

Alibaba Cloud

Security Center Quick Start

Document Version: 20211231

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 .
<code>Courier font</code>	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.Configure common features (simplified) ----- 05

2.Configure best practices tasks ----- 24

1. Configure common features (simplified)

Security Center provides various features to protect your cloud assets and on-premises servers. These features include alert notifications, antivirus, webshell detection, client protection, and container image scan. This topic describes how to configure these features.

Context

The following sections are arranged based on the read habits of users.

After you activate Security Center, we recommend that you enable the following features in sequence:

- [Alert notifications](#)
- [Proactive defense, webshell detection, and client protection](#)
- [Container image scan](#)
- [Configuration assessment](#)
- [Security group check](#)
- [Defense rules against brute-force attacks](#)
- [Web tamper proofing](#)
- [Anti-ransomware](#)

Alert notifications

If Security Center detects exceptions in your assets, it sends alerts based on the severity levels, notification periods, and notification methods that you specify. This allows you to monitor the security of your assets in real time. The notification methods include text messages, emails, internal messages, and DingTalk chat bots. For more information, see [Use the notification feature](#).

1. Log on to the [Security Center console](#).
2. In the left-side navigation pane, click **Settings**. On the page that appears, click the **Notifications** tab. Then, select the notification periods, notification methods, and severity levels for the notification items on which Security Center sends alerts.

Settings

General **Notifications** Agent

Notification Settings You can quickly receive security information through SMS, emails, or internal messages. You can click [configure security message recipients](#).

Item	Notify At	Severity	Notify By
Vulnerabilities Send weekly reports on unhandled vulnerabilities Once every 7 days	8:00-20:00	All	<input type="checkbox"/> SMS <input type="checkbox"/> Email <input checked="" type="checkbox"/> Internal Message
Baseline Risks Send weekly reports on unhandled baseline risks Once every 7 days	8:00-20:00	All	<input type="checkbox"/> SMS <input checked="" type="checkbox"/> Email <input checked="" type="checkbox"/> Internal Message
Alerts Send alerts on security events	<input checked="" type="radio"/> 00:00-24:00 <input type="radio"/> 8:00-20:00	<input checked="" type="checkbox"/> Urgency <input checked="" type="checkbox"/> Warning <input checked="" type="checkbox"/> Reminder	<input checked="" type="checkbox"/> SMS <input checked="" type="checkbox"/> Email <input checked="" type="checkbox"/> Internal Message
AccessKey leakage info When the AccessKey is leaked on GitHub, an alert is triggered. Please pay attention to the alarm information in time.	<input checked="" type="radio"/> 00:00-24:00 <input type="radio"/> 8:00-20:00	All	<input checked="" type="checkbox"/> SMS <input checked="" type="checkbox"/> Email <input checked="" type="checkbox"/> Internal Message
Config Assessment When there is a risk, a notification will be sent. Please pay attention to the alert information.	8:00-20:00	All	<input checked="" type="checkbox"/> SMS <input type="checkbox"/> Email <input type="checkbox"/> Internal Message
Emergency Vul Intelligence The vul operations Lab of the Security Center provides free intelligence of recent and large-scale vuls, helping you respond quickly.	8:00-20:00	All	<input checked="" type="checkbox"/> SMS <input checked="" type="checkbox"/> Email <input checked="" type="checkbox"/> Internal Message
Anti-Tampering of web pages Alerts are sent when the protected web page is tampered with without authorization.	<input checked="" type="radio"/> 00:00-24:00 <input type="radio"/> 8:00-20:00	All	<input checked="" type="checkbox"/> SMS <input type="checkbox"/> Email <input type="checkbox"/> Internal Message

Notification items refer to the threat events and security risks that Security Center detects in your assets. By default, Security Center provides the following notification items: **Vulnerabilities**, **Baseline Risks**, **Alerts**, **AccessKey leakage info**, **Config Assessment**, **Emergency Vul Intelligence**, and **Anti-Tampering of web pages**.

Proactive defense, webshell detection, and client protection

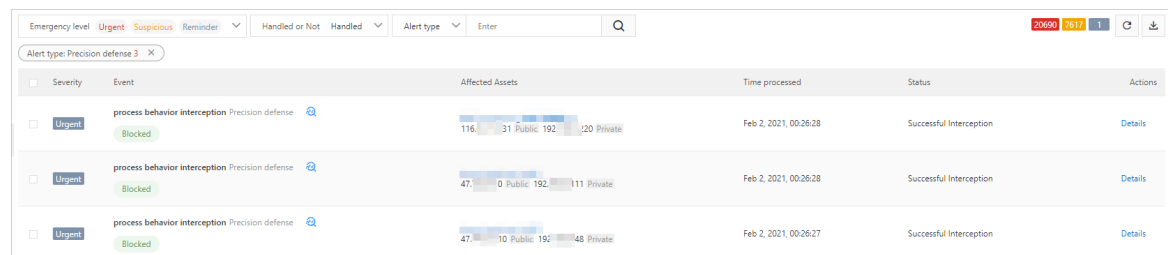
If you want to enable the proactive defense, webshell detection, or client protection feature, go to the Settings page and select the servers for which you want to enable the features.

Note If you do not turn on the switches in the Proactive Defense section, Security Center only detects related threats but does not automatically process detected common viruses or malicious network behavior.

