ALIBABA CLOUD

Alibaba Cloud

Security Center

Overview of Console

Document Version: 20220331

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	**Danger:** Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	**Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Overview (new version)

This topic provides a brief introduction to the Overview tab of the Security Center console. The Overview tab is a security operations center for your Alibaba Cloud services. The tab displays the information about your assets, including the security score, risks, security trends, and brief asset information. The tab also provides entry points to upgrade and renew Security Center, and increase related quotas. You can perform security operations on your assets in a centralized manner on the Overview tab.

Background information

The new version of the **Overview** tab is released on February 22, 2022. Compared with the old version of the **Overview** tab, the new version of the **Overview** tab has the following benefits: The UI is re-designed, and the statistics that you must know are conspicuously displayed.

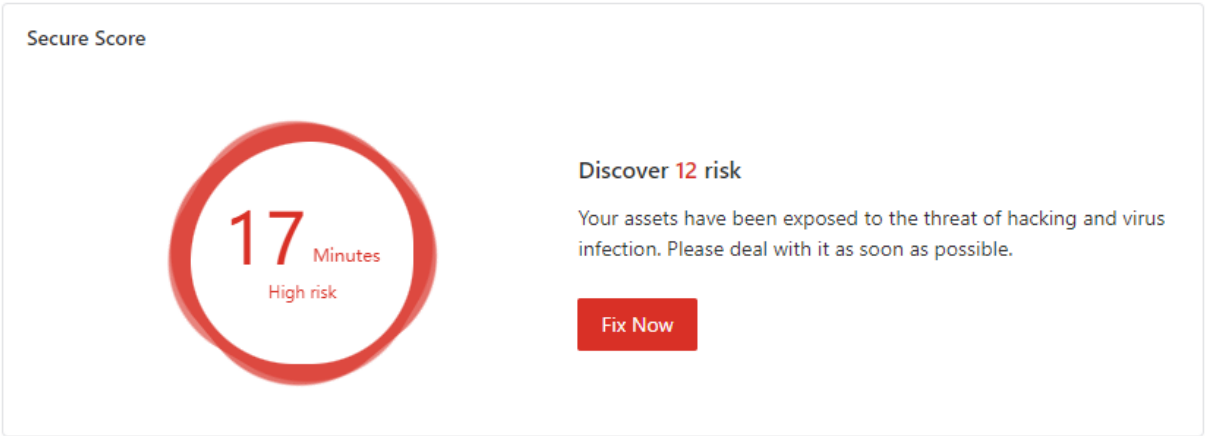
> **Note** The Security Center console automatically displays the new version of the **Overview** tab. If you want to use the old version of the **Overview** tab, you can click **Use Previous Version** in the upper-right corner of the tab. For more information about the old version of the **Overview** tab, see Overview.

On the **Overview** tab of the , you can view the security information of your assets and perform operations based on your business requirements. You can view the following information on the **Overview** tab:

- Security score
- Edition and protection details
- Security risks
- Security operations trend
- Recommended information
- Entry points to Security Center documentation

Security score

The **Secure Score** section displays the security score of your assets and the number of risks that are detected on your assets. For more information about the security score, see Security scores. For more information about how to improve the security score, see Improve the security score of your assets.



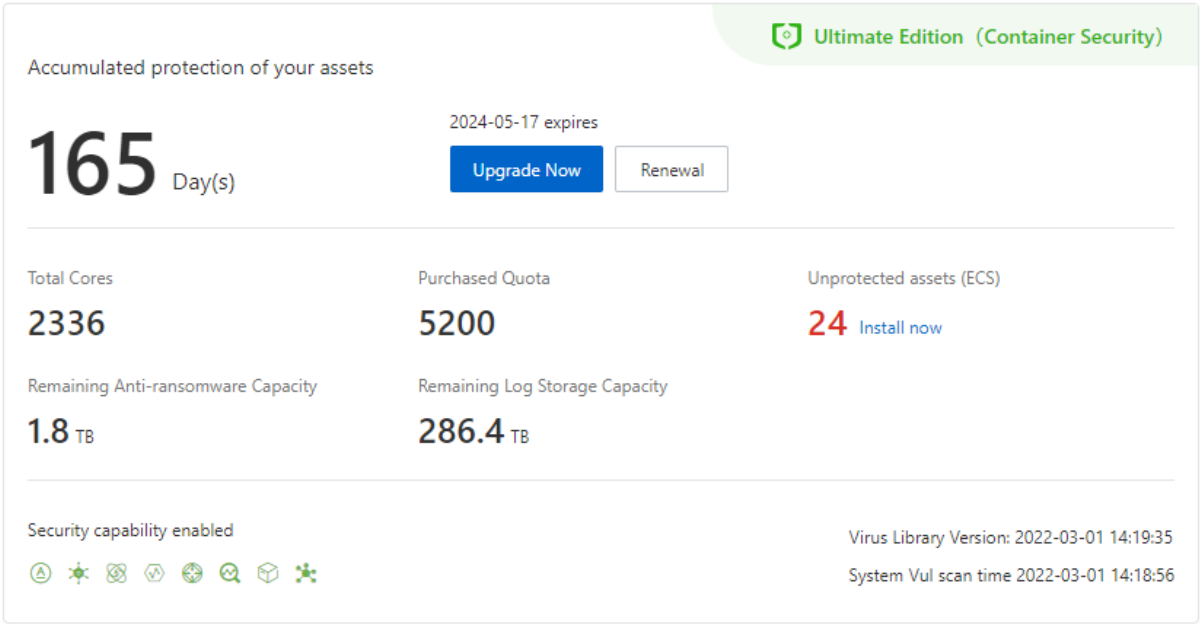
Click **Fix Now** to go to the **Security Risk** panel. In the panel, you can view the penalty point for each risk. If you want to handle a risk, you can click **Process Now** to the right of the risk to go to the page on which you can view the related risk. You can handle the risk based on the risk details or the solutions that are provided on the page.

The Security Risk panel displays the following types of risks that you must handle at the earliest opportunity:

- Risks that must be handled at the earliest opportunity by using the Security Center protection features
- Configuration risks of core features
- Unhandled alerts
- Unfixed vulnerabilities
- Baseline risks
- AccessKey pair leaks
- Configuration risks of cloud services
- Attacks and other types of risks

Edition and protection details

The section in the upper-right corner of the Overview tab displays the Security Center edition that you use, the date on which Security Center expires, and the statistics about your assets. The following statistics are displayed: **Purchased Quota**, **Total Cores**, **Unprotected assets (ECS)**, **Remaining Anti-ransomware Capacity**, **Remaining Log Storage Capacity**, **Security capability enabled**, **Virus Library Version**, and **System Vul scan time**.



