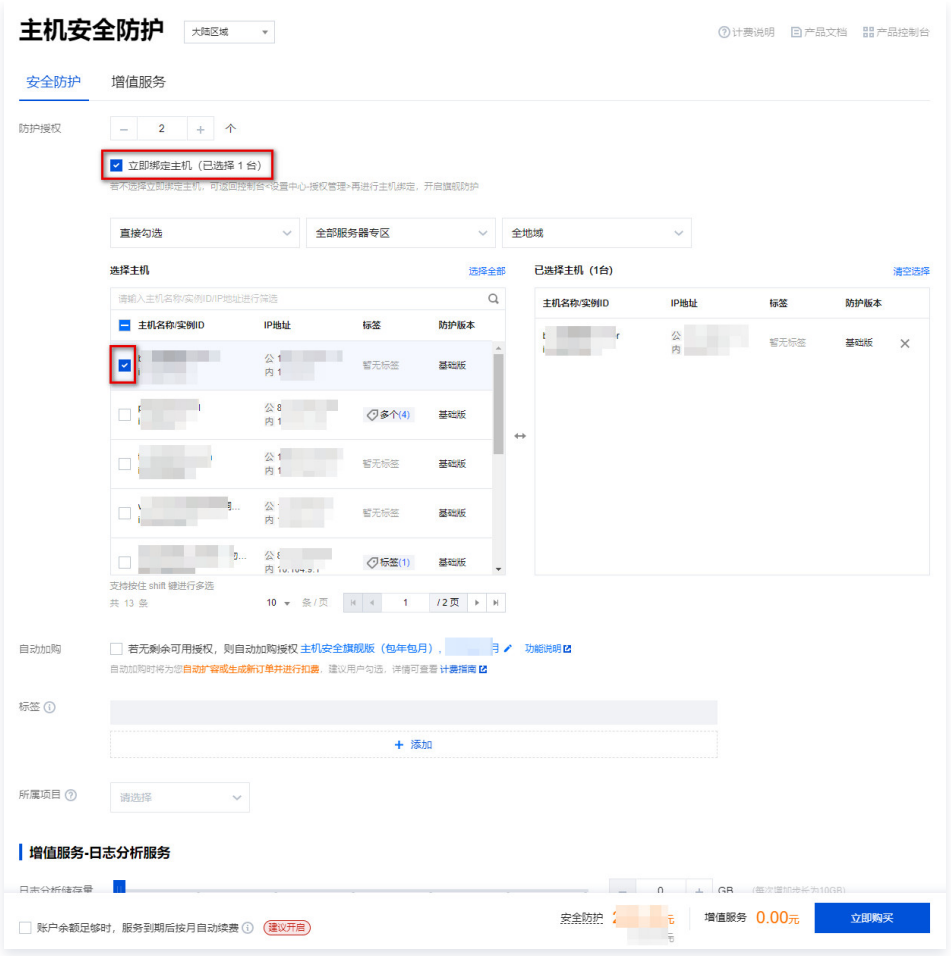
Note

- 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.

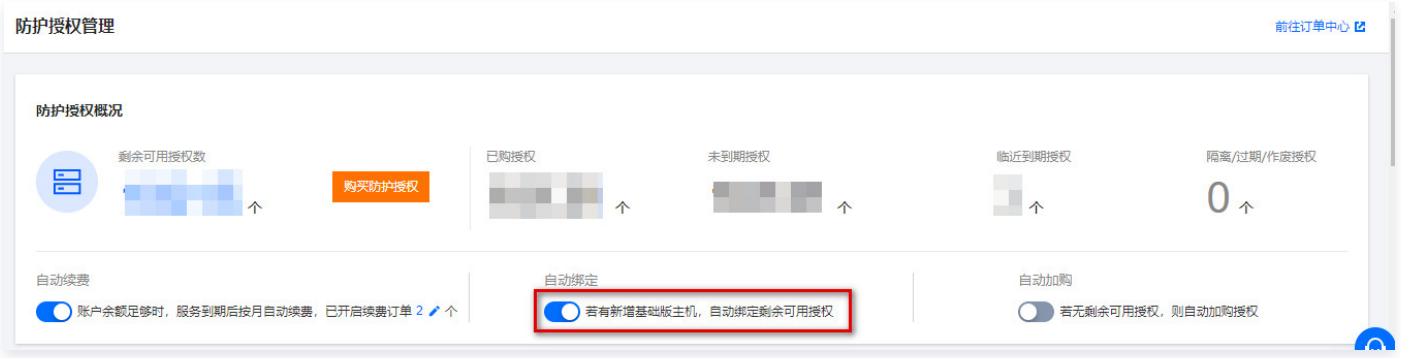
Will Purchasing the Security Protection License Automatically Bind It To the Host?