1. Log on to the [Security Center console](#).
2. In the left-side navigation pane, click **Settings**. On the page that appears, turn on or turn off the switches in the Proactive Defense section.

Click **Manage** for **Anti-Virus**, **Anti-ransomware (Bait Capture)**, **Webshell Protection**, and **Behavior prevention** to select the servers for which you want to turn on the switches.

After you enable the proactive defense feature, Security Center automatically quarantines the common viruses or abnormal connections that it detects. If you want to view the quarantined viruses and connections, you can go to the **Alerts** page and filter security events by using the **Precise Defense** type.



Severity	Event	Affected Assets	Time processed	Status	Actions
Urgent	process behavior interception Precision defense Blocked	116 Public 31 Private 192 120 Private	Feb 2, 2021, 00:26:28	Successful Interception	Details
Urgent	process behavior interception Precision defense Blocked	47 Public 0 Private 192 111 Private	Feb 2, 2021, 00:26:28	Successful Interception	Details
Urgent	process behavior interception Precision defense Blocked	47 Public 10 Private 192 48 Private	Feb 2, 2021, 00:26:27	Successful Interception	Details

3. Enable the webshell detection feature.
In the **Webshell Detection** section, click **Manage** to select the servers for which you want to enable the webshell detection feature.
4. Enable the client protection feature.
In the **Client Protection** section, turn on **Defense Mode** and click **Manage** to select the servers for which you want to enable the client protection feature.

Note For more information, see [Overview](#).

Container image scan

The container image scan feature is in public preview. Only the Enterprise and Ultimate editions of Security Center support this feature. If you do not use these editions, you must upgrade Security Center to the Enterprise or Ultimate edition before you can use this feature. For more information about how to purchase and upgrade Security Center, see [Purchase Security Center](#) and [Upgrade and downgrade Security Center](#). For more information about the features that each edition supports, see [功能特性](#).

1. Log on to the [Security Center console](#).

2. In the left-side navigation pane, choose **Precaution > Image Security**.

3. (Optional) Click **Authorize Immediately**.

If this is your first time to use the container image scan feature, you must obtain the required permissions.

4. On the **Image Security** page, click **Scan Now**.

Security Center takes about one minute to perform the scan. After the scan is complete, you can refresh the page to view the scan results.

5. Open the **Image System Vul**, **Image Application Vul**, or **Mirror Malicious Sample** tab to view the detected vulnerabilities or malicious samples.

You can perform the following operations:

- **Search for specific vulnerabilities or malicious samples**

Select a vulnerability severity (high, medium, or low) or a malicious sample severity (urgent, warning, or notice). Alternatively, enter an instance ID, repository name, namespace, or digest to search for a specific vulnerability or malicious sample.

- **View the details of a vulnerability or a malicious sample**

Click the name of a vulnerability or a malicious sample to view its details. On the vulnerability details page, you can view the vulnerability ID, impact score, and vulnerability announcement. On the malicious sample details page, you can view the priority, MD5 value, last scan time, and first scan time. On these details pages, you can also view a list of affected images.

- **View the details of affected images**

Click the name of a vulnerability or a malicious sample. On the vulnerability or malicious sample details page, find the image whose details you want to view and click **Details** in the Operation column. Then, you can view the details of the detected vulnerability or malicious sample.


Configuration assessment

The configuration assessment feature allows you to check for security risks in the configurations of cloud services. Security Center supports both manual and automated checks.

- **Manual checks:** On the **Cloud Platform Configuration Assessment** page, click **Check Now** to detect security risks in the configurations of your cloud services.
- **Automatic checks:** By default, Security Center automatically runs configuration checks during **00:00 - 06:00:00** every two days. You can also customize a detection cycle to periodically check for security risks in the configurations of your cloud services. This helps you detect and handle configuration risks at the earliest opportunity.

Manual check

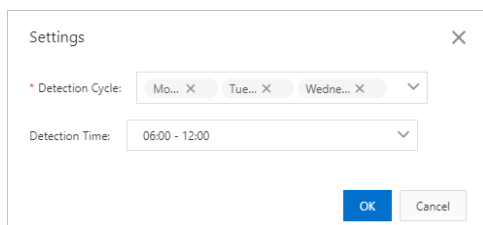
1. Log on to the **Security Center console**.
2. On the **Cloud Platform Configuration Assessment** page, click **Check Now** to detect security risks in the configurations of your cloud services. After you run a check, the number of affected assets appears on this page.

 **Note** Do not perform other operations until the check is complete.

After the check is complete, the results are listed in descending order based on the severity of risks detected.

Automated check

1. Log on to the [Security Center console](#).
2. In the upper-right corner of the **Cloud Platform Configuration Assessment** page, click **Settings**.
3. In the **Settings** dialog box, specify **Detection Cycle** and **Detection Time**.



- **Detection Cycle:** Monday to Sunday. You can select multiple values.
- **Detection Time:** 24:00 - 06:00 , 06:00 - 12:00 , 12:00 -18:00 , and 18:00 - 24:00 . You can select one value.

4. Click **OK**.

During the selected period, Security Center automatically runs checks on all check items.