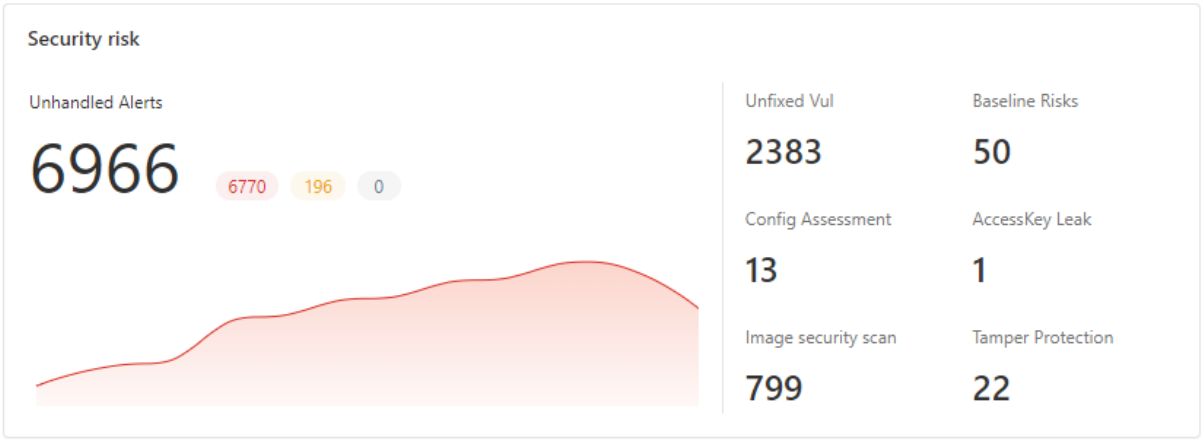
You can perform the following operations in this section:

- **Purchase Security Center**: If you use Security Center and you meet the requirements to apply for a free trial, you can click **Try Now** to start the free trial of Security Center . For more information, see Apply for a free trial of Security Center Ultimate. If you want to continue using Security Center after the trial period ends, you can click **Try Now** to purchase Security Center. For more information about the features that each edition supports, see Features. For more information about how to purchase Security Center, see Purchase Security Center.

- **Upgrade Security Center**: If you use the , , , or edition of Security Center and want to upgrade Security Center or increase the number of protected servers, the quota for cores of servers that you want to protect, or the purchased quota of a value-added feature, you can click **Upgrade Now**. You can also click Upgrade Now to separately purchase value-added features. For more information, see Upgrade and downgrade Security Center.
- **Renew Security Center**: If you use the , Multi-edition, , , , or edition of Security Center and want to renew Security Center before it expires, you can click **Renewal**. For more information, see Renew the subscription to Security Center.
- **Install the Security Center agent**: If you want to install the Security Center agent on unprotected servers, you can click **Install now** below **Unprotected assets (ECS)** to go to the **Agent** tab of the **Settings** page. Then, install the Security Center agent on the servers to protect the servers. For more information, see Install the Security Center agent.
- **Purchase additional capacity**: If the available anti-ransomware capacity or log storage capacity is less than 10%, you can click **Upgrade** to purchase more anti-ransomware capacity or log storage capacity.

Security risks

The **Security risk** section displays the following information: **Unhandled Alerts**, **Unfixed Vul**, **Baseline Risks**, **Config Assessment**, **AccessKey Leak**, **Image security scan**, and **Tamper Protection**.



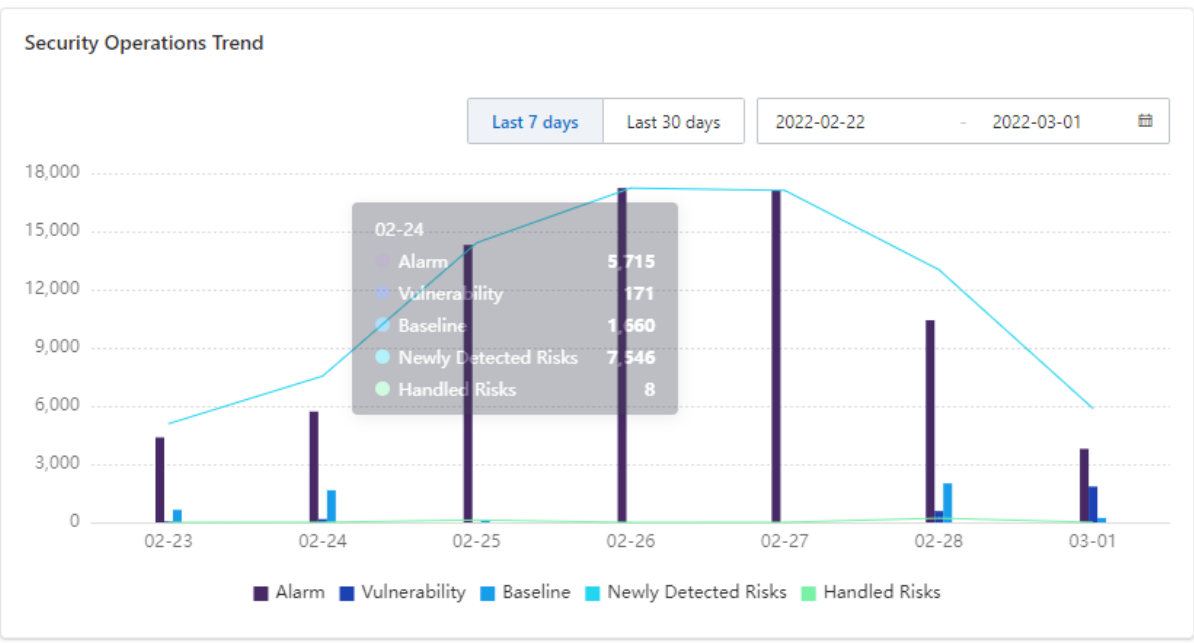
The following table describes the details.

