

# **Tencent Smart Advisor**

## **Getting Started**

## **Product Documentation**





#### **Copyright Notice**

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

#### S Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

#### Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

## **Getting Started**

Last updated : 2022-11-07 11:33:52

This document describes how to quickly perform resource inspections in the Tencent Smart Advisor console.

## Step 1. Log in to the Tencent Smart Advisor console

Log in to the Tencent Smart Advisor console.

Note:

If you don't have an account yet, sign up as instructed in Signing up for a Tencent Cloud Account.

## Step 2. Authorize the service

If this is your first time using Tencent Smart Advisor, you need to grant permissions to it, so that it can access the Tencent Cloud services. If you have authorized it, skip this step.

On the Authorization page, toggle on Service Authorization.

s	ervice Authorization
	Service Authorization Authorize Advisor to assess Tencent Cloud resources, such as CVM, VPC, and MySQL. For more information about service-linked role authorization, please see: Cloud Access Management - Role. Status Authorized successfully
	Report Access O

## Step 3. Start risk assessment

Select **Risk Assessment** on the left sidebar and click **Start Assessing**. Then, the system will perform the assessment automatically.

#### Note:

By default, the system performs an automatic inspection every day. You can also manually trigger it.

An assessment operation may take dozens of seconds to minutes subject to the Tencent Cloud resource size and number of assessment items. The result is dynamically refreshed on the page until the assessment is complete.

## Step 4. View the assessment result

After the assessment, you can view the result on the Risk Assessment page.

#### **Overall description**

The console UI is as shown below:

Sunt Assessment time: 2022-10-17 17:06:28      Filter by product name or assessment item; separate keywords     Q					
Overview	Security	Reliability	<b>Performance</b>	Cost	Service Restriction
• 1 • 8 • 79	•1 •1 •12	•0 •3 •32	• 0 • 0 • 19	• 0 • 4 • 6	

Last Assessment Time: Time of the last assessment.
Color: Red indicates "high-risk items", orange "mid-risk items", and green "healthy".
Overview: Collects and displays the assessment results of all items.
Security: Collects and displays the assessment results of items by Security.
Reliability: Collects and displays the assessment results of items by Reliability.
Performance: Collects and displays the assessment results of items by Performance.
Cost: Collects and displays the assessment results of items by Cost.

Service Restriction: Collects and displays the assessment results of items by Service Restriction.

#### **Risk item details**

Click to expand a risk item and view its details.

• CAM - account-MFA device binding									
Check whether an account is bound to an MFA device, and if not, dynamic verification code-based MFA is not required for account login, reducing the security level									
Alarm Condition	Alarm Condition								
<ul> <li>No MFA devices are bound for both login and sensitive operation</li> </ul>	No MFA devices are bound for both login and sensitive operations								
<ul> <li>No MFA devices are bound for login or sensitive operations</li> </ul>	No MFA devices are bound for login or sensitive operations								
Optimization Advice         We recommend you bind your account to a virtual MFA device in the console to add another layer of security verification for relevant account operations and thus protect the account security         Resource List         1 account(s) is/are not bound to MFA devices.0 account(s) was/were ignored.         Assessed Resource       Ignored Resources									
Ignore Restore			Separate keywords with $\uparrow\uparrow$ press Enter to separate filter tags $\hfill \ensuremath{\mathbf{Q}}$						
UIN	Sub Accout Count	Tag	Operation (						
• 100011015907	4	None	Ignore Restore						
Total items: 1			10 ▼ / page H < 1 / 1 page > H						

Alarm Condition: Alarm condition for triggering the risk item.

Optimization Advice: Suggested measures to avoid the risk item.

Resource List: List of resources with high- and mid-risk items in this assessment.

## Step 5. Download the assessment report

You can generate a report by module or risk item in the following steps:

1. Go to the **Risk Assessment** page, find the target module or risk item, and click **Generate Report**.

Overview • 1 • 8 • 79	Security •1 •1 •12	Reliability • 0 • 3 • 32	Performance • 0 • 0 • 19	Cost • 0 • 4 • 6	Service Restriction	
Overview 1 Generate Report						
• • CAM - account-MFA device bindin	g <u>I</u> Generate Report					
Check whether an account is bound	Check whether an account is bound to an MFA device, and if not, dynamic verification code-based MFA is not required for account login, reducing the security level					
1 account(s) is/are not bound to Mf	A devices.0 account(s) was/were ignored.					

2. After the report is generated, click **Download Report**.

3. In the **Download Assessment Report** pop-up window, select **Assessment report in Excel** or **Assessment report in PDF** as needed and click **OK**.

# Step 6. Get the expert explanation of the assessment report (optional)

You can get the expert explanation of the assessment report in this step.

1. Service authorization

Go to the Authorization page and enable Report Access to have Tencent Cloud architects read the report for you.

Service Authorization			
Service Authorization 🚺			
Authorize Advisor to assess Tencent Cloud resources, such as CVM, VPC, and MySQL. For more information about service-linked role authorization, please see: Cloud Access Management - Role.			
Status Authorized successfully			
Report Access 🔵			
Authorize Tencent Cloud architects to read assessment reports so that they can provide optimization advice.			

2. Expert explanation

To reach Tencent Cloud architects and have their insights into your report, contact us.