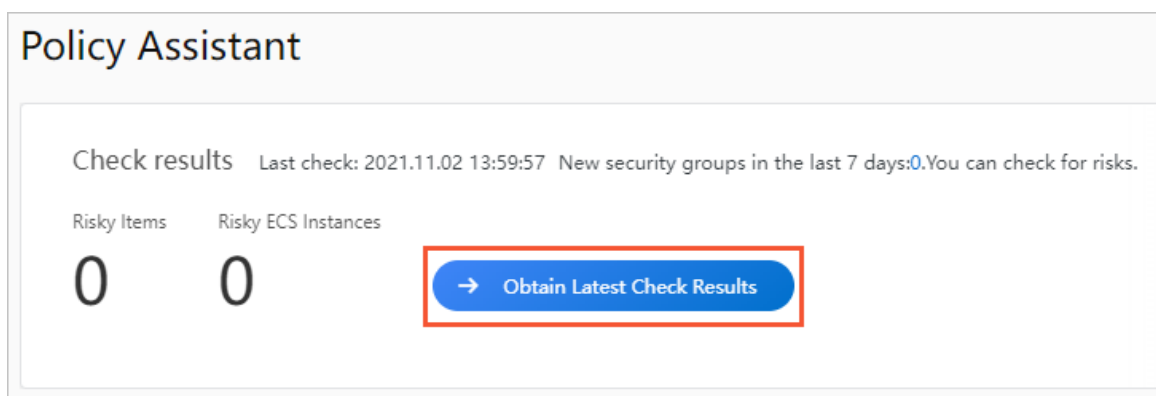
We recommend that you handle the detected security risks in a timely manner. For more information, see [View the check results of configuration assessment for your cloud services and handle the detected risks](#).

Security group check

The security group check feature detects high-risk rules in Elastic Compute Service (ECS) security groups and provides suggestions for fixing. This helps protect your network.

1. Log on to the [Security Center console](#).
2. In the left-side navigation pane, choose **Application market** > **Security group check**.
3. (Optional) On the **Security Check** page, click **Obtain Latest Check Results**.

The check requires 1 to 5 minutes.



Note The latest check results are obtained based on the static analysis of security group rules and may not cover all port risks. You can view complete check results about port exposure on the [Internet Access](#) page. For more information, see [Internet access](#).

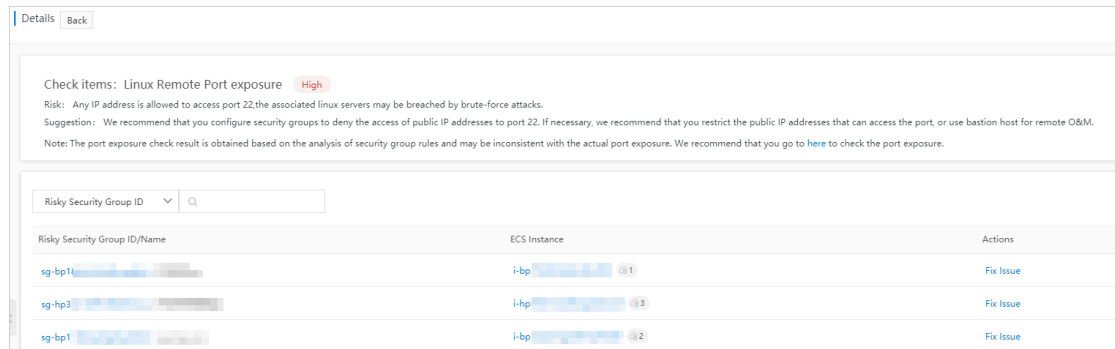
4. Find the required check item and click **View Details** in the **Actions** column. The **Details** page provides suggestions for fixing.

5. Manage weak security group rules.

- i. Find the rule that you want to manage and click **View Details** in the **Actions** column.

Alternatively, click the number in the **Risky Security Groups/Servers** column to go to the **Details** page.

- ii. On the **Details** page, find the security group for which you want to fix an issue and click **Fix Issue** in the **Actions** column.



Improper security group configurations may lead to security incidents. The **Details** page provides a **Suggestion** to manage the security group risk. You can manage the risk based on the **Suggestion**.

If you are using Cloud Firewall Premium, Enterprise, or Ultimate edition, you are redirected to the **Security Groups** page. You must manage security group risks based on the **Suggestion**. For more information, see [Modify security group rules](#). If you are using the Cloud Firewall Basic edition, you must perform substep c.

- iii. (Optional) In the **Cloud Firewall Premium Edition** dialog box, click **Upgrade Now** or **Fix Issue**.

You can use one of the following methods to manage security group risks:

- **Upgrade Now:** You can purchase the Cloud Firewall Premium edition and use the **security group check** function. This function is provided by Cloud Firewall to manage security group risks. We recommend that you select this method. You can use Cloud Firewall to centrally manage security groups and access control policies of public IP addresses. This reduces assets exposure and improves efficiency of security management.
- **Fix Issue:** You can go to the **Security Groups** page to manually manage the risk. For more information, see [Modify security group rules](#).

Defense rules against brute-force attacks

Security Center allows you to configure defense rules to protect your assets against brute-force attacks.

1. Log on to the [Security Center console](#).
2. In the left-side navigation pane, choose **Detection > Alerts**.
3. Click **Settings** in the upper-right corner.
4. In the **Settings** panel, click the **Anti-brute Force Cracking** tab.
5. (Optional) Complete authorization.
 - i. In the **Anti-brute Force Cracking** section, move the pointer over **Management** and click **Authorize**.

ii. Click **Confirm Authorization Policy**.

Note If this is your first time to configure a defense rule against brute-force attacks, you must obtain the required permissions. If you have obtained permissions, skip this step.