Type	Description
Unhandled Alerts	This section displays the total number of unhandled alerts on your assets and the numbers of alerts at different risk levels. You can click the number below Unhandled Alerts to go to the **Alerts** page to view and handle alerts. For more information, see Handle alerts.
Unfixed Vul	This section displays the total number of unfixed vulnerabilities in your assets. You can click the number below Unfixed Vul to go to the **Vulnerabilities** page to view and handle vulnerabilities. For more information, see Vulnerability fixes.
Baseline Risks	This section displays the number of baseline risks in your assets. You can click the number below Baseline Risks to go to the **Baseline Check** page to view and handle baseline risks. For more information, see Baseline checks.

Type	Description
Config Assessment	This section displays the risks in the baseline configurations of your cloud services. You can click the number below Config Assessment to go to the **Cloud Platform Configuration Assessment** page to view and handle the detected risks in the configurations of your cloud services. For more information, see Overview.
AccessKey Leak	This section displays the total number of unhandled AccessKey pair leaks on your assets. You can click the number below AccessKey Leak to go to the **AK leak detection** page to view and handle AccessKey pair leaks. For more information, see Detection of AccessKey pair leaks.
Image security scan	This section displays the total number of unhandled risks and vulnerabilities in your images. You can click the number below Image security scan to go to the **Image Security** page to view and handle image risks and vulnerabilities. For more information, see Overview.
Tamper Protection	This section displays the total number of tampered web pages in your assets. You can click the number below Tamper Protection to go to the **Tamper Protection** page to view and handle the tampering risks. For more information, see Overview.

Security operations trend

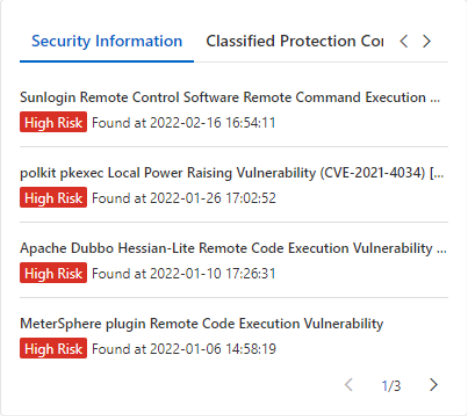
The **Security Operations Trend** section displays the trends of the numbers of alerts, vulnerabilities, and baseline risks within a specific time range in a column chart. The section also displays the trends of the numbers of detected risks and handled risks in the current day in a line chart. Risks that are ignored, fixed, or added to a whitelist are considered handled risks. By default, this section displays the statistics in the last seven days. You can specify a time range or set the time range to Last 30 days.



> **Note** You can click the legends below the chart to show or hide specific statistics.

Recommended information

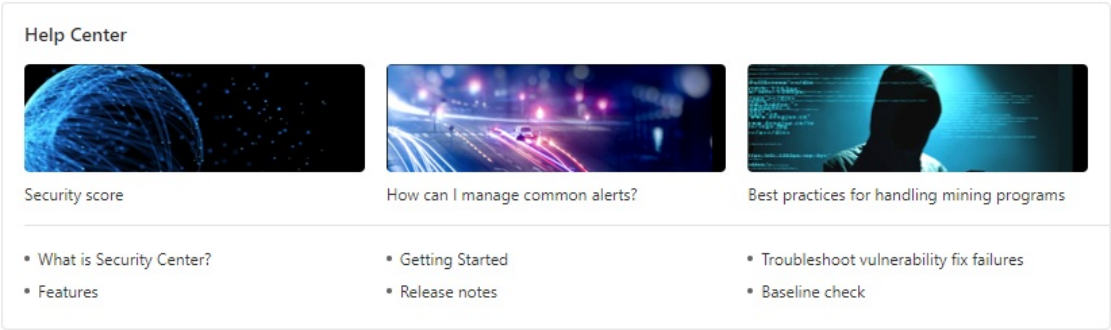
This section displays the most recent security information on the **Security Information** tab. The section also displays the **Security Group**, **Website**, and **Classified Protection Compliance** tabs for you to perform related checks. You are not charged for the checks.



- On the **Security Information** tab, you can view security information such as information about high-risk vulnerabilities that are detected in the last six months.
- On the **Classified Protection Compliance** tab, you can click **Check Now** to go to the **Compliance** page to view the results of classified protection compliance checks and ISO 27001 compliance checks. Security Center provides the feature of classified protection compliance check at no cost to assess the security of your communication networks, compute environments, zone boundaries, management centers, and system construction management. You can use the feature to check whether your system meets the MLPS 2.0 baseline requirements.
- On the **Website** tab, you can click **Check Now** to go the **Website Security Report** page to check your websites for vulnerabilities and risks in website configurations with a few clicks.
- On the **Security Group** tab, you can click **Check Now** to go to the **Policy Assistant** page of the Cloud Firewall console to check your security group configurations for risks with a few clicks.

Entry points to Security Center documentation

The Help Center section provides the entry points to Security Center documentation. The documentation covers the following content: introduction, tutorials, features, alert handling methods, and best practices. You can click a topic title to view the topic.



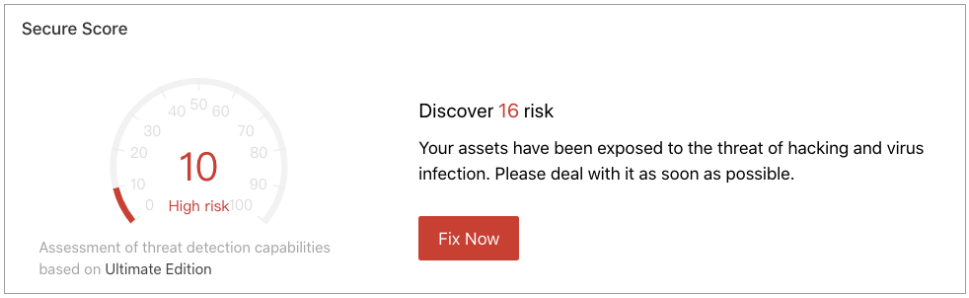
2.Overview

This topic provides a brief introduction to the Overview tab of the Security Center console. The Overview tab is a security operations center for Alibaba Cloud services. The tab dynamically displays the security score, risks that threaten your assets, and the features that you have enabled. The tab also provides you with entry points to upgrade and renew Security Center, and increase related quotas.
On the **Overview** tab of the Security Center consoleSecurity Center console, you can view the overall security information of your assets and perform operations based on your business requirements. You can view the security information in the following sections on the **Overview** tab:

- Security score
- Edition and protection details
- Security defense
- Security risks
- Configuration assessment
- Security operations

Security score

The **Secure Score** section displays the security score of your assets and the number of risks that are detected on your assets. For more information about the security score, see Security scores. For more information about how to improve the security score, see Improve the security score of your assets.

