Alibaba Cloud
Threat Detection

Pricing

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 due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
⛔	This warning information 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.
⚠️	This warning information 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 restore business.
📋	This indicates warning information, supplementary instructions, and other content that the user must understand.	ⓘ Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	📋 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d  C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae  log  list --` `instanceid` *`Instance_ID`*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *`[-all|-t]`*

Style	Description	Example
{} or {a|b}	**It indicates that it is a required value, and only one item can be selected.**	`swich` *{stand | slave}*

Contents

1 Billing method

Security Center Advanced and Enterprise Edition are billed by month or annual subscription.

Billing period

You are billed for the validity period specified in your subscription.

Bill calculation

Bill= (Number of billable assets * Price of protecting one server for validity period + Price of value-added functions * Number/Volumn of the value-added functions) * Validity period of subscription.

· Number of assets: Refers to the number of billable assets that require Security Center's protection, including ECS instances and external servers. The default Number of assets is the number of ECS instances you own, and the number of assets that you specify cannot be less than the number of your ECS instances.

· Value-added functions: The value-added functions provided by Security Center must be additionally purchased, such as Log Analysis service .

· Price of protecting one server: You could check the detailed price of protecting one server and the value-added functions on Security Center purchase page.

> Note:
> Security Center also protects assets such as SLB and NAT gateways. However, Security Center only charges for protecting your ECS instances and external servers. All other assets are currently protected free of charge.

Fee for Server protection (without value-added functions)

Version of Security Center	Price of protecting one server for validity period
Basic	Free of charge
Advanced	9.5 USD/Server/month
Enterprise	23.5 USD/Server/month

Fee for Value-added functions

Value-added functions are available for Advanced and Enterprise editions.

Value-added functions	Price
Web Guard	142.6 USD/Sever/month
Log Analysis	72.9 USD/T/month

Details on how to purchase Security Center, refer to Purchase Security Center.

Related documents

#unique_4

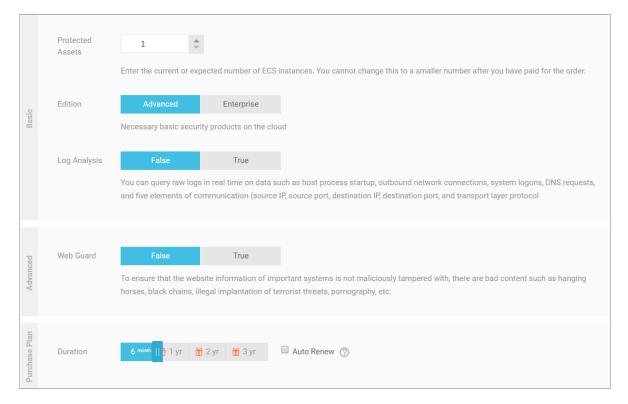#unique_5

2 Purchase Security Center

Security Center Advanced and Enterprise Edition provide comprehensive security monitoring and diagnosis services for your assets on the cloud. You can purchase Advanced and Enterprise Edition by Subscription.

Context

Before you start, refer to #unique_7 to check the features provided by different Editions.

Procedure

1. Log on to your Alibaba Cloud account, and go to the Security Center purchase page.

2. Configure your required Security Center.

- Protected Assets: The number of assets (ECS instances and external servers) needs to be protected by Security Center. By default, the purchase page displays the number of ECS instances you have. You cannot specify a number that is less than the default number.

> 📋 Note:

> If you predict that your number of servers may increase within the validity period of your subscription, specify the predicted number of servers you will need Security Center to protect in your total number of assets.

- Edition: Advanced Edition is selected by default. For more information on the differences between Advanced Edition and Enterprise Edition, refer to Security Center features.
- Log Analysis: Log Analysis is the value-added service of Security Center. Backtracing and security analysis are provided for ten types of security logs, such as server logs and network logs.
- Web Guard: Web Guard is the value-added service of Security Center. It can ensure your website is not maliciously tampered with illegal information, such as terrorist threats, gambling, etc.

3. Select a Duration and select Auto-renew if you want to enable automatic renewal.

> Note:
>
> - The minimum subscription duration is determined by the number of assets you want to protect:
>
>   - If you have less than 10 assets, you must purchase at least a six-month subscription.
>   - If you have more than 10 assets, you must purchase at least a one-month subscription.
> - If you enable Auto-renew, the automatic renewal cycle is aligned with the validity duration of your subscription. For example, if your subscription is monthly, the automatic renewal cycle is one month. If your subscription is yearly, the automatic renewal cycle is one year.

4. Click Buy Now and complete payment.

3 Renewal and upgrade

If you are using Advanced or Enterprise Edition of Security Center, we recommend that you renew your Security Center subscription before its expiration date to ensure the availability of the service. If the number of assets under your account is 120% of the number of assets configured for your current subscription, you must upgrade your subscription by specifying the larger number of assets and pay the additional fees to continue with your current subscription.

Expiration

One week before your Security Center subscription expires, Security Center sends you a message reminding you to renew your subscription. If you do not renew your subscription before it expires, your assets are no longer protected by Security Center starting from the first day after the expiration date.

For three days after the expiration date, Security Center retains all your configurat ions and data, such as your asset groups, tags, quarantined files, vulnerability whitelist, baseline check policies and baseline check whitelist, and asset fingerprin ts. You must renew your Security Center subscription within the three days to retain your configurations and data.

If you do not renew your subscription within three days of your Security Center subscription expiration date, your Security Center configurations and data are removed. You must purchase a new Security Center Advanced or Enterprise Edition subscription to resume use of Security Center.

Renew Security Center Enterprise Edition

1. Log on to the Security Center console.

2. In the upper-right corner, click Renew.

3. Confirm your order details and select your required validity .

   > 📋 Note:
   > You cannot change the number of assets to be protected by Security Center during a subscription renewal.

4. Click Pay Now and complete payment.

Upgrade

When upgrading your Security Center subscription, you must specify at least the actual number of billable assets, that is, the total number of ECS instances and external servers under your account. You cannot specify a number that is less than that. If you predict that the number of billable assets may increase within the validity period of your subscription, you must specify the predicted number of servers you will need Security Center to protect as your total number of assets.

During the subscription period of your Security Center Enterprise Edition, if the number of servers under your account is more than 120% of the number of assets configured for your current subscription, the system notifies you of an upgrade required to your Security Center subscription. If this occurs, you must upgrade your Security Center subscription to continue using the service.

For example, if the number of assets configured for your Security Center Enterprise Edition subscription is 10, but you now have 13 servers under your account, you must configure the number of assets as 13 and pay the additional fees generated for the three extra servers to continue using Security Center.

Upgrade Security Center

1. Log on to the Security Center console.
2. In the upper-right corner of the Overview page, click Upgrade.

   > **Note:**
   >
   > The Upgrade button only displays on the Overview page when the number of billable assets under your account is 120% of the number of billable assets configured for your current subscription.

3. Specify the number of assets that you want Security Center to protect, and click Pay Now.
4. Complete payment.