6. Click **Management** to the right of **Anti-brute Force Cracking**.7. In the **Add** panel, configure a defense rule.

The screenshot shows the 'Add' panel for configuring a defense rule. The panel has a title bar with 'Add' and a close button. The main content area includes the following sections:


- Defense Rule Name:** A text input field containing 'Alibaba Cloud best practices ag'.
- Defense Rule:** A section with three dropdown menus: '10 Minutes', 'Failures Exceeds', and '80 Times'. To the right of these is a text input field containing 'Disable logon', followed by a dropdown menu set to '6 hours'.
- Select Server(s):** A section with a search bar labeled 'Enter the server name or IP address for query' and a magnifying glass icon. Below the search bar is a list of servers, each with a checkbox and a server name (e.g., 'Default', 'wit', 'de'). A vertical scrollbar is on the right side of the list.
- Set As Default Policy:** A checkbox located at the bottom left of the main content area.

At the bottom of the panel are two buttons: 'Ok' and 'Cancel'. There are also two circular icons on the right side of the panel: a speech bubble icon and a blue icon with a grid pattern.

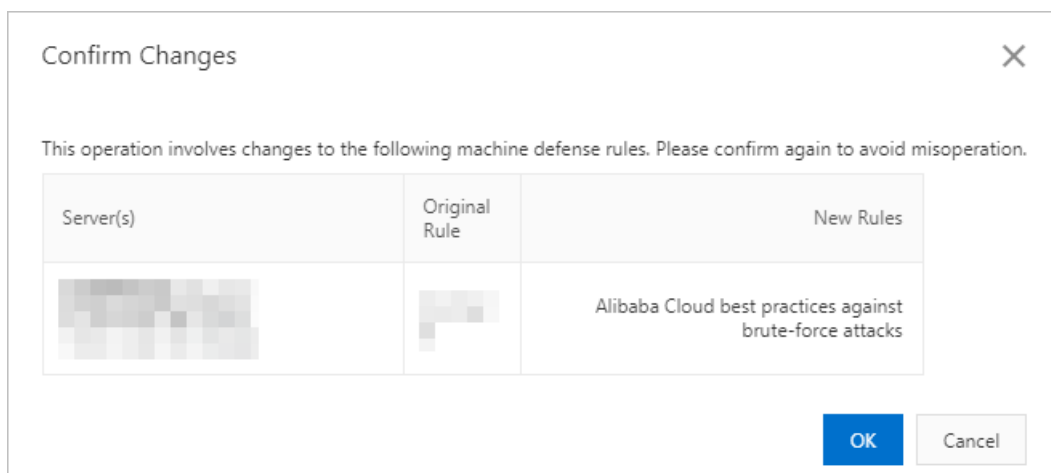
Security Center provides the default defense rule **Alibaba Cloud best practices against brute-force attacks**. The default rule defines that if the number of failed logon attempts exceeds 80 within 10 minutes, the IP address is blocked for six hours. You can use the default rule and select servers to which the default rule applies. You can also configure a custom defense rule. The following table describes the parameters.

Parameter	Description
Defense Rule Name	The name of the defense rule.
Defense Rule	<p>Specifies the defense rule conditions, including the maximum number of failed logon attempts from a specific IP address and the time period during which requests from the IP address are blocked. The maximum number of failed logon attempts can be <i>2, 3, 4, 5, 10, 50, 80, or 100</i>. The time period during which failed logon attempts are counted can be <i>1, 2, 5, 10, or 15 minutes</i>. The time period for blocking the IP address can be <i>5 minutes, 15 minutes, 30 minutes, 1 hour, 2 hours, 6 hours, 12 hours, 24 hours, or 7 days</i>. If you select Permanent, Security Center does not block the IP address.</p> <p>For example, you can configure a custom rule that has the following conditions: If the number of failed logon attempts exceeds <i>three</i> within <i>one minute</i>, the specific IP address is blocked for <i>30 minutes</i>.</p>
Select Server(s)	The servers to which the defense rule applies. You can select servers from the server list, or filter servers by server name or server IP address.
Set As Default Policy	<p>Specifies whether to set the defense rule as the default rule. By default, servers that have no defense rule attached use the default defense rule.</p> <div> <p> Note If you select Set As Default Policy, the defense rule takes effect on all the servers that have no defense rule attached, regardless of whether you select the servers in the Select Server(s) section.</p> </div>

