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 disseminat ed 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, adjustment s, 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 intellectu al 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.	📋 **Note:** 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]`*
{} 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

Threat Detection Service (TDS) Enterprise Edition is billed by month and annual Subscription.

Billing method

Subscription.

Billing period

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

Bill calculation

(Number of assets * Price of protecting one server + Value-added functions) * Validity period of subscription

- **Number of assets**: Refers to the number of billable assets that require TDS'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 TDS must be additionally purchased, such as Log service.

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

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

Details on how to purchase TDS, refer to *Purchase Threat Detection Service*.

2 Purchase Threat Detection Service

Threat Detection Service (TDS) Enterprise Edition provides comprehensive security monitoring and diagnosis services for your assets on the cloud. You can purchase TDS Enterprise Edition by Subscription.

Context

To purchase TDS Enterprise Edition, follow these steps:

Procedure

1. Log on to your Alibaba Cloud account, and go to the *Threat Detection Service purchase page*.

2. Configure your required TDS. The configurations are described as follows:

   - **Assets**: The number of assets (ECS instances and external servers) to be protected. By default, the purchase page displays the number of your ECS instances. You cannot specify a number that is less than the default number.

     > 📋 **Note:**
     >
     > If you predict that the number of your servers may increase within the validity period of your subscription, specify the predicted number of servers you will need TDS to protect as your total number of assets.

   - **Edition**: The Enterprise Edition is selected by default. For more information about the differences between the Enterprise Edition and Basic Edition, see *Threat Detection Service features*.

   - **All Logs**: Value-added service. If you select this option, TDS includes this service. Ten types of security logs (such as server logs and network logs) can be searched for event backtracing and security analysis.

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

   > 📋 **Note:**
   >
   > - If you want to protect up to five assets, you must purchase at least a one-year subscription. If you want to protect from six to ten assets, you must purchase at least a three-month subscription. If you want to protect more than 10 assets, you must purchase at least a one-month subscription.
   >
   > - If you enable automatic renewal, the automatic renewal cycle is aligned with the validity period of your subscription. For example, if your subscription is on a monthly basis,

> the automatic renewal cycle is one month. If your subscription is on a yearly basis, the automatic renewal cycle is one year.

4. Click **Buy Now** and complete the payment.

3 Renewal and Upgrade

To maintain normal service of your Threat Detection Service (TDS) Enterprise Edition subscription, we recommend that you renew your TDS subscription before its expiration date. If you do not renew your subscription before it expires, you can renew your TDS subscription within three days after it expires so that the system retains your configurations and data. If the number of servers under your account is more than 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 associated fees, to continue your current TDS Enterprise Edition subscription.

Expiration

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

For three days after your TDS subscription expiration date, the system retains all of your TDS configurations and data, including your asset groups, tags, quarantined files, vulnerability whitelist , baseline check policies, baseline check whitelist, function configurations, and asset fingerprints . You must renew your TDS subscription within the specified three days to retain your configurat ions and data.

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

Renew TDS Enterprise Edition

To renew your TDS Enterprise Edition subscription, follow these steps:

1. Log on to the *Threat Detection Service console*.

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

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

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

4. Click **Pay Now** and complete the payment.

Upgrade

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

During the subscription period of your TDS 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 as to upgrading your TDS subscription. If this occurs, you must upgrade your TDS subscription to continue using the service.

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

Upgrade TDS Enterprise Edition

To upgrade your TDS Enterprise Edition subscription, follow these steps:

1. Log on to the *Threat Detection Service console*.
2. In the upper-right corner of the **Overview** page, click **Upgrade**.

   > 📋 **Note:**
   >
   > Only when the number of servers under your account is more than 120% of the number of assets configured for your current subscription, the **Upgrade** button displays on the **Overview** page.

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