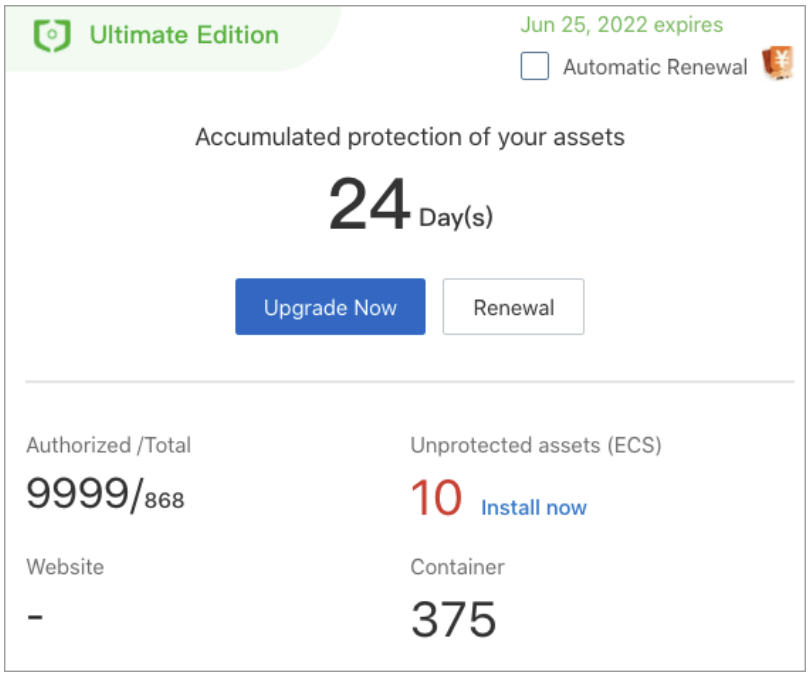


Click **Fix Now** to go to the **Security Risk** panel. In the panel, you can click Help to go to the specific help documentation to handle risks. You can also click Process Now to handle risks. The Security Risk panel displays the following types of risks that you must handle at the earliest opportunity:

- Configurations of core features
- Unhandled alerts
- Unfixed vulnerabilities
- Baseline risks
- AccessKey pair leaks
- Configuration risks in cloud services
- Attacks and other types of risks

Edition and protection details

The section in the upper-right corner of the Overview tab displays the Security Center edition that you use, the date on which Security Center expires, and the statistics on your assets. The statistics include the numbers of websites, containers, and unprotected Elastic Compute Service (ECS) instances within your Alibaba Cloud account. The statistics also include the cores of servers within your Alibaba Cloud account and the purchased quota for cores of servers that you want to protect.

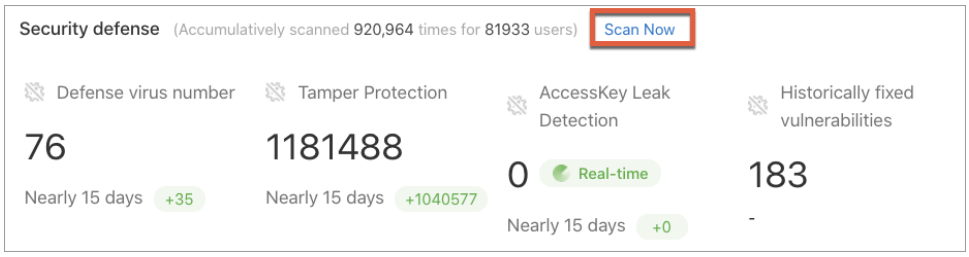


You can perform the following operations in this section:

- **Try Security Center Ultimate**: If you use Security Center and meet the requirements to apply for a free trial, click **Try Now** to start the free trial of Security Center . For more information, see Apply for a free trial of Security Center Ultimate.
- **Purchase Security Center**: If you use Security Center , click **Improve Defense Capabilities** to purchase Security Center. For more information about the features that each edition supports, see Features. For more information about how to purchase Security Center, see Purchase Security Center.
- **Upgrade Security Center**: If you use the , , , or edition of Security Center and want to upgrade Security Center or increase the number of protected servers, the quota for cores of servers that you want to protect, or the purchased quota of a value-added feature, click **Upgrade Now**. You can also click Upgrade Now to separately enable value-added features. For more information, see Upgrade and downgrade Security Center.
- **Renew Security Center**: If you use the , , , , or edition of Security Center and want to renew Security Center before it expires, click **Renewal**. For more information, see Renew the subscription to Security Center.
- **Enable auto-renewal by month**: If you want to use Security Center for a long period of time, select **Automatic Renewal** to enable auto-renewal by month. After you enable auto-renewal by month, the system automatically renews your subscription before Security Center expires. You do not need to manually renew the subscription. If Security Center expires, attacks can pose threats to your business. We recommend that you enable auto-renewal by month to protect your business.
- **Install the Security Center agent on unprotected servers**: Click **Install now** below **Unprotected assets (ECS)** to go to the **Agent** tab of the Settings page. On the tab, you can install the Security Center agent on unprotected servers. This allows Security Center to protect the servers. For more information, see Install the Security Center agent.

Security defense

The **Security defense** section displays the numbers of blocked viruses, detected AccessKey pair leaks, fixed vulnerabilities, and blocked web tampering attempts. The **Security capability enabled** section displays the engines that are enabled to scan assets, the version of the virus library, and the time when the system scans for vulnerabilities. The **Anti-ransomware** section displays the purchased anti-ransomware capacity and its usage information. The **Log analysis** section displays the purchased log storage capacity and its usage information. You can monitor the defense and security status of your assets in real time in these sections.

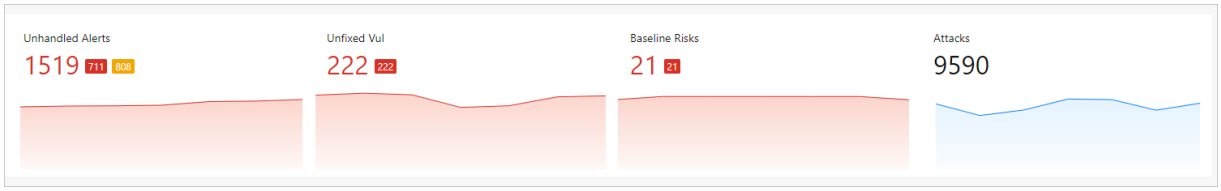


> **Note** **Anti-Virus Version** indicates the version of the virus library. The version is also the update time of the virus library. Security Center dynamically updates the virus library and the characteristics of viruses in the virus library based on the analysis results of specific engines. The engines include lexical analysis engines, virus detection engines, machine learning engines, deep learning engines, big data-based threat detection engines, threat intelligence engines, and abnormal behavior analysis engines. We recommend that you use Security Center to detect vulnerabilities and viruses on a regular basis to protect your servers from the latest viruses. For more information, see Use the quick scan feature and Scan for viruses.