8. Click **OK**.

 **Note** You can configure only one defense rule for each server.

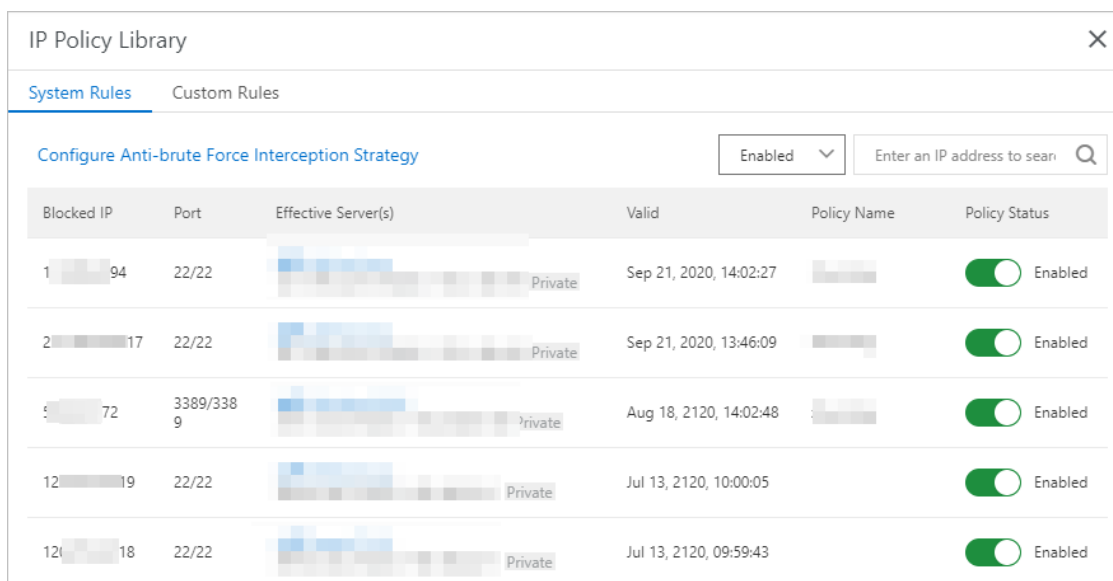
- If a server has an existing defense rule, the **Confirm Changes** dialog box appears. Click **OK**.



- If a server has no defense rule, the configuration of the current defense rule succeeds.
9. In the **IP Policy Library** panel, view the IP blocking rules that Security Center automatically generates.

After you configure a defense rule on the **Anti-brute Force Cracking** tab of the **Settings** panel, the rule triggers IP blocking, and Security Center generates an IP blocking rule. To view the IP blocking rules, perform the following steps:

- i. On the **Alerts** page, click the number below **IP blocking / All**.
If you click the number under **IP blocking**, you are redirected to the page that contains enabled system policies. If you click the number under **All**, you are redirected to the page that contains both enabled and disabled system rules.
- ii. On the **System Rules** tab of the **IP Policy Library** panel, view the IP blocking rules that Security Center automatically generates.



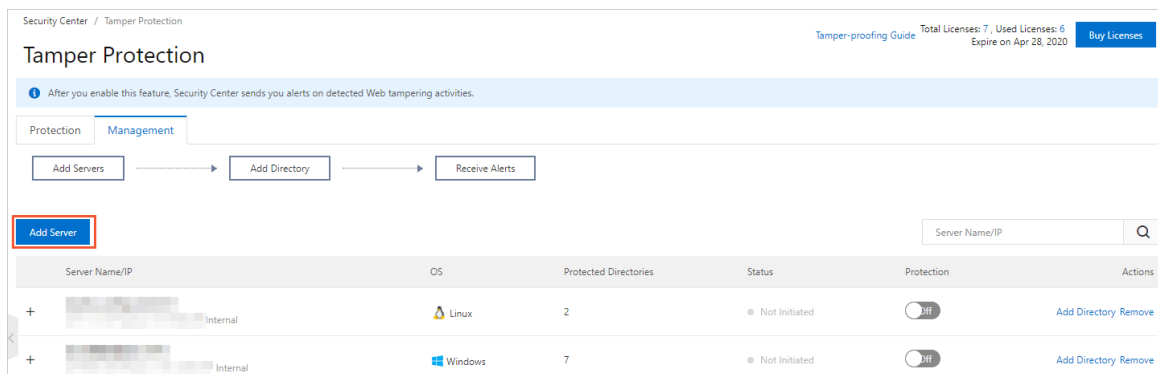
IP Policy Library					
System Rules Custom Rules					
Configure Anti-brute Force Interception Strategy				Enabled	Enter an IP address to search
Blocked IP	Port	Effective Server(s)	Valid	Policy Name	Policy Status
1 94	22/22	Private	Sep 21, 2020, 14:02:27		Enabled
2 17	22/22	Private	Sep 21, 2020, 13:46:09		Enabled
5 72	3389/3389	Private	Aug 18, 2120, 14:02:48		Enabled
12 19	22/22	Private	Jul 13, 2120, 10:00:05		Enabled
12 18	22/22	Private	Jul 13, 2120, 09:59:43		Enabled

For more information about IP blocking rules, see [Configure blocking policies based on IP addresses](#).