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.



- 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.



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.

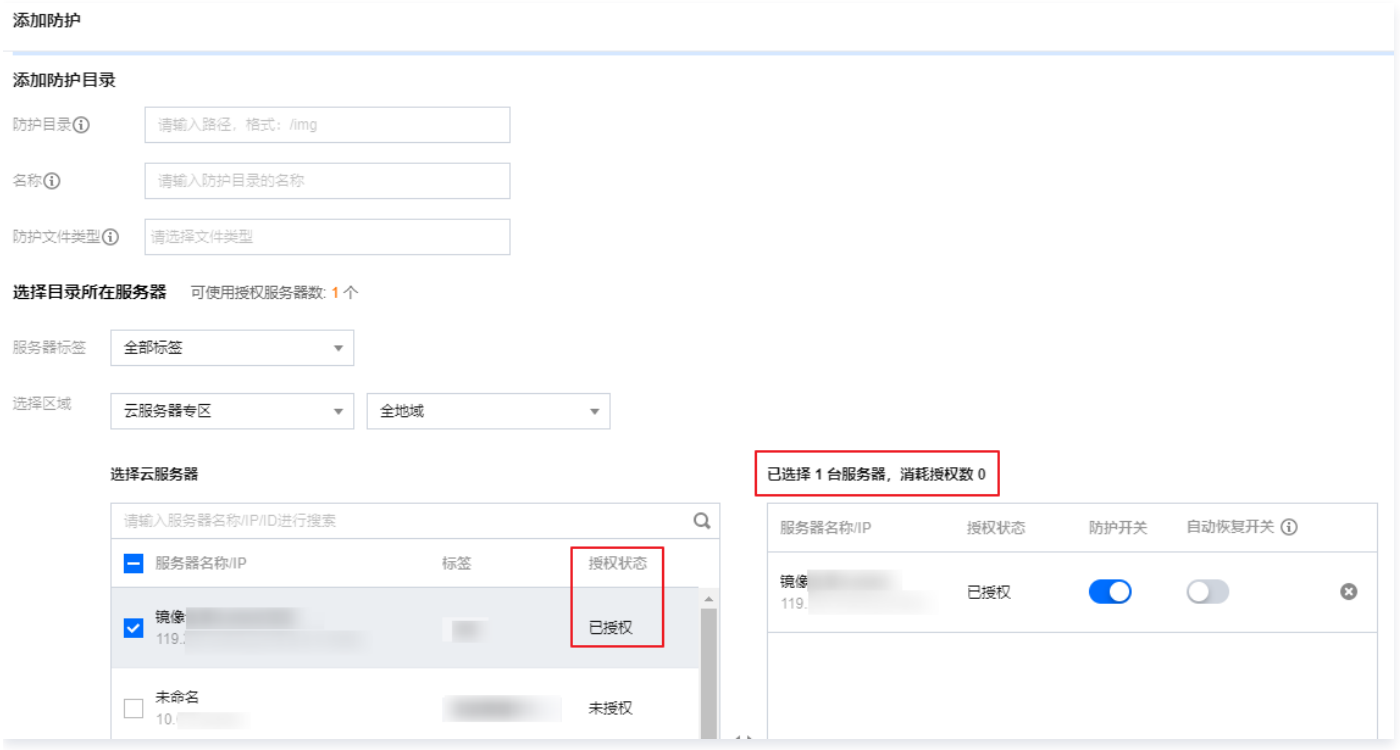
How To Uninstall the Tencent Cloud CVM CWPP Client?

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.



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.

- 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**.

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

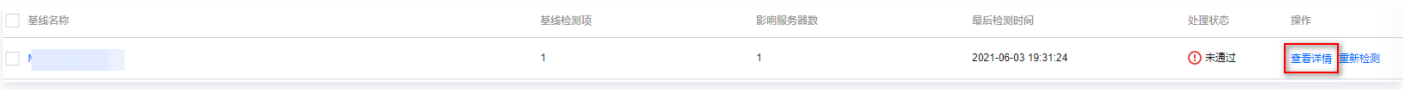
For more information, see the Snapshot Overview and Creating Snapshots documents.

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.



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

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

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

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.

- **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.

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.