If you want to perform in-depth virus detection on your servers, click **Scan Now** to go to the **Virus Defense** page. For more information about how to scan for viruses, see Scan for viruses.

Security risks

The **Security risk** section displays the statistics on unhandled alerts, unfixed vulnerabilities, baseline risks, and attacks. The following table describes the statistics.

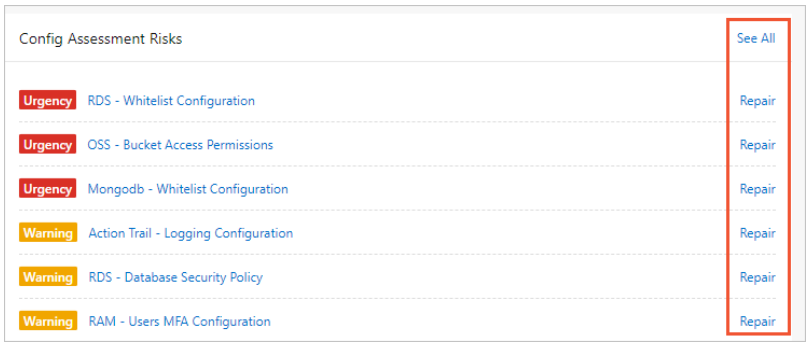


Type	Description
Unhandled Alerts	This section displays the total number of alerts that are generated for your assets and the numbers of alerts at different risk levels. You can click the total number below Unhandled Alerts to go to the **Alerts** page to view and handle alerts. For more information, see Handle alerts.
Unfixed Vul	This section displays the total number of unfixed vulnerabilities and the numbers of vulnerabilities with different priorities. You can click the total number below Unfixed Vul to go to the **Vulnerabilities** page to view and handle vulnerabilities. For more information, see Vulnerability fixes.

Type	Description
Baseline Risks	This section displays the total number of baseline risks in your assets and the numbers of baseline risks at different risk levels. You can click the total number below Baseline Risks to go to the **Baseline Check** page to view and handle baseline risks. For more information, see Baseline checks.
Attacks	This section displays the total number of attacks against your assets. You can click the number below Attacks to go to the **Attack Awareness** page to view attack analysis. For more information, see Attack analysis.

Configuration assessment

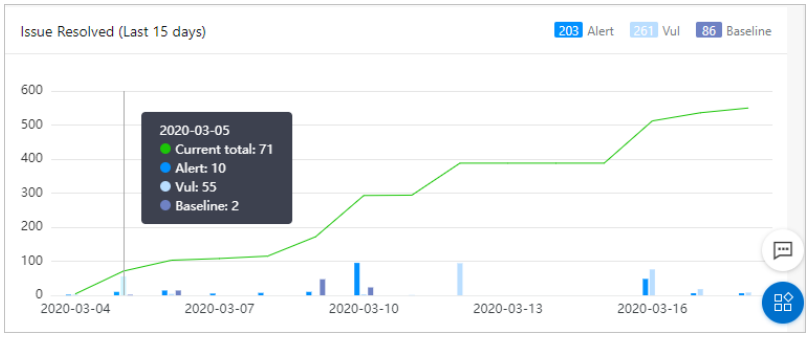
The **Cloud platform configuration check** section displays the risks detected in the baseline configurations of cloud services.



You can click **See All** to go to the **Cloud Platform Configuration Assessment** page to view the check results of configuration assessment for your cloud services and handle the detected configuration risks. For more information, see View the check results of configuration assessment for your cloud services and handle the detected risks.

Security operations

The **Issue Resolved (Last 15 days)** section displays the trends in the numbers of alerts, vulnerabilities, and baseline risks that have been handled in the last 15 days. The statistics are displayed in a column and line chart.



3.Security score

Security Center monitors the security status of your assets in real time, and provides a security score for your assets and the number of detected risks. This topic describes the ranges of scores and deduction items.

Security scores

Security score	Description	Font color
95 to 100	Your assets are secure.	Green
85 to 94	Your assets are exposed to a few of security risks. We recommend that you reinforce the security of your system at the earliest opportunity.	Yellow
70 to 84	Your assets are exposed to a large number of security risks. We recommend that you reinforce the security of your system at the earliest opportunity.	Yellow
69 or lower	Your assets are at high risk. We recommend that you reinforce the security of your system at the earliest opportunity.	Red

Deduction items

Note

- The maximum security score is 100, and the minimum security score is 10.
- If the security score is greater than 60 after penalty points are endorsed but unhandled alerts are detected, the final score is still 60.
- If the security score is greater than 80 after penalty points are endorsed but unhandled alerts or vulnerabilities are detected, the final score is still 80.
- If the security score is greater than 90 after penalty points are endorsed but unhandled baseline risks are detected, the final score is still 90.
- All paid editions in the following table indicate the , , , and editions of Security Center.

Category	Edition	Reduction item	Penalty point	Suggestion
	All paid editions	Web tamper proofing is disabled.	5	Enable web tamper proofing
		No rules are configured to prevent brute-force attacks.	2	Configure IP address blocking policies
		Quick installation of the Security Center agent is not authorized.	2	If this is the first time that you use this feature, obtain the required permissions.