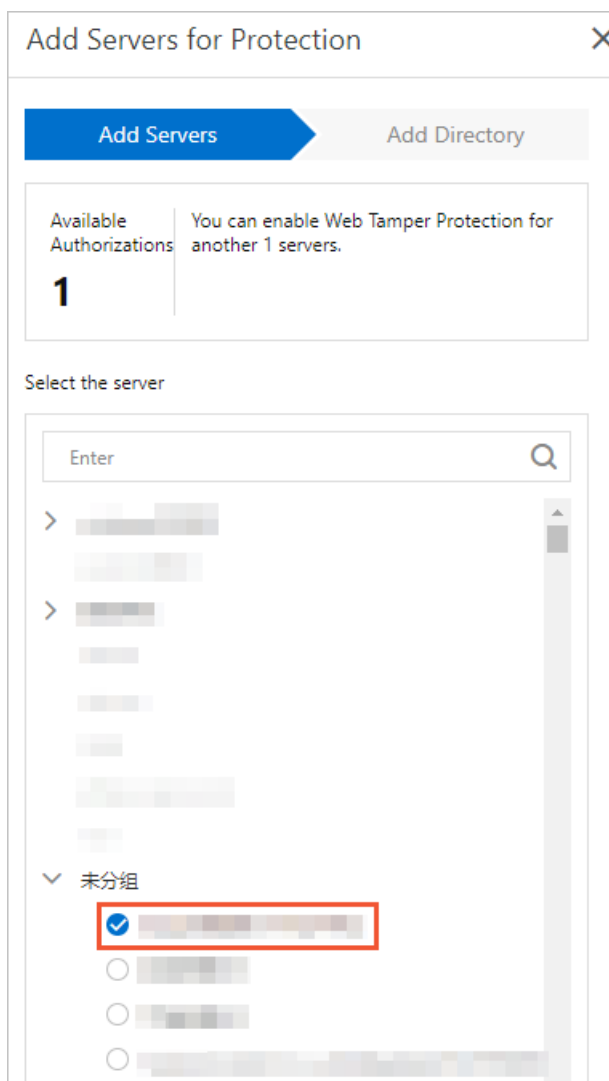
Web tamper proofing

The web tamper proofing feature allows you to monitor web directories in real time. This feature also allows you to restore files or directories that have been tampered with based on the backup files. This protects important website information from being tampered with. Before you can use this feature, you must purchase a specific quota. This quota allows you to enable web tamper proofing for specific servers. For more information, see [Enable web tamper proofing](#).

1. Log on to the [Security Center console](#).
2. In the left-side navigation pane, choose **Defense > Tamper Protection**.
3. On the **Tamper Protection** page, click the **Management** tab.
4. On the **Management** tab, click **Add Server** to enable the web tamper proofing feature for a server.



5. In the Add Servers step of the **Add Servers for Protection** wizard, select a server that you want to protect.



Note

6. Click **Next** to go to the **Add Directory** step.
7. In the **Add Directory** step, configure the parameters.

Add Servers for Protection

Add Servers

Add Directory

We recommend that you use the **whitelist mode**. In this mode, the file formats that usually require protection have been added to the protection list by default. You can add more directories and file formats for protection.[Blacklist Mode >](#)

* Protected Directory

Enter or select the directory to be protected. the directory curre

* Protected File Formats

php X

jsp X

asp X

aspx X

js X

cgi X

html X

htm X

xml X

shtml X

shtm X

jpg X

gif X

png X

* Local Backup Directory

Enable Protection

Cancel

Select a protection mode. You can select **Whitelist Mode** or **Blacklist Mode**. In whitelist mode, this feature is enabled for the specified directory and file formats. In blacklist mode, this feature is enabled for the subdirectories, file formats, and files that are not excluded. By default, the whitelist mode is used.

o Whitelist mode

Parameter	Description
Protected Directory	<div>Enter the path of the directory that you want to protect.</div> <div> Note Servers that run Linux and Windows operating systems use different path formats. Enter the correct directory path based on your operating system.</div>
Protected File Formats	Select file formats that you want to protect from the drop-down list, such as <i>js</i> , <i>html</i> , <i>xml</i> , and <i>jpg</i> .


Parameter	Description
Local Backup Directory	<p>The default path where the backup files of the protected directory are stored.</p> <p>By default, Security Center assigns <code>/usr/local/aegis/bak</code> as the backup path for servers that run Linux operating systems and <code>C:\Program Files (x86)\Alibaba\Aegis\bak</code> for servers that run Windows operating systems. You can modify the default path as needed.</p>

o **Blacklist mode**

Parameter	Description
Protected Directory	Enter the path of the directory that you want to protect.
Excluded Sub-Directories	<p>Enter the path of the subdirectory for which you do not need to enable this feature.</p> <p>You can click Add Sub-Directory to add multiple subdirectories.</p> <p>The files under the excluded subdirectories are not protected by Security Center.</p>
Excluded File Formats	<p>Select the formats of files for which you do not need to enable this feature.</p> <p>Valid values: log, txt, and ldb.</p> <p>The files of the specified formats are not protected by Security Center.</p>
Excluded Files	<p>Enter the path of the file for which you do not need to enable this feature.</p> <p>You can click Add File to add multiple paths.</p> <p>The files in the specified paths are not protected by Security Center.</p>
Local Backup Directory	<p>The default path where the backup files of the protected directory are stored.</p> <p>By default, Security Center assigns <code>/usr/local/aegis/bak</code> as the backup path for servers that run Linux operating systems and <code>C:\Program Files (x86)\Alibaba\Aegis\bak</code> for servers that run Windows operating systems. You can modify the default path as needed.</p>

8. Click **Enable Protection**.

After you enable this feature for a server, the server is displayed in the server list on the Management tab of the **Tamper Protection** page.

 **Note** By default, **Protection** is turned off for the new server. To use the web tamper proofing feature, you must turn on **Protection** of the server on the Management tab of the **Tamper Protection** page.

Security Center / Tamper Protection

Tamper-proofing Guide Total Licenses: 7, Used Licenses: 6 Buy Licenses

After you enable this feature, Security Center sends you alerts on detected Web tampering activities.

Protection Management

Add Servers Add Directory Receive Alerts

Add Server

Server Name/IP OS Protected Directories Status Protection Actions

Server Name/IP	OS	Protected Directories	Status	Protection	Actions
+ [Redacted]	Linux	2	Not Initiated	Off	Add Directory Remove
+ [Redacted]	Windows	7	Not Initiated	Off	Add Directory Remove

9. In the server list, turn on **Protection** to enable this feature for the new server.

Security Center / Tamper Protection

Tamper-proofing Guide Total Licenses: 7, Used Licenses: 7 Buy Licenses

After you enable this feature, Security Center sends you alerts on detected Web tampering activities.

Protection Management

Add Servers Add Directory Receive Alerts

Add Server

Server Name/IP OS Protected Directories Status Protection Actions

Server Name/IP	OS	Protected Directories	Status	Protection	Actions
+ [Redacted] Internal	Linux	2	Running	On	Add Directory Remove
+ [Redacted] Internal	Windows	7	Not Initiated	Off	Add Directory Remove

Note By default, **Protection** is turned off for the new server. To use the web tamper proofing feature, you must turn on **Protection** of the server on the **Management** tab of the **Tamper Protection** page.

If this is the first time you enable this feature for a server, the status of the server is **Initializing**, and a progress bar appears. It requires a few seconds to enable this feature. After this feature is enabled, the status changes to **Running**.

Server Name/IP	OS	Protected Directories	Status	Protection	Actions
+ [Redacted]	Windows	8	Running	On	Add Directory Remove
+ [Redacted]	Linux	10	Not Initiated	Off	Add Directory Remove
+ [Redacted]	Linux	3	Initializing 0%	On	Add Directory Remove
+ [Redacted]	Linux	1	Not Initiated	Off	Add Directory Remove

If the status of a server is **Exception**, move the pointer over **Exception** in the **Status** column. A message that indicates the causes appears. Click **Retry** in the message. For more information, see .

Server Name/IP	OS	Protected Directories	Status	Protection	Actions
+ [Redacted]	Linux	1	Running	On	Add Directory Remove
+ [Redacted]	Windows	8	Exception	On	Add Directory Remove
+ [Redacted]	Windows	9	Exception	On	Add Directory Remove

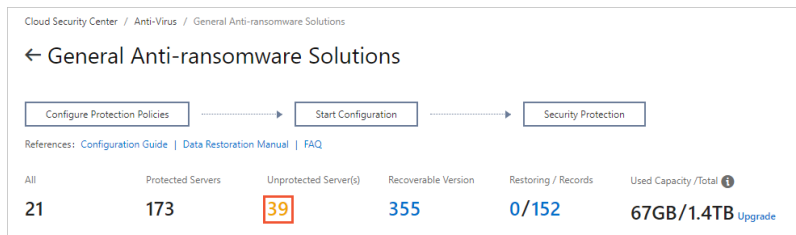
Maximum number of protected directories reached, or the backup space is insufficient. Retry

Anti-ransomware

Security Center provides protection, alerting, and data backup capabilities that prevent ransomware from compromising your servers. Before you can use this feature, you must purchase a specific quota. This quota allows you to enable anti-ransomware for specific servers. For more information, see [开通服务](#).

1. Log on to the [Security Center console](#).
2. In the left-side navigation pane, choose **Defense > Anti-ransomware**.
3. On the **General Anti-ransomware Solutions** page, click **Authorize Now**.
4. On the **General Anti-ransomware Solutions** page, click **Create Policies**.

You can also click the number below **Unprotected Server(s)** to go to the **Create Policies** panel.



5. In the **Create Policies** panel, configure the parameters.

Create Policies

* Policy Name:

Enter a policy name.

* Select Assets:

Asset Group

☐ All Groups (182)

☐

☐

☐

☐

☐

☐

☐


☐

☐

☐

Assets 0 total 0

Search by asset name



No Data

* Protection Policies:

☒ Recommendation Policy ☐ Custom policy

Protected Directories: All Directories (excluding system directories)

Protected File Types: All File Types

Start Time: 00:18:00

Backup policy execution interval: One Day

Backup data retention period: Seven Days


Backup Network Bandwidth Limit(MByte/s): 5MB


OK

Cancel




The following table describes the parameters.


Parameter	Description
Policy Name	The name of the protection policy.

Parameter	Description
Select Assets	<p>The assets that you want to protect. You can select an asset, an asset group, or multiple assets from asset groups. To select the assets to which you want to apply the protection policy, perform the following operations as needed:</p> <ul style="list-style-type: none"> ◦ In the Asset Group section, select an asset group. The system automatically selects all assets in the group. You can clear assets that no longer require protection in the Assets section. ◦ In the Assets section, enter an asset name in the search box to search for the specific asset. Fuzzy match is supported. <div> <p> Note</p> <ul style="list-style-type: none"> ◦ ◦ ◦ The anti-ransomware data backup feature is available in the following regions: China (Chengdu), China East 2 Finance, China North 2 Ali Gov, China (Shanghai), China (Hangzhou), China (Beijing), China (Shenzhen), China (Zhangjiakou), China (Hohhot), China (Qingdao), China (Hong Kong), Singapore (Singapore), Indonesia (Jakarta), Australia (Sydney), US (Silicon Valley), US (Virginia), Germany (Frankfurt), Japan (Tokyo), and India (Mumbai). This feature is not supported in other regions. You can select only ECS instances that reside in the supported regions. </div>
Protection Policies	<p>Valid values:</p> <ul style="list-style-type: none"> ◦ Recommendation Policy <p>If you select Recommendation Policy, the following parameter settings are used by default:</p> <ul style="list-style-type: none"> ■ Protected Directories: All Directories (excluding system directories) ■ Protected File Types: All File Types ■ Start Time: a point in time within the range of 00:00:00 to 03:00:00 ■ Backup policy execution interval: One Day ■ Backup data retention period: Seven Days ■ Backup Network Bandwidth Limit(MByte/s): 5MB ◦ Custom policy <p>If you select Custom policy, you must configure the following parameters: Protected Directories, Protected File Types, Start Time, Backup policy execution interval, Backup data retention period, and Backup Network Bandwidth Limit(MByte/s).</p>