Category	Edition	Reduction item	Penalty point	Suggestion
Configurations of core features	, , and	Configuration assessment is not authorized.	2	If this is the first time that you use this feature, obtain the required permissions.
	All paid editions	Log analysis is disabled.	2	Enable log analysis
	All paid editions	Antivirus is disabled.	2	Use proactive defense
	All paid editions	No anti-ransomware policies are created.	15	创建防护策略
	All paid editions	Periodic virus detection is disabled.	5	Periodic virus scanning
	, , and	Container images that can be scanned are not specified.	5	Configure a cycle to scan for image vulnerabilities
		Kubernetes threat detection is disabled.	5	Use threat detection on Kubernetes containers
Unhandled alerts	All paid editions	Unhandled high-risk alerts are detected.	20	查看和处理告警事件
	All paid editions	Unhandled medium-risk alerts are detected.	20	查看和处理告警事件
	All paid editions	Unhandled low-risk alerts are detected.	20	查看和处理告警事件
Unfixed vulnerabilities	, , and	Unfixed Web-CMS vulnerabilities are detected.	2	View and handle Web-CMS vulnerabilities
	, , and	Unfixed Windows system vulnerabilities are detected.	2	View and handle Windows system vulnerabilities
	, , and	Unfixed Linux software vulnerabilities are detected.	2	View and handle Linux software vulnerabilities
	, , and	Unfixed urgent vulnerabilities are detected.	5	View and handle urgent vulnerabilities
	, , and	Urgent vulnerabilities exist but are not detected. If no Elastic Compute Service (ECS) instances are used, no penalty points are endorsed.	3	View and handle urgent vulnerabilities

Category	Edition	Reduction item	Penalty point	Suggestion
Baseline risks	and	Baseline risks are detected.	1	Manage baseline risks
Configuration risks	, , and	Anti-DDoS Pro and Anti-DDoS Premium fail the back-to-origin configuration check.	• High risk: 2 • Low risk: 1	Manage configuration risks
	, , and	Two-factor authentication is disabled for your Alibaba Cloud account.	• High risk: 2 • Low risk: 1	
	, , and	ApsaraDB RDS fails the security policy check.	• High risk: 2 • Low risk: 1	
	, , and	High risks are detected in cloud service configurations.	2	
	, , and	Low and medium risks are detected in cloud service configurations.	1	
AccessKey pair leaks	All editions	AccessKey pair leaks are detected.	30	View and handle AccessKey pair leaks
Others	and	Attack events are detected.	5	Improve the security score of your assets

References

What are the priorities to handle security events that I can access in the Secure Score section?

The deduction items in the Enterprise and Ultimate editions are different from those in the Basic, Anti-virus, and Advanced editions. What are the differences?

How does the vulnerability scan level affect the security score?

How does the baseline check level affect the security score?

Improve the security score of your assets

4.Container network topology

The feature of container network topology allows you to perform security-related operations on your assets, such as clusters, containers, images, and applications, in a visualized manner. The feature also displays the network topology of your containers. The feature allows you to manage your containers in a more efficient manner. You can use container network topology to obtain the up-to-date security information and network connections of your containers. This topic describes how to view the network topology of running containers.

Prerequisites

The network topology of running containers displays the image vulnerability information that is obtained by using the feature of **container image scan**. If you want to view container risks, you must enable container image scan and scan images. For more information, see Enable container image scan .

> **Note** If you use container network topology and you do not enable container image scan, you can view only the server vulnerabilities and the network topology of the current cluster. You cannot view the container vulnerabilities in the current cluster. To ensure the security of the container runtime environment, we recommend that you enable container image scan.

Context

Security Center automatically refreshes the network topology of running containers and security information about the current cluster on the **Radar** tab at intervals of 1 minute. This ensures that you can view the up-to-date network topology and security information.

Scenarios

Compliance with classified protection requirements

Container network topology displays the network topology of your assets to ensure that your system meets the requirements of classified protection.

Visualization

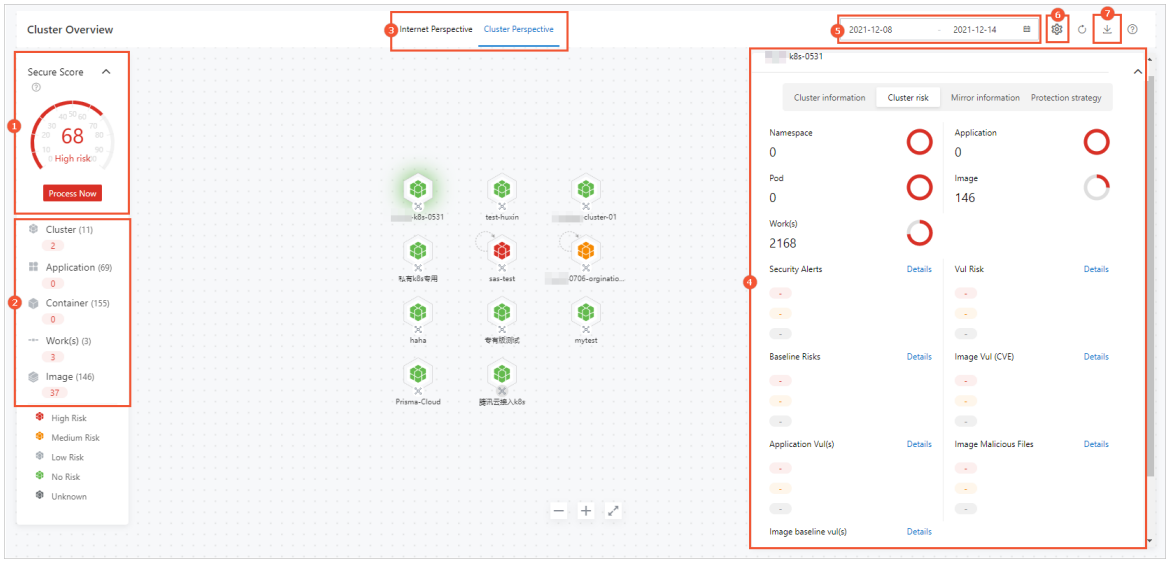
Container network topology automatically displays the ports that are exposed on the Internet. You can perform security-related operations on your assets, such as clusters, containers, images, and applications, in a visualized manner.

Procedure

1.
2.
3.
4. View the network topology of your assets.

   The following figure shows the sections on the **Radar** tab. The following list describes the operations that you can perform in each section.

- View the security score of your assets (marked 1 in the following figure)
- View the total numbers of clusters, applications, containers, nodes, and images, and the numbers of vulnerable clusters, applications, containers, nodes, and images (marked 2 in the following figure)
- View the network topology of a cluster by perspective (marked 3 in the following figure)
- View the details and security information about a cluster (marked 4 in the following figure)
- View the network topology of a cluster in a specified time range (marked 5 in the following figure)
- Turn on or turn off Enable the network topology of all clusters (marked 6 in the following figure)
- Export a container network topology (marked 7 in the following figure)



View the security score of your assets

In the left-side section of the **Radar** tab, you can view the security score of your assets. The security score is calculated based on the security information of your assets. If you want to handle the risks in your assets, you can click **Process Now** to go to the **Security Risk** panel. A higher security score indicates fewer risks in your assets. For more information about the security score, see Security score.