Parameter	Description
Protected Directories	<p>The directories that you want to protect. Valid values:</p> <ul style="list-style-type: none">◦ Specified directory: Only specified directories of the specific assets are protected. Enter the addresses of the specified directories in the Directory address field.◦ All directories: All directories of the specific assets are protected. You must set Whether to exclude system directories. <div> Note If you select All directories, we recommend that you select Excluded for Whether to exclude system directories. This prevents system conflicts.</div>

Parameter	Description
Whether to exclude system directories	<p>Valid values: Excluded and Not Excluded. If you select Excluded, the following directories in Windows and Linux operating systems are excluded:</p> <ul style="list-style-type: none">◦ Windows:<ul style="list-style-type: none">▪ Windows\▪ python27\▪ Program Files (x86)\▪ Program Files\▪ ProgramData\▪ Boot\▪ \$RECYCLE.BIN\▪ System Volume Information\▪ Users\Administrator\NTUSER.DAT▪ pagefile.sys◦ Linux:<ul style="list-style-type: none">▪ /bin/▪ /usr/bin/▪ /sbin/▪ /boot/▪ /proc/▪ /sys/▪ /srv/▪ /lib/▪ /selinux/▪ /usr/sbin/▪ /run/▪ /lib32/▪ /lib64/▪ /lost+found/▪ /var/lib/kubelet/

Parameter	Description
Directory address	<p>The address of the directory that you want to protect. If you want to protect more than one directory, click Add to add more directory addresses. If you want to delete a directory address, click Delete.</p> <div><p> Note</p><ul style="list-style-type: none">You must set this parameter only when you select Specified directory for Protected Directories.</div>
Protected File Types	<p>The file types that you want to protect. Valid values:</p> <ul style="list-style-type: none">Specify file type: Only the files of the specified types are protected. You must select a file type from the Select file type drop-down list.All File Types: All files are protected.
Select file type	<p>Valid values:</p> <ul style="list-style-type: none">DocumentPictureCompressedDatabaseAudio and videoScript code <div><p> Note</p><ul style="list-style-type: none">You must set this parameter only when you select Specify file type for Protected File Types.You can select multiple file types. Security Center protects only the files of the selected file types.</div>
Start Time	<p>The time at which you want to start a data backup task. Data backup may consume a small number of CPU and memory resources. We recommend that you set this parameter to a point in time during off-peak hours, such as 00:00:00.</p> <div><p> Note</p></div>





Parameter	Description
Backup policy execution interval	<p>The time interval between two data backup tasks. Default value: One Day. Valid values:</p> <ul style="list-style-type: none"> ◦ Half a day ◦ One Day ◦ Three days ◦ Seven Days
Backup data retention period	<p>The retention period of backup data. Default value: 7 Days. Valid values:</p> <ul style="list-style-type: none"> ◦ 7 Days ◦ 30 Days ◦ Half a year ◦ One year ◦ Permanent
Backup Network Bandwidth Limit (MByte/s)	<p>The maximum bandwidth that can be consumed by a data backup task. Valid values: 1 Mbit/s to unlimited.</p> <div> <p> Note We recommend that you configure an appropriate bandwidth threshold based on the bandwidth of your server. This prevents the backup tasks from using an excessive amount of bandwidth and ensures business stability.</p> </div>

6. Click **OK**.

After you create and enable a protection policy, Security Center installs the anti-ransomware client on your ECS instance. Then, Security Center backs up data in the protected directories of your ECS instance based on the backup settings that you specified in the protection policy.

7. Enable a protection policy in the policy list.

After you create a protection policy, you must enable it in the policy list. Then, Security Center backs up server files based on the file directories that you specify in the policy.

Protection Policies	Prevention Mode	Server	Policy Status	Status	Actions
+ 	All directories	1		Exception	Edit Delete
+ 	Specified directory	1		Exception	Edit Delete


2. Configure best practices tasks

If you have activated the 7-day free trial of Security Center Ultimate, you can configure the best practices tasks free of charge. This way, you can increase the security score of your assets. After you activate the free trial, we recommend that you immediately configure the best practices tasks to make full use of the free resources. This way, Security Center can comprehensively detect risks on your assets and handle the detected risks.


Prerequisites

The free trial of the Ultimate edition is activated. For more information about how to activate the free trial of the Ultimate edition, see [Apply for a free trial of Security Center Ultimate](#).

Procedure

1. Log on to the [Security Center console](#).
2. In the lower-right corner, click the  icon.
3. On the page that appears, configure the tasks in sequence.

After you configure the tasks, you are offered rewards. For example, you can extend the duration of the free trial of the Ultimate edition or receive coupons to purchase Alibaba Cloud services.

 **Note** After you configure the tasks, the security score of your assets increases. We recommend that you configure tasks at the earliest opportunity. For more information, see [Security score](#).