View the total numbers of clusters, applications, containers, nodes, and images, and the numbers of vulnerable clusters, applications, containers, nodes, and images

In the left-side section of the **Radar** tab, you can view the total numbers of **clusters**, **applications**, **containers**, **nodes**, and **images**. You can also view the numbers of vulnerable clusters, applications, containers, nodes, and images. A number in red indicates the number of vulnerable assets. If you want to view the details of a specific type of assets, you can click the asset type to go to the **Assets** page.

View the network topology of a cluster by perspective

On the **Radar** tab, the network topology of a cluster is displayed by perspective. You can view the network topology on the **Internet Perspective** or **Cluster Perspective** tab. In the upper part of the network topology, you can click **Internet Perspective** or **Cluster Perspective** based on your business requirements.

View the details and security information about a cluster

On the **Radar** tab, click the required cluster. In the panel that appears, the information about the cluster is displayed on the following tabs: **Cluster information**, **Cluster risk**, **Mirror information**, and **Protection strategy**.

- **Cluster information**
  On the Cluster information tab, you can view the following basic information about the cluster: **Name**, **ID**, **Cluster Type**, and **Region**. You can also view the numbers of the following items in the cluster: **Namespace**, **Pod**, **Work(s)**, **Application**, and **Image**.
- **Cluster risk**
  On the Cluster risk tab, you can view the following types of risks in the cluster: **Security Alerts**, **Baseline Risks**, **Application Vul(s)**, **Image baseline vul(s)**, **Vul Risk**, **Image Vul (CVE)**, and **Image Malicious Files**. Click **Details** to the right of a risk name. On the details page of the cluster or the vulnerability list of the **Image Security** page, view the details of the detected risks and handle the risks. For more information about how to handle risks, see 查看和处理告警事件,Overview, and View image scan results.
- **Mirror information**
  On the Mirror information tab, you can view the images that belong to the cluster. Find an image whose image repository is not added to Security Center and click **Access Now** on the right. On the **Image Security** page, you can add the image repository to Security Center.
- **Protection strategy**
  On the Protection strategy tab, you can view the following information in the **Defense details** section: **Number of intercepted alarms in the past 7 days**, **Total number of rules**, and **Defensive status**. Click **Create rules** to go to the **Create rules** panel. In the panel, you can create protection rules for the cluster.

View the network topology of a cluster in a specified time range

By default, the **Radar** tab displays the network topology of your cluster traffic in the last seven days. You can use the date picker in the upper-right corner of the **Radar** tab to specify a time range based on your business requirements. This allows you to view the network topology of your cluster within the specified time range. You can specify a time range within the last seven days.

Turn on or turn off Enable the network topology of all clusters

By default, the network topology of all clusters is enabled. After you enable the feature of container network topology, a small amount of CPU resources are consumed. If you do not require the network topology of all clusters, you can click the  icon in the upper-right corner of the **Radar** tab and click the  icon. If you want to view the network topology of all clusters, you can turn on Enable the network topology of all clusters.

> **Note** We recommend that you turn on Enable the network topology of all clusters so that you can obtain the security status of each node in the network topology of all clusters.

Export a container network topology

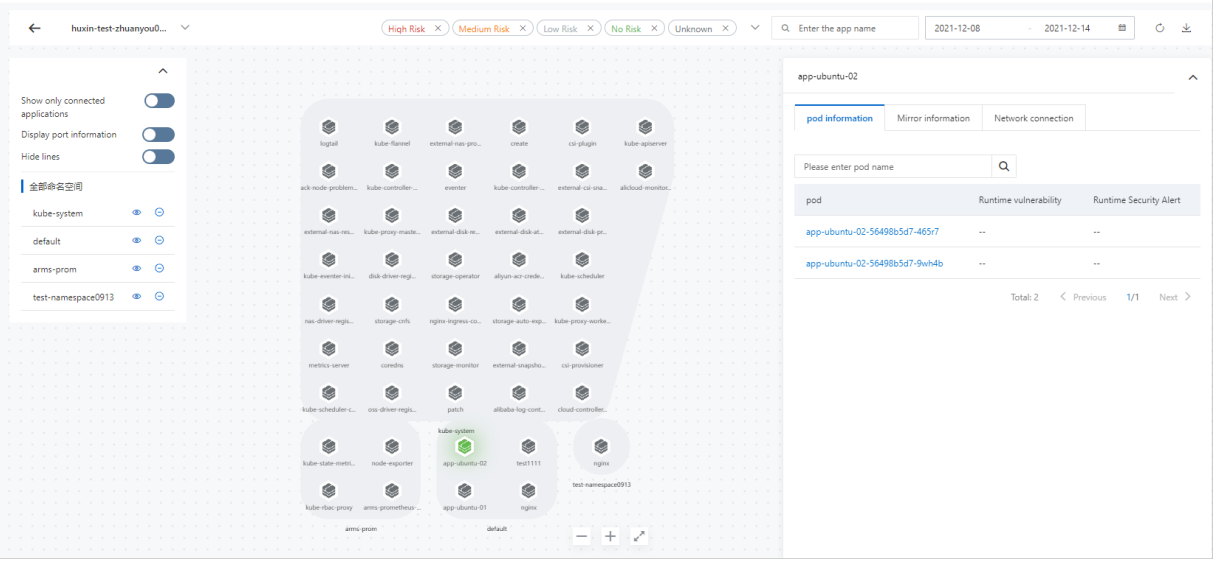
You can click the  icon in the upper-right corner of the **Radar** tab to export a container network topology. The exported network topology is in the PNG format.

View the container network topology of a cluster

You can use one of the following methods to view the container network topology of a cluster:

- On the **Cluster information** tab, click **View** to the right of **Container Network Topology**.
- On the **Radar** tab, click the icon below the cluster.

On the page that displays the network topology of the cluster, an application is a node in the network topology. The network topology displays the communication links among all containers in the cluster.



In the left-side section of the page, you can turn on or turn off **Show only connected applications**, **Display port information**, and **Hide lines** to view the topology information based on your business requirements.

In the left-side section of the page, you can view all namespaces that belong to the cluster. You can click the icon to the right of a namespace to hide or show the namespace. You can also click the icon to the right of a namespace to hide or show the namespace.

> **Note** If a cluster contains a large number of applications, the network topology of the cluster is not displayed by default.

Click an application in the network topology of the cluster and view the following information in the panel that appears: **pod information**, **Mirror information**, and **Network connection**. On the **pod information** tab, move the pointer over the name of a pod, the **pod details** message appears. In the message, click **View assets** to go to the **Assets** page to view the vulnerabilities and alerts of the pod.

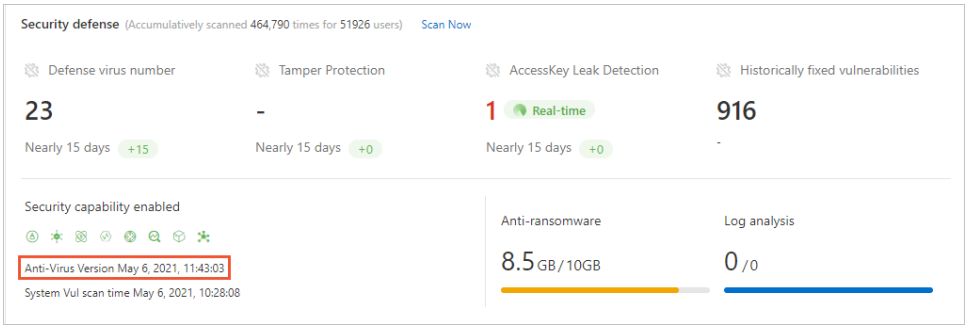
5.FAQ

This topic provides answers to some frequently asked questions about the Overview tab of the Security Center console.

- Virus library
  - How do I view the version of the virus library?
  - After I install the Security Center agent on my Elastic Compute Service (ECS) instances, will the virus library of Security Center be installed on the instances?
- Security score
  - What are the priorities to handle security events that I can access in the Secure Score section?
  - What are the differences of the deduction items in the Advanced edition and in the Enterprise, Ultimate, Basic, and Anti-virus editions?
  - How do I enable the feature of protection against brute-force attacks?
  - How do I handle common alerts?
  - How does the vulnerability scan level affect the security score?
  - How does the baseline check level affect the security score?

How do I view the version of the virus library?

The update time of the virus library that is displayed in the Security Center console indicates the version of the virus library. In the **Security defense** section on the **Overview** tab, you can view the update time of the virus library to the right of **Anti-Virus Version**. Security Center dynamically updates the virus library and the characteristics of viruses in the virus library based on the analysis results of specific engines. The engines include lexical analysis engines, virus detection engines, machine learning engines, deep learning engines, big data-based threat detection engines, threat intelligence engines, and abnormal behavior analysis engines. We recommend that you use Security Center to detect vulnerabilities and viruses on a regular basis to protect your servers from the latest viruses. For more information, see Use the quick scan feature and Scan for viruses.



After I install the Security Center agent on my Elastic Compute Service (ECS) instances, will the virus library of Security Center be installed on the instances?

No,

after you install the Security Center agent on ECS instances, Security Center does not install the virus library on your instances or download the virus library to your instances. The virus library is stored on and is updated by the server of Security Center. The server of Security Center updates the virus library in real time. Security Center checks whether your servers are exposed to viruses based on the virus library.

What are the priorities to handle security events that I can access in the Secure Score section?

The following table describes the priorities to handle security events that you can access in the Security Score section. A smaller number indicates a higher priority. The number 1 indicates the highest priority.

Priority	Event handling
1	Configure or enable core features. • Enable web tamper proofing. • Configure rules to protect against brute-force attacks. • Authorize quick installation of the Security Center agent. • Grant Security Center the permissions to run configuration checks on cloud services. • Enable log analysis. • Enable antivirus. • Create an anti-ransomware policy. • Enable periodic virus detection. • Specify the container images that can be scanned. • Enable Kubernetes threat detection.
2	Handle AccessKey pair leaks.
3	Handle configuration risks in cloud services.
4	Handle baseline risks.
5	Handle security alerts.
6	Fix vulnerabilities.

What are the differences of the deduction items in the Advanced edition and in the Enterprise, Ultimate, Basic, and Anti-virus editions?

The , , and editions of Security Center do not support the attack awareness feature. Therefore, this feature is not covered in the scope of security score. For more information about deduction items, see Deduction items.

How do I enable the feature of protection against brute-force attacks?

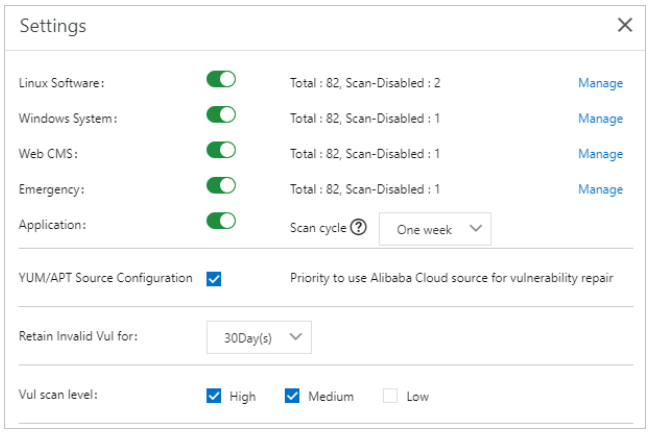
The feature of protection against brute-force attacks blocks malicious IP addresses that attempt to log on to your servers. This improves the security score of your assets. We recommend that you enable this feature. For more information, see FAQ.

How do I handle common alerts?

Security Center allows you to handle alerts detected on your assets. This way, you can reinforce your asset security and increase the security score. For more information, see FAQ.

How does the vulnerability scan level affect the security score?

If you focus only on high- and medium-level vulnerabilities and ignore low-level vulnerabilities, you can exclude the low-level vulnerabilities from the scope of the security score. To exclude low-level vulnerabilities from the scope of the security score, click **Settings** in the upper-right corner of the **Vulnerabilities** page in the Security Center console. In the **Settings** panel, select **High** and **Medium** for **Vul scan level**. Then, Security Center detects only high- and medium-level vulnerabilities.



How does the baseline check level affect the security score?

If you focus only on high- and medium-level baseline checks and ignore low-level baseline checks, you can exclude the low-level baseline checks from the scope of the security score. To exclude low-level baseline checks from the scope of the security score, choose **Baseline Check > Manage Policies** in the Security Center console. In the panel that appears, select **High** and **Medium** in the Baseline level section. Then, Security Center runs only high- and medium-level baseline checks.